RESEARCH ON MOBILE CLOUD COMPUTING CHALLENGES, SECURITY ISSUES AND EFFECTIVENESS ON SMART DEVICES

Muhammad Aater Javed, Akmal Rehan, Samiullah
Department of Computer Science, University of Agriculture Faisalabad.
Corresponding Author E-mail: maaterjaved@gcuf.edu.pk

ABSTRACT: *Mobile cloud computing provides cloud services to mobile devices using wireless networks. In this research an examination activity in the region of mobile cloud computing has been conducted which highlighted different open issues and challenges in it. In mobile cloud computing security remains utmost important factor for moving data to the cloud. The main objective of this research has been to investigate mobile cloud computing challenges especially security issues and different effects on smart devices, which helped general readers and is helpful in the future for related implementation in mobile device. The working concepts of mobile cloud computing and its various security issues and challenges have been analyzed in different scenarios by using simulation. The primary goal was the impact of cloud computing on smart devices and comprehend the idea of cloud computing which proved that mobile cloud computing made the smart devices more efficient.*

Keywords: Smart Devices, Universal Mobile telecommunication System, Mobile Cloud Computing (MCC), Mobile Cloud Computing Challenges, Mobile Cloud Computing Security issues.

INTRODUCTION

For providing the user with fast and more reliable execution of the programs and application and keeping its data secure and accessible from anywhere at any time a new technique named mobile cloud computing is being used that is a mixture of the mobile devices, cloud computing and wireless networking. Providing more execution and computing power to users of the mobile devices for better experience is the main concern of mobile cloud computing.

By using simple internet, wireless network or the Ethernet and avoiding the heterogeneity issues mobile cloud computing is a very flexible approach that provides services to a large number of the mobile clients with the offer of that you have to pay when you use the paid services which in turns categorized the mobile cloud computing as a flexible processing revolution that greatly signifies the mobile device [1]. To utilize the advantages of the mcc there is no need to develop a lot of settings and wasting a lot of money in designing some new system for them, in fact it only needs to connection to the mcc [2]. The architecture of the mobile cloud computing is not much different than the architecture of the simple cloud computing only the mobile nodes are included in it [3]. Mobile cloud computing is simple advancement in cloud computing [4].

The explanation behind the theory is to scrutinize the substantiality of mobile cloud computing in the area of smart devices applications. The inside lies on how mobile cloud computing can enhance smart devices computational execution and usability, including parts of limitations and drawbacks concerning the building being alluded to. Since computational limit of smart devices are restricted and on the grounds that mobile cloud computing could be an answer for enhance the said territory, the accompanying examination inquiries are researched. For this purpose different scenarios are made using the simulation in OPNET MODELER to check are smart devices with cloud based environment works more rapidly as compare to those devices without cloud environment in similar task?

MOBILE CLOUD COMPUTING CHALLENGES

Many challenges that provider and the users of the mobile cloud computing faces are as follow.

In mobile cloud computing whenever any of the users require any resource it would be automatically allocated to it also that allocation must be observed and immediately after completing the task that resource must be released from that user so that it would be vacant for any upcoming requirement. The major hazard in mobile cloud computing is the use of the resources; they all utilized the same shared resources. Occupying the same resource by multiple users at the same time is of very much worry for the users and made them confused and fearful of their personal and confidential data might be handover to some other processor because the same hardware is being used by other users also. Using the shared resources enhances the chances of these fears that some unauthorized user may get into your data and can misuse it.

There is also a challenge of the surety that the entire user's personal information is encrypted and that encryption key is not shared with anyone. Data is the most important asset for all the users and they can never compromise with the leakage, loss or corrupted so it's a big challenge for manage their data and make the storage area secure as well as use advanced storage techniques.

Energy management is also one of the major challenge regarding the mobile cloud computing. Big servers contain huge amount of users data requires big amount of energy also the user can access their data at any time so the energy supply must be uninterruptable.

