International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 11 (November 2014), PP.16-27

A Proposed Solution to Secure MCC Uprising Issue and Challenges in the Domain of Cyber Security

Dr. Mani Sarma Vittapu[1,] Atoyoseph Abate[2] and Dr.Venkateswarlu.Sunkari[3]

[1]*Assistant Professor, Dept. of. ITSC, Addis Ababa Institute of Technology, AAU, Addis, Ethiopia.*
[2] *HOD of ITSC, Addis Ababa Institute of Technology, AAU, Addis, Ethiopia.*
[3] *Assistant Professor, Dept. of. ITSC, Addis Ababa Institute of Technology, AAU, Addis, Ethiopia.*

Abstract:- The development of cloud computing and mobility,mobile cloud computing has emerged and become a focus of research. By the means of on-demand self-service and extendibility, it can offer the infrastructure, platform, and software services in a cloud to mobile users through the mobile network. Security and privacy are the key issues for mobile cloud computing applications, and still face some enormous challenges. In order to facilitate this emerging domain, we firstly in brief review the advantages and system model of mobile cloud computing, and then pay attention to the security and privacy in the mobile cloud computing. 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. By deeply analyzing the security and privacy issues from three aspects: mobile terminal, mobile network and cloud, we give the current security and privacy approaches. 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,challenges and possible solutions for the security issues.

Keywords:- Mobile Cloud Computing (MCC), Security, privacy,

I. INTRODUCTION

Mobile services have gained speed by the emerging cloud computing technologies, as these devices take an important role in the human life as both communication and entertainment, not bounded by time and place. The mobile computing (MC) becomes powerful and rapid in the development of IT technology within commerce and industry fields, as well. On the other hand, the mobile devices are facing up with many struggles in their resources (e.g., battery life, storage, and bandwidth) and communications (e.g., privacy, mobility and security) [1]. These challenges affect the improvement of service qualities badly. Cloud computing (CC) started to be widely used and brought many opportunities in the means of resources like servers, networks, and storages, platforms and software at very low costs. This ease of use and low cost of CC can lead mobile applications to be more widespread and provide variety of services in the mobile environment. The mobile applications can be thought a new way from the cloud providers' perspective; it can be integrated with the existing cloud system without needing any additional costly infrastructure, but new types of services and facilities for the mobile users. 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.

II. MOBILE CLOUD COMPUTING

Mobile Cloud Computing is a new paradigm for mobile applications whereby most of the processing and data storage associated with the applications is moved off the mobile device to powerful, centralized computing platforms located in the Cloud. These centralized applications are then accessed over the mobile Internet, using either a thin native client or web browser on the device. However, this model for Mobile Cloud Computing still does not fully leverage the powerful communications, context and commercialization capabilities of the mobile network itself. Mobile Cloud Computing builds

on the principles of cloud computing, bringing attributes such as on demand access, no on premise software and "XaaS" (Everything as a Service) to the mobile domain, adding Network as a Service (NaaS) and

Payment as a Service to the maximum of on demand capabilities and allowing applications to leverage the full power of mobile networking and billing without the need for specialist application servers. The phrase “Mobile Cloud Computing” was introduced after the concept of “Cloud Computing” was launched in mid2007. It has been attracting the attention of entrepreneurs as a profitable business option that reduces the development and running cost of mobile applications and mobile users as a new technology to achieve rich experience of a variety of mobile services at low cost, and of researchers as a promising solution for green core IT.

The Mobile Cloud Computing Forum defines MCC as “Mobile Cloud computing at its simplest refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just smart phone users but a much broader range of mobile subscribers”.

In 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. 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 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 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 software’s 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 .

