Security issues in Mobile Computing Vs Mobile Cloud Computing from User Perspective

Beenish Abid, Namra Sheikh

Abstract- With the advancement in computing devices, the methods of computation evolved quite rapidly. It was just today when the computation became mobile. With the increased demand of better computation capabilities, vendors are looking for ways of achieving computation speeds unheard of. Every device offers some limit to the computation speed as there is always a tradeoff between cost and computation capability. Researchers took a big step towards enhancing the computation capability of mobile devices by introducing cloud computing, thus leading to a new era where mobile cloud computing improves user experience by utilizing cloud resources for processing. This approach facilitates the vendors to offer improved computation capabilities but associated security issues proved to be a great hurdle in the path of mobile cloud computing success. This research highlights some major security concerns of a mobile user to bring vendors and researchers are on the same page. We compare traditional mobile computing approach of these security issues with the emerging mobile cloud computing technique. Motivation behind this initiative is that unless smartphone vendors understand user perspective clearly they will not be working on the right track for achieving user appreciation for new trends like mobile cloud computing.

Index Terms—— Mobile computing; mobile cloud computing, security issues, mobile computing Vs mobile cloud computing, user concerns over mobile computing ,cloud computing issues, security threats in mobile computing

1. INTRODUCTION

In today's world, mobile computing (MC) is getting more attention than before due to an increased user interest in mobile devices such as laptops, PDAs, tablets or smartphones etc. [1]. Following the success of desktop computers and laptops, the latest market trend shows a rapid increase in the use of smart phones that are capable of performing most of the computation tasks themselves that a personal computer is capable of doing. Every individual whether he is a child or an adult possess at least one such computation device.

With the growth of mobile phone market, the emphasis on MC is now increasing day by day. The focus of device vendors is on providing better and better computation devices so that users can access everything over their smart phones. This situation led to a competition between different vendors which push them to launch new devices each year with enhanced feature. However, the computation limits have already been reached so the researchers and vendors are trying to come up with new strategies to open the gateway of further improvement in computation metrics. Since last few year, various research teams have been working to overcome the limitation of mobile computing devices and thus after lot of effort they introduced the idea of mobile cloud computing (MCC).

MCC takes advantage of mobile computing, cloud computing and wireless technologies to facilitate the user by improving the computation of a mobile device [2]. MCC technology facilitates user by removing the device computation constraints and allowing the device to utilize resources over cloud for improving the user computation experience. Although mobile computing is revolutionizing the way computation is being done on a mobile device, but it is also introducing some issues regarding the user security which raises concerns from user community.

Many users are resisting the shift from traditional computing methodologies to the emerging mobile cloud computing techniques. One major cause of this resistance is the communication gap between users and vendors of the mobile devices, which is creating hurdles in the success of new technological advancements. Users have been raising security concerns again and again but the vendors continue to focus on feature enhancement instead of addressing these concerns properly. Unless the users are satisfied and safe from the major threats that include privacy, information leakage, data loss etc. they will continue to step aside from these new trends leading to the loss of both parties. In order to get active participation from users, the vendors need to address the user concerns appropriately by either accommodating their requests in later versions of mobile devices or help the users understand the perspective of device vendors, so that both parties are on the same page. This will not only resolve misunderstanding among consumers but also help them to figure out future direction of mobile market collectively.

The motivation behind this comparative study is to identify such concerns related to MCC and present a comparison with MC technique for achieving the same functionality for a particular consumer. We also highlight some user concerns which have not been addressed by mobile vendors and researchers so far. These issues if addressed properly will increase user trust and develop a mutual understanding between consumers and vendors in the use of a particular mobile device. Our goal is to reduce the communication gap between users and vendors by bringing them on same page to resolve these security issues in mobile computation devices with consensus from both parties. This will reduce the hurdles in path of technical growth of mobile market by securing user trust and their involvement in the technological advancement.

This paper is organized as follows. Section 2 reports the literature survey on security issues of mobile computing and mobile cloud computing. In section 3, we present a comparison of these issues in MC and MCC from a user perspective. Section 4, covers the results and discussions. In section 5, we conclude our work and propose future directions.