The most important and the most difficult challenge for the providers of mobile cloud computing is to deal with the heterogeneous nodes. Users of the mobile cloud computing can be heterogeneous, they can be of different brands containing different hardware components and also different software models, their mode of data transmission can be different and might operate different OS. Bandwidth management is also a big challenge for the mobile cloud computing suppliers because of the varying nature of the data and the network architecture. It might be possible that a mobile node is more fast then the connection between the cloud and that node because of the low bandwidth which in turns affects the overall performance of the system.

MOBILE CLOUD COMPUTING SECURITY ISSUES

There is a huge number of security issues are present in mobile cloud environment. Because the clouds are open by nature at different locations the user doesn't have control on their data. The users have no control to see what is happening in the database and all operations in it. Security is always very important for the client and if any of the cloud suppliers failed to provide the security this is a serious security threat. Data stored on the cloud can be sniffed by some 3rd party software also chances are there that the data that is stored in the cloud may be accessed by some hacker and they misuse it. To avoid such situation authentication must be required to get access to data [5]. Most the information of the cloud user is confidential and they never want it to leak out and hope that their privacy is in the trustworthy hands [6]. There is possibility that the sites where the data is stored came under attack and became irresponsible, making user to have no access to their data when it is need. Or that site might completely shut down making user loss all its data. Denial of service is example of such situation. This is also a security risk that the encryption / decryption keys are shared among whom. Do they are in safe hands. Also this is a fear that the providers of the cloud service share the confidential data among different providers breaching the confidentiality of the user. And they may use it for some illegal activity. There is possibility that the site goes down and all the

MATERIALS AND METHODS

For testing the effectiveness of the mobile cloud computing a scenario based study has been held by using mobile devices that are connected to the mobile clouds with Gateway GPRS support node in universal mobile telecommunication. Nodes in UMTS have high speed of communication and are able to communicate in different environment [7]. For this research, network simulator OPNET MODELER has been used to test cloud computing performance. OPNET MODELER is very flexible in its functionality but it's not open source just like NS2 [8]. Different applications (cloud based and Non-cloud based) have been run; their performance is measured and compared. Examination of cloud security is measured by making different scenarios with and without security measures and both results are compared. A firewall used as a security measure for the mobile cloud computing and acts as screening object [9]. Load on the processor, ram and battery is recorded. And then different cloud based applications are executed and the parameters are recorded. After that these parameters are compared and best method is highlighted.

SIMPLE MOBILE CLOUD COMPUTING

The principle goal of this situation is to force no security measure conditions over the system. Two unique applications are made over this situation, one is the database application and the other is the web application. Fig.1 demonstrates essential workplace in OPNET MODELER also mandatory recreations prepared here

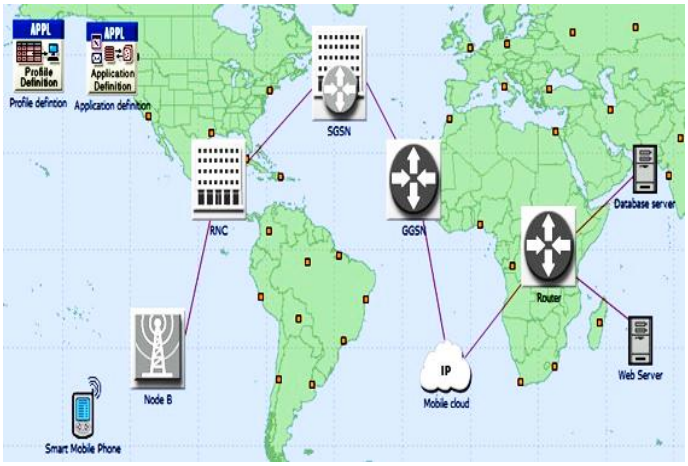

Fig.1 Network setup

Cloud is used for providing services to mobile devices in this simulation and these devices can utilize both the database and web servers. No security measures are taken here and the performance of the cloud is measured. Taking after are the execution measurements utilized for the execution assessment of cloud when there is no security measures are taken.

HTTP page reaction period evaluated for web applications and database inquiry spell and reaction period regarding database applications is evaluated. End point measurements such as dB-server inquiry reaction period as well as burden are likewise evaluated regarding database applications.