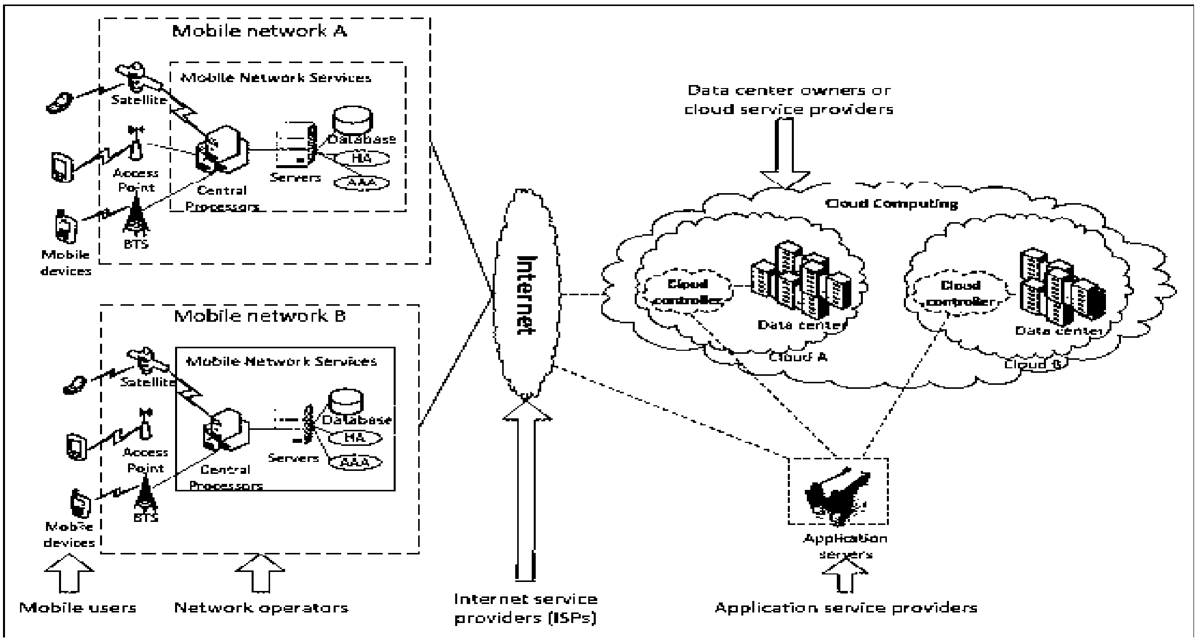

Figure.1. Mobile Cloud Computing Architecture

2.1 Cloud Service Delivery Models

The cloud computing model is based on three service delivery models and three cloud deployment models. 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.

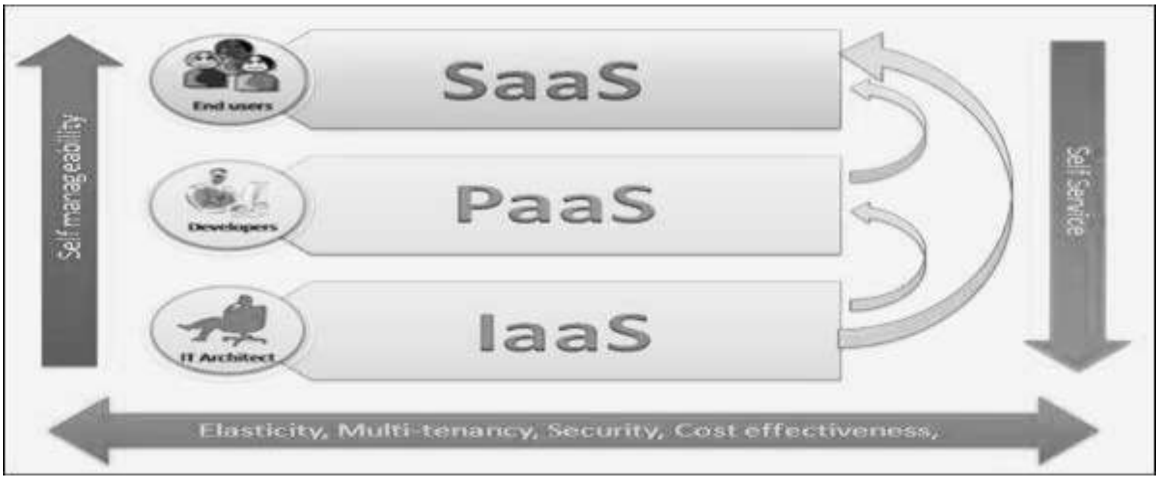

Figure.2 Layered architecture of Cloud Computing

2.2. 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 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 3 gives a literature review on mobile cloud computing. Section 4 provides the issues and challenges of MCC. Existing solutions provided for security issues in section 5. Explained proposed work and experimental results in section 6. Section 7 gives possible solutions for the security issues and the last section 8 concludes with summary.