2. LITERATURE SURVEY

A vast domain such as mobile computing [3] covers software, hardware, communication and interaction processes for a mobile computer. With the evolution of computing from computers to laptops, and then from laptops to mobile devices, users are now able to work anywhere in the world. Mobile computing [4] has increased productivity with reduced cost for its customers. Portability in mobile computing has no comparison with the basic desktops and laptops. It facilitates business workers by allowing them to access and create their information quickly. This feature increased economy of people.

The author in [5] has described the characteristics of mobile computing, different communication technologies and many such mobile interaction modules. Author presented an overview of the limitations faced in mobile computing such as security and power issues. There are computation limitations to the users of mobile computing. Usually the mobile internet access is slower as compared to the LAN networks thus providing less bandwidth. Interfaces of mobile devices are often small and hard to use. Authors in [5, 6] have also discussed security issues in mobile computing which are the drawbacks of this technology.

Security Issues in mobile computing [5] also cover the information security issues involved in it. With the advancement in technology, mobile computing must fulfill needs of the users around the world by securing their information, data, and privacy modules. Websites that are viewed on laptops and desktops are often more visible for human interaction as compared to interaction with the mobile device. People mostly don't use all the applications of a mobile device because most of them access their personal data for installation and usage of that application. Security of the user information is very important for the success of any application or computing device. Till now mobile computing has introduced many security challenges but still it has to work to fulfill its promises to the consumer world [6].

Authors in [1] focus on security issues related to interaction in mobile computing. They discussed types of mobile computing and security issues such as disconnection, data access, mobility and operation modes etc. They highlight interaction issues over wireless communication network. Authors emphasize three major sources of mobile user data which put potential threats of user information leakage. These data sources include mobile devices themselves, the network traffic and the databases holding user information. Protecting these sources of data from unauthorized access is very important for ensuring integrity and security of user information. Authors suggested some approaches that if used will lessen the vulnerability and make the interaction of mobile device more secure.

In [7] author highlights the issues in mobile computing and gives insight on cryptographic solutions for dealing with wireless security problems. They discuss different architectures and protocols such as encryption techniques, symmetric key, RSA, public or private key and many more which use cryptography for ensuring data security of the mobile user. Author acknowledges the contribution of a project in introducing protocols to overcome MC security issues of wireless technology.

Authors in [8] discuss some operational and security issues related to mobile computing. They present the basic infrastructure of mobile computing and highlight the benefits that it provides. They propose that use of mobile agents' increases reliability of mobile computing in wireless networks. As an example, authors discuss a health care mobile computing system using this concept with respect to the security concerns.

Authors in [9] present the working of MCC and different security concerns that are emerging with the growth of smartphone market. According to the authors, remote processing of data is leading to more and more vulnerability thus causing security issues for the user. Authors also discuss solutions for some of these problems and propose the development of a security plan for reducing such problems in future.

In [10] authors describe the infrastructure flexibility offered by MCC and corresponding security concerns regarding the user data. Authors say that MCC offers on-demand networking infrastructure leading to a new dimension of data processing, however these features of MCC impose a security threat. According to the authors, user privacy and data security is one of the major concerns of cloud service providers. Authors categorized the issues related to security into two major parts: mobile network security and the security over cloud.

Cloud computing has various challenges and possibilities in it. Amongst them security is thought to be the most critical issue in the success of cloud computing [11]. The security challenges are very versatile and thus raising alerts from user community. Data location is the considered to be a crucial factor [12]. In the context of cloud computing, a security concern is usually some type of risk but any risk cannot be blindly listed as a security concern. Among many parties which are involved in the cloud computing infrastructure, assignment of responsibilities might come out to be an experiencing inconsistency due to which security vulnerabilities may arise. The provision of insider attack still remains a valid threat for cloud computing [5].

Mobile devices can connect with different types of wireless networks. Smartphones today are capable of using various generations of mobile data transmissions and technologies like 1G, 2G, 3G, and 4G. Infrared, Bluetooth, Wi-Fi, Satellite and WiMAX based communication are some of the other standards used for data transmission now days. All these technologies may not be used for mobile data transmission particularly but still they can be used to some extent for this purpose. Some of the major security threats for mobile cloud computing listed by Authors in [6] include Electronic tracking, Spam, Cloning, Incorrect disposal of the device, loss, theft or removable memory cards and their data, unauthorized access and wireless connection vulnerabilities.