MOBILE CLOUD COMPUTING UNDER ATTACK

After making the situation with no security measures for mobile cloud computing the same project is copied to modify and an attacker is added to situation as in Fig.2. For making specific situation an attacker is made with steady packet latency of .05 sec is forced for data transmission. Comparable execution measurements are utilized as a part of the main situation

MOBILE CLOUD COMPUTING WITH FIREWALL

For making the situation to block the attacker's access the previous project is copied with the need to block all the unauthorized access to the servers from the attacker that is a serious threat to the mobile cloud computing as seen in Fig.3. The firewall can be utilized here for authenticating the users and allowing only the mobile cloud users to pass through it [10].

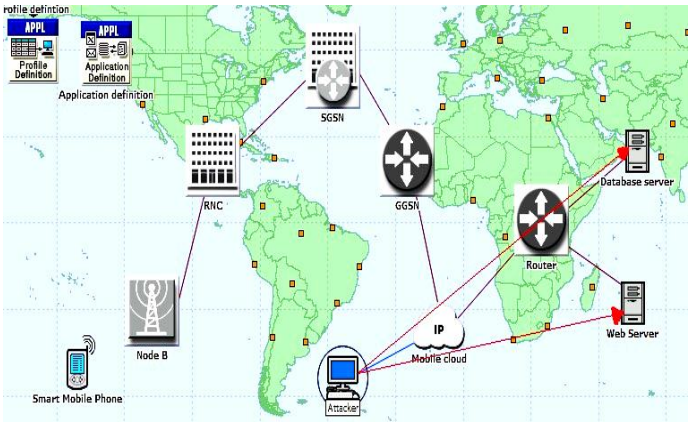

Fig.2 Attacker breaching cloud security

The attacker attacks the cloud that provides services from the database and the webserver, making it un-respondent to the mobile device that is requesting for the services. In this way the mobile users became unable to utilize any services offered by the mobile cloud computing providers. When all the work is done same statics as the previous scenarios are made for making comparison at last.

Fig.3 Firewall design

RESULT AND DISCUSSION

When done with all above scenarios these scenarios are executed for a specific amount of time to record different performances in these different environments then these are compared.

WEB TRAFFIC RECEIVED

Fig.4 showing the response of the web traffic received over a period of sixty minutes. These results are same for all the three scenarios (Simple mobile cloud computing, Mobile cloud computing under attack and mobile cloud computing with firewall). In this figure the blue curves are showing the response of the web traffic received in the first scenario simple cloud computing. The red curves are showing the response of web traffic received for mobile cloud computing when it is under attack. And in the last the green curves are showing the response of the web traffic received in mobile cloud computing with firewall used.

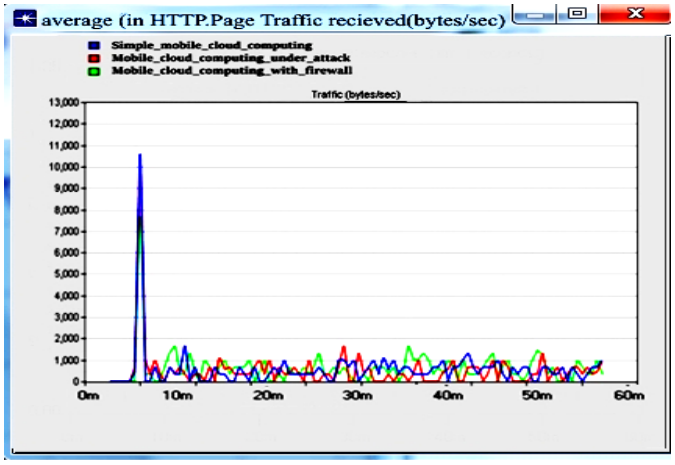

Fig.4 Web traffic received

Traffic received at mobile nodes at the begging is very high then it is decreased and the less traffic is received in all the three scenarios. Means the web performance is almost same in all three scenarios.