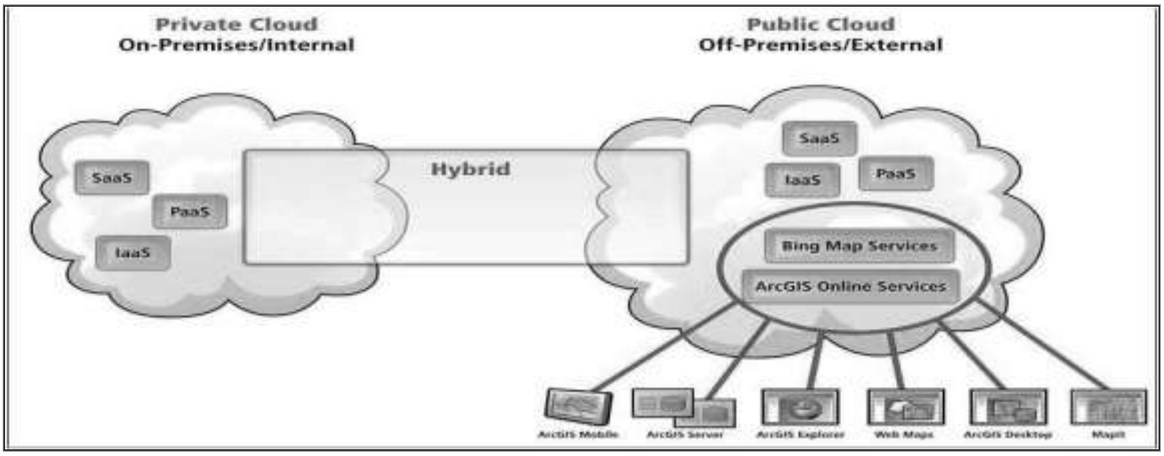

Figure.3 Three types of Cloud Computing Deployment Models

III. LITERATURE REVIEW

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 hasalso 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.

IV. MAJOR 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.

Table 1: Categorized Issues and Challenges.

Category	Issues	Challenges
Data Security and Privacy Issues	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.Servicesincompatibility because of different vendors involvement 9. Generation of Data. 10. Transfer of Data. 11. Use and Share of Data. 12. Storage. 13. Archival and Destruction.	1. Device Data Theft 2. Virus and Malware Attacks via Wireless Devices 3. Miss-use of Access Rights 4. System Security of Server and Database 5. Networking Security 6. User Authentication 7. Data Protection 8.System and Storage Protection
Architecture and Cloud Service Delivery Models Issue	1. Computing off-loading. 2.SecurityforMobile 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	***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.DataSecurity Management 2.Web Application Vulnerability and Scanning
Mobile Cloud Infrastructure Issues	1.Attacks on Virtual Machines 2.Vulnerabilities exists at platform level 3. Phishing 4.Authorizationand Authentication 5. Attacks from Local Users 6.Hybrid Cloud Security Management Issues	
Mobile Cloud Communication Channel Issues	1. Access Control Attacks 2. Data Integrity Attacks 3. Attacks on Authentication 4. Attacks on Availability	1. Low Bandwidth and Latency problems 2. Availability of Desired Services 3. Heterogeneity 4. Limited Resources

V. EXISTING SOLUTIONS PROVIDED FOR SECURITY ISSUES

Anand Surendra Shimpi [8] proposed a secure framework for processing data in mobile cloud computing. This framework stores data in a secured fashion which helps in protecting the user's privacy. In addition, he has implemented a project named "Focus Drive" which improves the driving safety of teenagers. Jibitesh Mishra [9] proposed a secure architecture for MCC to integrate mobile applications with the various cloud services. This architecture improves the storage and processing of data on mobile devices in a secured manner. It helps in maintaining the integrity and security of data. Itani et al [10] proposed a framework which was energy efficient for mobile devices to assure mobile user's integrity i.e. using *incremental cryptography and trusted computing,* the data/files of users are stored in the cloud. This framework results in saving 90% of processing energy on the mobile devices when compared to other conventional techniques with more security. Eugene E. Marinelli [11] developed *Hyrax*, a platform from Hadoop which supports cloud computing on Smartphones. It allows user's applications to utilize data and computing process on networks on Smartphones. It offers a sane performance in data sharing and tolerates node departure. Eugene also implemented a distributed media search and data sharing approach. Jon Oberheide [17] proposed an architecture which contains three components:

a) **Host Agent:** It is a lightweight process that runs on each device and inspects the activities of the files on the system. It stores the unique identifier (such as hash) in the cache for files received. If a new file does not hold file identifier, it will be sent to the Network Service.