With an increase in mobile devices, a new technology from the inheritance of cloud computing is introduced which is known as Mobile Cloud Computing (MCC) [13]. This technical advancement attracted many entrepreneurs and businessman by providing them a prospective business opportunity. MCC overcomes many mobile resource limitations by utilizing the idea of virtual resources for a common user. The author provided comprehensive information related to MCC security problems and also some of its limitations. With the use of MCC in mobile devices a tremendous change has been revolutionized along with some new challenges to encounter.

In recent years, much attention from research perspective has been given to data security issues in the cloud environment. In [14] author focuses on privacy in cloud environment. Author believes to accept cloud for improving security, reducing risk thus encouraging MCC technology. Author's targets are the consumers using cloud computing in order to identify the security situation in cloud based mobile environment. Author proposed an organization as a guardian for security and thus developed an interface between customer and the service provider, which provides a reliable transfer of data between consumers.

Author in [15] highlights the three main aspects namely the security, architecture and challenges of MCC technology. If all these three conditions are addressed properly, then services of the cloud are acceptable. Although the absolute security is unattainable but still maintaining an acceptable level by defining the type of security required for these technologies, mobile devices are within our access.

The author [16] has discussed security issues and risks involved in MCC. There are two types of issues namely: cloud and security threats. Some basic pillars need to provide a major security in order to secure the whole cloud computing process. According to a recent research, a number of security attacks have been found such as application, physical and web based attacks. These are all linked to the privacy threats. Attackers used different techniques to attack private data of the client, who has no idea that what is happening to his assets. MCC raises many security concerns due to the fact that it combines mobile computing with the cloud.

The MCC consumers have many serious concerns over cloud environment [14]. Although cloud computing is common these days and developing day by day, still it has some architectural issues for the mobile users. The author discussed MCC infrastructure issue and concerns which cover the detail of the attacks on the computing devices from local users. Author presented an overview and understanding of MCC with an explanation of its architecture, advantages, security issues and limitations. The main issues and challenges of MCC are being discussed including data security, information security and communication channel security. Main idea behind the research is to identify the major issues regarding the information, data, architecture and new challenges which prevent the users to move towards the cloud services. The author wants to make this research useful for the mobile vendors so that by taking all the aspects in their view, they can provide a well secured and innovated technology to their consumers where the user is free to use the cloud services without any threat. The users are still below the expectations to adopt MCC because of the security and privacy factors. A lot of research is being done to cover this flaw but still now a significant amount of work has to be done to cover the security prone.

As discussed above lot of concerns and issues have been raised in both and mobile computing domain as well as mobile cloud computing domain. User concerns are increasing as the device vendors continue to adapt MCC architecture for enhancing device computation capabilities. The purpose of this study is to gather some major concerns that have been raised so far and review them in the light of both MC and MCC architectures. This comparison will help the users and vendors understand more clearly, what are the basic architectural differences between MC and MCC from the point of view of a particular security issue raised by users. This develops a better understanding by bringing smartphone users and vendors on the same page in order to address these problems precisely. Unless the user concerns are resolved, the acceptance of MCC trend by the users will be slow and fearing.

3. SECURITY ISSUES

Lot of research is being done on the issues of both the domains of MC and MCC. But some of the major user concerns that are highlighted time and again not only by the user community but also many researchers are presented in this section. We review each security issue for traditional MC approach as well as the emerging trend of MCC. Keeping both approaches in view while analyzing the security problems will help in understanding that how the shift from MC to MCC is affecting the mobile device user and why the list of security issues is increasing day by day. Let's review the following security issues:

A. *Connectivity*

Connectivity in mobile computing refers to the link that exists between two nodes when these nodes are continuously connected through a network terminal and there is no limitation in their connection. Connectivity in mobile computing and mobile cloud computing is shown in Fig. 1 below.