THE ACTUAL PERFORMANCE OF THE CLOUD

For analyzing the cloud performance point to point utilization is observed and the results are evaluated this with different point of views. The fig.5 is indicating that in the scenario in which an attacker is involved in the mobile cloud computing the attacker is disturbing the overall normal functions of the cloud as well as affecting the point to pint utilization of the cloud making it busier. The attacker in this scenario is an unauthorized user who is enters in the network and now it's disturbing the normal functionalities of mobile cloud.

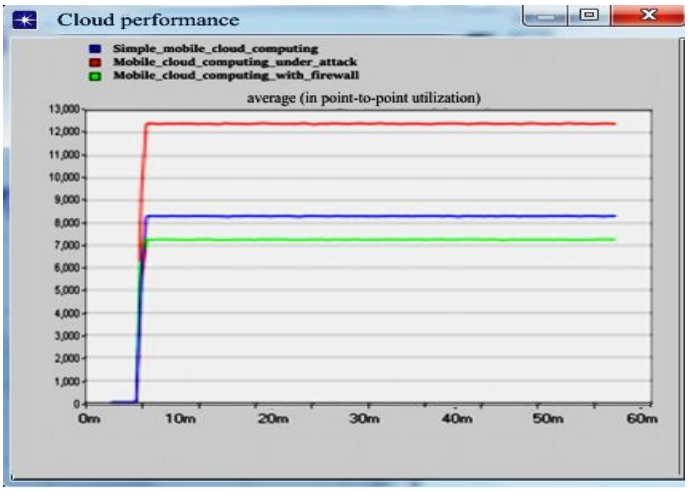

Fig.5 Cloud performance

In the case of simple mobile cloud computing the utilization of the cloud is less than the scenario with the attacker. The utilization is less because in this scenario only the traffic from the mobile devices is passed through the cloud and only the authenticated mobile users utilized the cloud. That makes a smooth running of the scenario. But what is some attacker got access to the network; in that case the performance of the cloud can go down as discussed above in the case of attacker attacking with dummy packets.

In the last scenario the utilization of the cloud is less than all the two other scenarios. This is because the use of the firewall as a screening agent who automatically blocks the unauthorized access to the cloud in this way making the attacker's attacks went empty. In this way the firewall is providing a smooth execution environment and the utilization of the cloud to the mobile users.

SMART MOBILE PHONE PERFORMANCE

Node level statistics the CPU utilization is selected for both the scenario in which the smart mobile phone is used as an alone device without getting any service from the cloud for this the same first scenario simple mobile cloud computing is used but the mobile's connection to the cloud computing is removed. In the second case the same simple cloud computing environment is used and the performance of result of the CPU utilization is recorded and analyzed as shown in the fig.6.

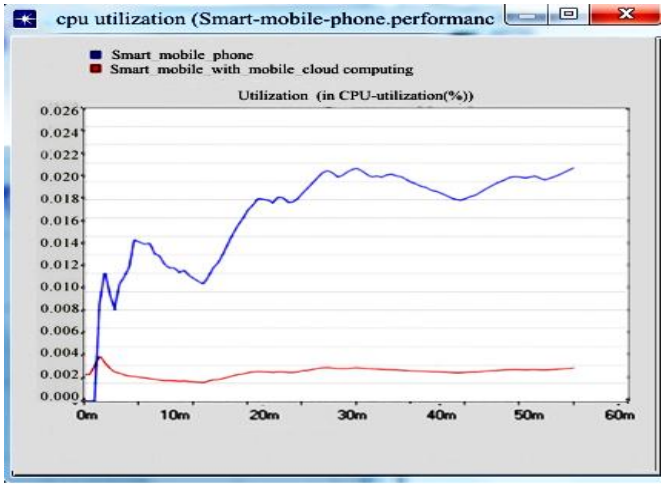

Fig.6 CPU Utilization for smart phone

As it seems the CPU utilization is less in the begging, but gradually it increased with passing the time for the smart mobile phone. The blue curves in the fig.6 is showing the utilization of the smart phone's CPU that is too much as compared to the other scenario in which the services of the mobile cloud computing are utilized.