b) **Network Service:** This service analyses the files sent by the host agent. There can be multiple instances of Network Services that are running on the cloud using virtualization technique which supports parallel detection of multiple files sent by multiple host agents.

c) **Caching:** *Local private cache (LPC) and Global shared cache (GSC)* are the two cache agents where LPC can be put into the identifier of inspected files and GSC cache resides on the Network Service which has the identifiers of all inspected files received so far.

Security and privacy are always a key issue when the data are shared between mobile devices and the cloud. Even though WPA2 (Wi-Fi Alliance, 2012) provides layer-2 encryption of the data, layer-6 encryption is still a requirement because it requires some external applications like bioinformatics or computational chemistry that are executed on mobile devices and remotely on rented/ commercial cloud platforms (such as Google (2012, AWS (2012), Microsoft (2012)) which require an additional layer of security.

Table 2: Comparison of evaluated data security framework

Basic Theory	Data Protection	Data Integrity	Authentication	Scalability	Data Access
Incremental Message Authentication n Code	**No**	**Yes**	**No**	**Moderate**	**---**
Standard Cryptography Functions	**Yes**	**Yes**	**Yes**	**Moderate**	**Automated**
Merkle Hash Tree, Diffie-Hellman Key Exchange	**Yes**	**Yes**	**Yes**	**Moderate**	**Automated**
Exclusive- OR	**Yes**	**Yes**	**Yes**	**Highly Scalable**	**Semi-Automated**
Bilinear- Pairing, Access Policy Tree	**Yes**	**No**	**No**	**Highly Scalable**	**Automated**

Table 2. Comparative Analysis for Strengths and Limitations of Some of the Existing Security Schemes

Security	Scheme	Suggested Approach	Strengths Limitations
Data Storage security	Uses holomorphic token with distributed verification of erasure-coded data towards ensuring data storage security and locating the server being attacked.	1.Supports dynamic operations on data blocks such as: update, delete and append without data corruption and loss. 2. Efficient against data modification and server colluding attacks as well as against byzantine failures.	1. Supports dynamic operations on data blocks such as: update, delete and append without data corruption and loss. 2. Efficient against data modification and server colluding attacks as well as against byzantine failures.
User identity safety in cloud computing	Uses active bundles scheme, whereby predicates are compared over encrypted data and multiparty computing.	Does not need trusted third party (TTP) for the verification or approval of user identity. Thus the user's identity is not disclosed. The TTP remains free and could be used for other purposes such as decryption.	Active bundle may not be executed at all at the host of the requested service. It would leave the system vulnerable. The identity remains a secret and the user is not granted permission to his requests.
Trust model for interoperability and security in cross cloud	1. Separate domains for providers and users, each with a special trust agent. 2. Different trust strategies for service providers and customers. 3. Time and transaction factors are taken into account for trust assignment.	1. Helps the customers to avoid malicious suppliers. 2. Helps the providers to avoid cooperating/serving malicious users.	Security in a very large scale cross cloud environment is an active issue. This present scheme is able to handle only a limited number of security threats in a fairly small environment.
Virtualized defence and reputation based trust management	1. Uses a hierarchy of DHT-based overlay networks, with specific tasks to be performed by each layer. 2. Lowest layer deals with reputation aggregation and probing colluders. The highest layer deals with various attacks.	Extensive use of virtualization for securing clouds.	The proposed model is in its early developmental stage and needs further simulations to verify the performance.
Secure virtualization	1. Idea of an Advanced Cloud Protection system (ACPS) to ensure the security of guest virtual machines and of distributed computing middleware is proposed. 2. Behaviour of cloud components can be monitored by logging and periodic checking of executable system files.	A virtualized network is prone to different types of security attacks that can be launched by a guest VM. An ACPS system monitors the guest VM without being noticed and hence any suspicious activity can be blocked and system's security system notified.	System performance gets marginally degraded and a small performance penalty is encountered. This acts as a limitation towards the acceptance of an ACPS system.
Safe, virtual network in cloud environment	Cloud Providers have been suggested to obscure the internal structure of their services and placement policy in the cloud and also to focus on side-channel risks in order to reduce the chances of information leakage.	Ensures the identification of adversary or the attacking party and helping us find a far off place for an attacking party from its target and hence ensuring a more secure environment for the other VMs.	If the adversary gets to know the location of the other VMs, it may try to attack them. This may harm the other VMs in between.