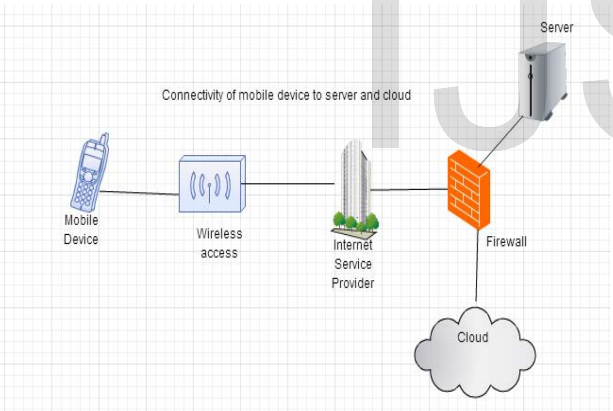
Server
Connectivity of mobile device to server and cloud
Mobile Device
Wireless access
Internet Service Provider
Firewall
Cloud

Fig.1. Connectivity in mobile and mobile cloud computing

Many people require connectivity between their mobile devices over a wired or wireless network. Mobile connectivity is variable in the aspect of performance and reliability. It depends on the building infrastructure that is able to provide whether a low or a high bandwidth network. In wireless communication disconnection is a major security concern. Whenever a mobile is connected to a network, resources must be handled elegantly to avoid disconnections [4].

Portable Internet access is by and large slower than immediate link associations, as it uses advances, for example, GPRS, 3g systems and so forth. These systems are normally accessible inside scope of business wireless towers. For taking care of moderate information network, clamping procedures can be connected. Document perfecting method can search for a few assets that encourage smooth stream of versatile figuring.

Connectivity in mobile computing means that mobile is able to connect with the local server for information and data sharing. Due to limited number of resources such as limited battery power, etc. available on a device, it occasionally encounters network disconnection [9]. This disconnection may introduce a security threat not only for the server but also for the device during the time span in which device prepares to connect again. In case of traditional mobile computing, the threat is minor as the external connections are less frequent and usually user authorized so the user is mostly familiar with the environment in which he is connected.

Cloud mobile distributed computing integration alludes to the procedure of associating the versatile to the cloud segment so client can get to the information by sitting at any piece of the world [9]. Versatile clients will most likely be unable to unite with the cloud to get an administration because of activity clogging, system disappointments, and portable sign quality issues. Taking care of remote integration with exceedingly heterogeneous systems to fulfill MCC prerequisites like accessibility, network, on-interest versatility, and vitality proficiency is troublesome.

Usually the network failures occur due to high traffic due to which the user is unable to connect to the cloud. In a technique which facilitates the user to search the nearby nodes over the cloud, the connection can be made to the neighboring nodes instead of the direct connection to the cloud as an alternative.

B. *Authentication*

Authentication is the process of verifying that someone is who they claim, in fact, there are or not. This process is done in mobile and cloud computing through the verification of passwords and logins assigned to a particular person. Authentication process is shown in Fig. 2 below.

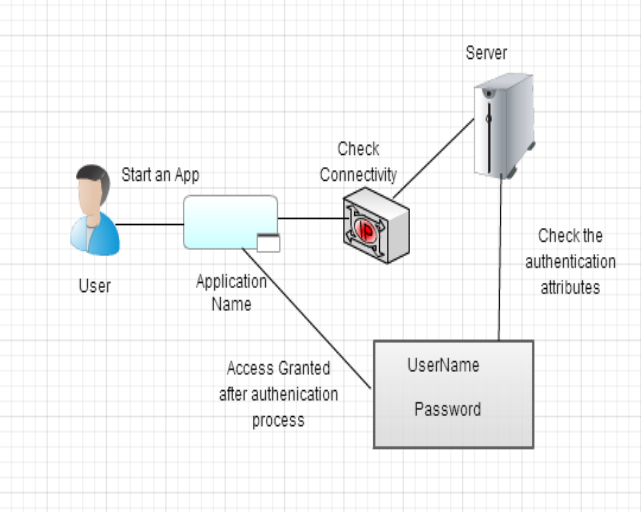
Server
Check Connectivity
Start an App
User
Application Name
Check the authentication attributes
Access Granted after authenication process
UserName
Password

Fig. 2. Authentication process

A wireless network in mobile computing is more susceptible than wired network. There are many possibilities that any kind of intruder can access the mobile communication using a false identity [7]. For example in a large company where confidential data is made accessible to only authorized users and other data is freely accessible to all the users with a mobile computer. So if any person who is not obliged to access the authorized data is trying to access it, here comes the determination of the process of authentication.

In mobile computing the confidential and personal information is kept in our mobiles so whenever we have connected our mobile to the internet then there could be a major security issue in the accessibility of our saved passwords and logins. Encryption key is applied to secure the sensitive data so that only the person knowing the key can access the data.

Distributed computing has been spreading generally, clients and administration a supplier empowers to utilize assets or administrations inexpensively and effortlessly without owning all the assets required [10]. Then again, Cloud Computing has likewise some security issues, for example, confirmation, secret word administration accessibility, application security and so on. Client Authentication among them obliges an abnormal state security.

At the point when a client chooses to utilize different cloud benefits, the client will need to store his watchword in various mists. More client data duplicates will be made for various mists [15]. This is a security issue for the clients and the cloud administration suppliers. The different duplicates of record will prompt numerous confirmation forms. For each cloud benefit, the client needs to trade his/her validation data. This excess activity may prompt an endeavor of the confirmation system. To fathom this issue, Cloud administration suppliers use distinctive verification systems for validating clients.

C. *Information Sharing*

Information sharing is to share your personal information on the websites, some specific links on the internet. Information sharing in a web cluster is shown in Fig. 3 below.

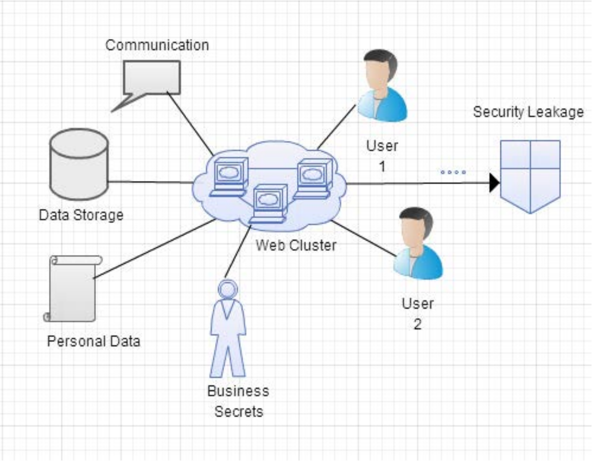

Fig.3. Information sharing

In mobile computing information sharing issue greatly damage your mobile as well as personal security in mobile computing usually user save their passwords and logins to exclude the process of re-entering the information again and again to save their time [8]. But this problem may lead the user to the process of information sharing to the unauthorized users. During the interaction with different mobile users, your information/data can be shared between them or you might lose your personal information as a result of this event.

In Mobile cloud computing it is highly prevented to share your personal information on the cloud. Any attacker can use or access your data and use it for any unpredictable purpose. The security of your data includes security of photos, files and videos related to you [15].

D. *Data Access*

Security identifies with the exposure and pulverization of individual information. Administration suppliers can get to the information and reveal the information to unapproved clients as shown in Fig. 4.

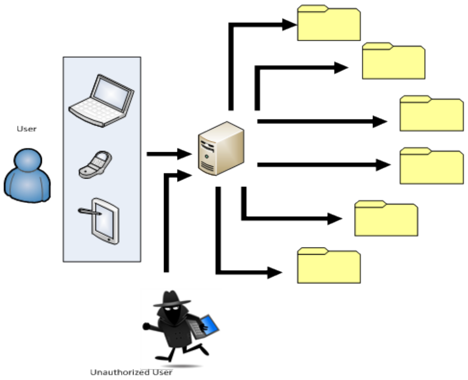

Fig.4. Data access

In versatile registering the cell phone obliges a remote show arrange that is naturally less secure as anybody can see the association, and can get to with pilfered access

Besides, cell phones expand the shot of physical robbery of gadget and data put away on the gadget. In versatile robbery all your information can be spilled out if the other individual has the ability to get to your security coded portable figuring gadget [13]. The merchant must consider that the client individual information is secured from the administrators. He ought to verify that who is getting to the client individual information. On the other way the client ought to likewise be secured about his activities to keep any loss of information from the cell phones.