VI. PRIVACY SCHEMA DETAILS

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

RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. By securing the data, we are not allowing unauthorized access to it. User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider, Cloud provider authenticates the user and delivers the data. RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with thecorresponding Private-Key only.

RSA algorithm involves three steps:
1. Key Generation
2. Encryption
3. Decryption

6. 1. Key Generation

Before the data is encrypted, Key generation should be done by the Cloud Identity Service Provider. Let F be a pseudo-random function, let Ƞ be a pseudo-random permutation and let H be a cryptographic hash function.

Generate pk = (N, g) and sk = (e, d, v), such that $ed \equiv 1(\mathrm{mod}\, p' q')$, e is a large secret prime such that $e > \lambda$ and $d > \lambda$, g is a generator of QRN and v R ← {0, 1}k.
Output (pk, sk).
Tag Block (pk, sk, m, i):
1. Let (N, g) = pk and (d, v) = sk.
Generate Wi = v||i.
Compute Ti,m = (h(Wi) · gm) d mod N.
2. Output (Ti,m, Wi).

6.2 Encryption

Encryption is the process of converting original plain text (data) into cipher text (data).

Steps:
1. Cloud service provider should give or transmit the Public Key (N, g) to the user who wants to store the data with him or her.
2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
3. Data is encrypted and the resultant cipher text (data) C is C = mg (mod N).
4. This cipher text or encrypted data is now stored with the Cloud service provider.

6.3 Decryption:

Decryption is the process of converting the cipher text (data) to the original plain text (data).

Steps:
1. The cloud user requests the Cloud service provider for the data.
2. Cloud service provider verifies the authenticity of the user and gives the encrypted data i.e, C.
3. The Cloud user then decrypts the data by computing, m = Cd (mod N).
4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

6.4. EXPERIMENTALRESULTS

In this section, we are taking some sample data and implementing RSA algorithm over it.

Key Generation:
1. We have chosen two distinct prime numbers a=61 and b=53.
2. Compute n=a*b, thus n=61*53 = 3233.
3. Compute Euler's totient function, Ø(n)=(a-1)*(b-1), Thus Ø(n)=(61-1)*(53-1) = 60*52 = 3120.

4. Choose any integer e, such that 1 < e < 3120 that is co-prime to 3120. Here, we chose e=17.
5. Compute d , d = e-1(mod Ø(n)), thus d=17-1(mod 3120) = 2753.
6. Thus the Public-Key is (e, n) = (17, 3233) and the Private- Key is (d, n) = (2753,3233). This Private-Key is kept secret and it is known only to the user.

Encryption:
1. The Public-Key (17, 3233) is given by the Cloud service provider to the user who wishes to store the data.
2. Let us consider that the user mapped the data to an integer m=65.
3. Data is encrypted now by the Cloud service provider by using the corresponding Public-Key which is shared by both the Cloud service provider and the user. C = 6517(mod 3233) = 2790.
4. This encrypted data i.e, cipher text is now stored by the Cloud service provider.

Decryption:
1. When the user requests for the data, Cloud service provider will authenticate the user and delivers the encrypted data (If the user is valid).
2. The cloud user then decrypts the data by computing, m = Cd(mod n) =27902753(mod 3233)= 65.
3. Once the m value is obtained, user will get back the original data.

VII. POSSIBLE SOLUTIONS FOR THE SECURITY ISSUES

Of all the above discussed issues, data security is the most prevalent issue during data transfer. Here are some possible solutions. The first solution is to come with a new model of security where detection services like Intrusion Detection System (IDS) and Cloud Intrusion Detection System Services (CIDSS) take place in the cloud which obviously saves the device CPU process and memory. This detection services solution have several benefits:

- Better detection of malicious code.
- Reduced consumption of resources on mobile devices.
- Reduced Software complexity of mobile devices.