Privacy is one the biggest challenge in mobile cloud computing. Privacy issue has serious concerns with the data security. In all the applications using cloud computing in their products, user's data is stored remotely. This is the major concern in mobile cloud computing [16] and mobile computing privacy that the company may sell the user data to other company or may use it in an unauthorized way.

Information security in cloud atmosphere includes:

1) Information larceny

2) Isolation of customer delicate data

3) Protection of privacy rights

Decryption and encryption processes are used to make the data private now days. Where as to alert the user about its data privacy loss, many intrusion detection systems are also implemented which alert the user about their personal data privacy loss controls. In respond to data access, if a user stores its data online and completely relies on internet then it would also significantly affect the user and its storage data.

E. Data Loss

Information misfortune prompts the condition in which any sort of data or information is annihilated by disappointments amid transmission or handling of data as the Fig. 5 demonstrate. It's much the same as a plate drive kicks the bucket when its manager has not made its reinforcement record. The possibilities of seeing your significant information vanish into the ether without a follow [6].

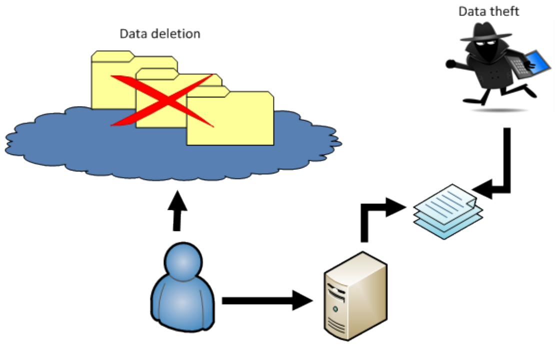

Fig.5. Data loss

A noxious programmer may erase a target's information out of hate however then, you could lose your information to a heedless cloud administration supplier or a debacle, for example, a flame, surge, or seismic tremor. Encoding your information to avert robbery can reinforcement in the event that you lose your encryption key. Information misfortune isn't just tricky regarding affecting associations with clients, the report notes.

In mobile computing all the chief concerns identified in mobile security from data loss to theft, all are related to data leakage. Hacking is a crime involved in the process of data leakage. Data leakage points are:

1) E-mails

2) Stolen mobile or laptops

3) Intruded databases

4) Reuse of backup devices

5) Insecure transmission of data

Data loss is major problem in cloud computing. Although most of the companies are adopting mobile cloud computing features but still due to the data leakage fear they are holding back.

Cloud environment gives asset offering, so it is by all accounts unsafe to move information in hands of cloud supplier. Information in cloud put away in an imparted environment, so it could be hacked effortlessly either because of noxious programmer assault or coincidentally. To handle this issue a sensible information encryption procedure ought to be utilized. Encryption ought to be performed at customer side and client ought to have control over the keys utilized for unscrambling [14].

Cloud suppliers ought to additionally guarantee that the client information has been reinforcement up over the different servers so if there should arise an occurrence of any information spillage the customer has the capacity recover its information whenever. Generally the information spillage happens because of the risk far reaching between the portable clients which are joined with the same cloud.

F. *Data Positioning*

Data positioning is the measurement of the data which is stored on your mobile phone or a cloud server as shown in Fig. 6.

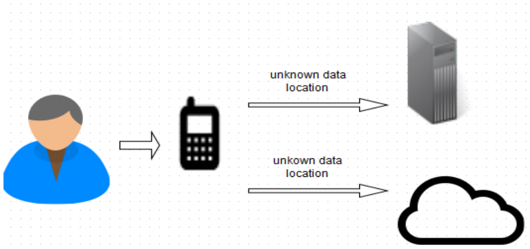

Fig.6. Data positioning

When it comes to positioning of the data in mobile computing nothing is transparent even the customer doesn't know where his own data's are located. The mobility of users and data related is to the presence and location of a user, authenticity of the data exchanged, and the privacy of user profile [5].

Whenever a mobile user connects to the internet, there are the possibilities that the data can be accessed from its mobile phone due to the lack of adequate data positioning. To allow mobility, certain parameters should be made available to the user so that he can access his data safely during roaming. But due to the replication of data at various sites, the points of the attack are also increased on the mobile data.

In the cloud environment, the issue of information an association or organization, wherever spotted is extremely difficult. Shoppers store their information on cloud without knowing where their information is going to be put away. Information territory is of essential as a few clients would prefer not to store their information at the area outside of their nation [15].

For this situation an understanding is marked between the cloud supplier and the buyer who need to store information at a specific area or server. Information area of put away information on cloud is a huge issue from the perspective of customers trust and security of information. Area of information put away in cloud can be prioritized as per clients wish whether the information is delicate or not.

G. *Data Ownership*

Data ownership refers to the responsibility and control of particular information of the data as shown in Fig. 7. A person having the data ownership has the ability to share its data with the other user on the basis of his responsibility.

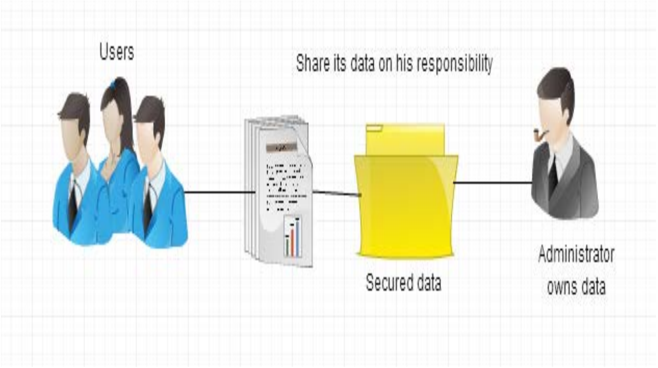

Fig.7. Data ownership

Due to an increase in mobile computing, the issue of data ownership rises. It is difficult to decide which user owns which type of data [3].

An alternate issue that emerges from versatile distributed computing alludes to the responsibility for computerized media. With distributed computing it is conceivable to purchase features, media sound and eBooks on the web. This prompts the responsibility for in versatile distributed computing [2]. Clients ought to comprehend what sort of rights they can profit in regards to the buy of media substance.

H. *Accountability*

Accountability refers to the medium that an entity should accept responsibility for its own actions. Fig. 8 presents a basic accountability approach.

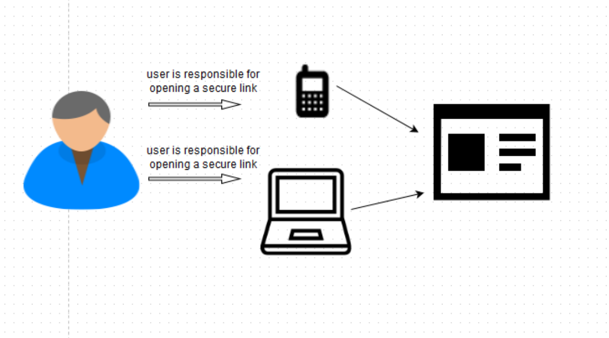
user is responsible for opening a secure link
user is responsible for opening a secure link

Fig.8. User responsibility in accessing web and cloud

In mobile computing accountability issue arises when the user are held responsible for their activities on using mobile devices [4]. They are searching the secure websites, links or not. It's the responsibility of the user to take measure to secure its device from the attackers by applying safe surfing.

In mobile cloud computing, accountability is the lack of consumer trust in cloud service providers when they face different problems after changing the location of their mobile devices [10]. This lack of confidence threatens the organization to choose and implement a secure cloud for their users.

Accountability is all about developing an applied approach to achieve trust and security in the cloud.

4. RESULTS AND DISCUSSIONS

A brief comparison of threat levels in Mobile computing and Mobile Cloud Computing is shown in Table 1 below.

TABLE 1

Mobile Computing Vs. Mobile Cloud Computing

Serial#	**Threat level of security issues in MC Vs. MCC**		
	Security Issue	***MC***	***MCC***
1	Connectivity	Minor	Critical
2	Authentication	Minor	Medium
3	Information sharing	Critical	Critical
4	Data Access	Minor	Critical
5	Data Loss	Critical	Critical
6	Data Positioning	Minor	Critical
7	Data Owership	Minor	Medium

According to the summary shown in Table 1, MCC increased threat level of many security issues for the mobile users such as data access, data positioning. Therefore, the security concerns continued to grow as the vendors launched more devices utilizing cloud based services. Fig. 9 presents the threat levels of both MC and MCC approach from a common user perspective.