Next, it is possible to achieve the security by implementing the homomorphic encryption mechanism with the combination of level-6 encryption that can be adopted when the data passes between the cloud, mobile and cloudlet without any requirement of external applications. Level-6 encryption is mainly used for secure text encode and decode which requires the use of JavaScript and browsers. To save the mobile resources, level-6 encryption should rely and be executed remotely on the cloud. This solution provides the best security and scalability feature during data sharing.

If the data with malicious codes are downloaded by a user, the cloud account and data will be extracted and the unfair accounting will occur.

Only verified data should be downloaded and the applications with abnormal activities should be blocked.

Through broadcasted SSID, the information can be leaked and unauthorized user can gain access.

Disable the SSID broadcast and utilize an enhanced key authentication algorithm.

Here are some steps given for winning the battle of breaches:

1. Prioritize the objectives and set the risk tolerance.
Protecting data assets in the workplaces has been a challenge to the security professionals for decades. The truth is that there is no such thing as 100-percent secure. Hard decisions should be made at different levels of protection needed for different parts of the business.

2. ***Protect the data with proactive security plan.***
Security planning is not an easy task for an organization. This includes understanding the threat landscape (i.e. hacking cybercrime attacks, media & social scams, etc.) and working to protect the organization against these threats, require both policy and technology.

3. Prepare the response to the inevitable sophisticated attacks.
With the evolution of advanced continual threats, hackers aim on finding vulnerability. It is certain that eventually the organization will move towards data breach. Since the malware attacks are on the increase in today's technology, the unified and tested response plan is under critical state for the right resources and skills.

4. ***Promote the culture of security awareness.***

It is important to note that the careless mistakes of one employee will affect the master plan of chief security officer. That's why every employee must work in a group with security professionals to ensure the safety of enterprise data. Security must be built on the culture of the organization.

VIII. CONCLUSION

This paper investigates the security concepts of Mobile Cloud Computing (MCC), challenging security issues and breaches, various existing security frameworks and finally some solutions that increase the security in the Mobile Cloud Environment. Most of the frameworks overlooked the security of user data privacy, data storage and energy preserving data sharing. It is evident that user data privacy and mobile application that uses cloud are the most challenging factor. To attain more security in mobile cloud environment, threats need to be addressed and studied accordingly. To address all these security issues, the data security plan needs to be developed which reduces the security risks and also to cut costs and complexity to adopt the cloud computing in mobile environment. It is essential to keep in mind that the designing of the future framework solutions should be more cost effective and should provide better security and performance today.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.

REFERENCES

[1]. MohsinNazir ,MirzaShuja 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.

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

[3]. 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.

[4]. 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).

[5]. 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.

[6]. 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).

[7]. 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.

[8]. 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.

[9]. 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).

[10]. 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.

[11]. Preston A. Coz, “Mobile Cloud Computing: Devices, trends, issues & enabling technologies”, 2012.

[12]. [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]. Anand SurendraShimpi and R. Chander, “Secure Framework in Data Processing for Mobile Cloud Computing”, International Journal of Computer & Communication Technology, ISSN (Print) 0975-7449, vol. 3, Iss. 3, 2012.

[14]. Itani et al, “Towards secure mobile cloud: A survey”, Proceedings of Analyses paper, 2012.

[15]. Han Qi and Abdullah Gani, “Research on Mobile Cloud Computing: Trends, Review and Perspectives”, Proceedings of Analyses paper, University of Malaya, Malaysia, 2012.

[16]. Jibitesh Mishra, Sanjit Kumar Dash and Sweta Dash, “Mobile Cloud Computing: A Secure Framework of Cloud Computing for Mobile Application”, Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2012, pp. 347- 356.

[17]. 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.

[18]. E. Bertino (2009) Privacy-preserving Digital Identity Management for Cloud Computing. IEEE Data Engineering Bulletin, 32, p. 21-27.

[19]. NEC Company, Ltd. and Information and Privacy Commissioner, Ontario, Canada. "Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach, (2010), http://www.ipc.on.ca/images/Resources/pbd-NEC-cloud.pdf.

[20]. https://wiki.cloudsecurityalliance.org/guidance/index.php/Cloud_Computing_Architectural_Framework.

[21]. 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.