References

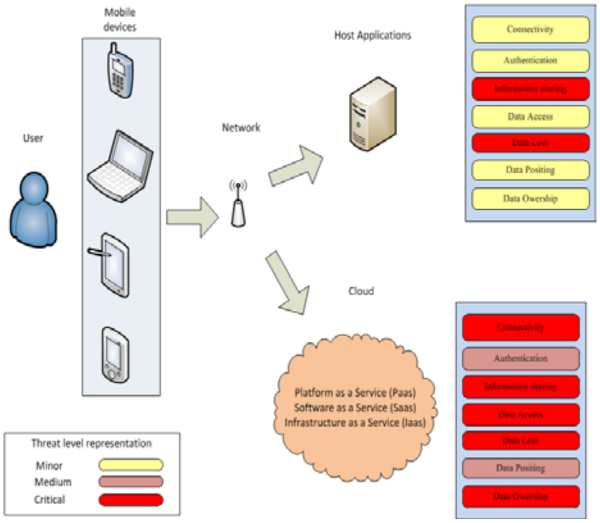

Fig.9. Comparison of security threat levels in MC and MCC

5. CONCLUSION

From the comparison of security issues in MC with MCC presented in this paper, it is clear that as the computation move from local device to the cloud, the security concerns from user side will continue to grow. The reason for these emerging security issues is that more user data is exchanged between the server and user device, thus leading to more vulnerability. Vendors easily accepted the computation shift to the cloud but a continuous resistance has been observed from the users. We compare how the shift from mobile computing to mobile cloud computing affected the threat level of the listed security issues. This domain of security issues still needs attention not only from researchers but also from the vendors to address existing user concerns before moving forward with the new technology trends. Unless the core issues are resolved, the overall computation structure will not be safe enough to gain user trust.

Refernces

[1] Hardjono T, and Jennifer Seberry. Information security issues in mobile computing. 2010.

[2] Ko S-KV, Jung-Hoon Lee, and Sung Woo Kim. Mobile Cloud Computing Security Considerations. Journal of Security Engineering 92. 2012.

[3] Bedre Heeramani BN. Research Dimensions of Advanced Mobile Computing Technology Security Issues for the Complex Applications. International Journal of advanced research in computer science and software engineering. 2013;3(4).

[4] Deepak G DPB. Challenging Issues and Limitations in Mobile Computing. International journal of computer technology and applications. 2012;3.

[5] Ogigau-Neamtiu F. Cloud Computing Security Issues. Journal of Defense Resource Management. 2012;3(2):141-8.

[6] H Khiabani ZS, JL Ab Manan. A Review on Privacy, Security and Trust Issues in Mobile Computing. 2009.

[7] Pullela S. Security Issues in Mobile Computing. 2002.

[8] G. MIaP. Security Issues in a Mobile Computing Paradigm.

[9] A. Cecil Donald SAOaLA. Mobile Cloud Security Issues and Challenges: A Perspective. International Journal of Engineering and Innovative Technology (IJEIT). 2013;3(1).

[10] Soeung-Kon(Victor) Ko J-HLaSWK. Mobile Cloud Computing Security Considerations. Journal of Security Engineering. 2012;9(2).

[11] Khorshed TM, Ali, A.B.M.S. and Wasimi, S.A. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation Computer Systems. 2012;28:833-51.

[12] Teneyuca D. Internet cloud security: The illusion of inclusion. Information Security Technical Report. 2011;16:102-7.

[13] Abid Shahzad MH. Security Issus and Challenges of Mobile Computing. Internatinal journal of grid and distributed computing. 2013;6.

[14] F.S. Gharehchopogh SH. Security Challenges in Cloud Computing with More Emphasis on Trust and Privacy. International Journal of Scientific & Technology Research. 2012;1(6):49-54.

[15] P. Gupta SG. Mobile Cloud Computing: The Future of Cloud. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. 2012;1:134-45.

[16] D.Popa KB, M.Cremene, M.Borda. Overview on Mobile Cloud Computing Security issues. 2013.

[17] Bal, G¨okhan. “Revealing Privacy-Impacting Behavior Patterns of Smartphone Applications”. Goethe University Frankfurt, Germany, April 2012.