The red curve is indicating the utilization of the CPU for the same smart phone devices. The only difference is that the smart mobile is utilizing the services of the mobile cloud computing. In this way all the processing is made on the cloud converting the entire burden to the servers on the cloud and making the smart mobile more efficient and light. In Fig.6 the red line is increased for a very short period in the begging of the simulation. This is because in the beginning the CPU of the smart device is utilized a little before the burden was shifted to the cloud. As the traffic is shifted to the cloud the CPU utilization of the smart mobile device is again fell down and remains at the possible minimum value. This is because the background applications are running in the smart phone as its operating system and other system applications.

As it seems the CPU utilization is less in the begging, but gradually it increased by passing the time for the smart mobile phone. The blue curves in the fig.6 is showing the utilization of the smart phone's CPU that is too much as compared to the other scenario in which the services of the mobile cloud computing are utilized.

The red curve is indicating the utilization of the CPU for the same smart phone devices. The only difference is that the smart mobile is utilizing the services of the mobile cloud computing. In this way all the processing is done on the cloud converting the entire burden to the servers on the cloud and making the smart mobile more efficient and light. In Fig.6 the red line is increased for very short period in the begging of the simulation. This is because in the beginning the CPU of the smart device is utilized a little before the burden was shifted to the cloud. As the traffic is shifted to the cloud the CPU utilization of the smart mobile device is again fell down and remains at the possible minimum value. This is because the background applications are running in the smart phone as its operating system and other system applications.

CONCLUSION

For all this investigation different scenarios are evaluated and after analyzing all of them, I concluded that smart mobile devices are greatly affected by the use of the mobile cloud computing in a positive way. When talking about the efficiency of the smart mobile phone devices it is increased as it is proved when the performance of the CPU of the mobile device is evaluated with and without the use of mobile cloud computing and it is concluded that the performance of the CPU is best when utilizing the services provided by the mobile cloud computing and by shifting all the mobile's CPU load to the server, that in turns makes the CPU in the mobile device vacant. Also power consumption is less in that case. When less power is used by the CPU the battery life time is also increased.

As a contrast in the other scenario the mobile phone's CPU was being utilized with almost full potential and making the mobile device inefficient and slow. Also the battery power consumption is very high.

By using the mobile cloud computing services user's data is stored to the cloud storage rather than the phone storage which solved the storage issues. But still there are some issue related to storage like security and confidentiality issues which needs the attention of researchers.

When results of the all the three scenarios above are compared the cloud utilization in mobile cloud computing was most when that attacker attack at the cloud and in turns makes the other traffic from the mobile to block. In this way the no service is provided to the mobile device's users. This is a big issue. The utilization of cloud for the simple mobile cloud computing was moderate and the cloud utilization in the firewall scenario was minimum. This is because the firewall blocked all the fake traffic coming from the attackers.

At the end it is concluded that the mobile cloud computing is a beneficial option for the smart mobile phone users but still there is some area where the improvement is needed, the most important of them is the security issues and different challenges related to it.

REFERENCES

[1] Pooja, N. D and P. L. Ramteke. Mobile Cloud Computing. *International Journal of Science and Research*, **4**(1): 2072-2075 (2011)

[2] Guan, L., X. Ke, M. Song and J. Song. A survey of research on mobile cloud computing. *Proceedings of the 2011 10th IEEE/ACIS International Conference on Computer and Information Science IEEE*, **10**(1):387-392 (2011)

[3] Fernando, N., S. Loke and W. Rahayu. Mobile cloud computing A survey. *Future Generation Computer Systems*, **29**(1): 84-106 (2013)

[4] Rahimi, M., J. Ren, C. Liu, A. Vasilakos, and N. Venkatasubramanian. Mobile cloud computing A survey, state of art and future directions. *Mobile Networks and Applications*, **19**(2):133-143 (2014)

[5] Kundu, A. Authentication of Data on Devices. Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on, **1**(1):236-242 (2012)

[6] Simoens, P., F. Turck, B. Dhoedt, and P. Demeester. Remote display solutions for mobile cloud computing. IEEE Internet Computing, **13**(5):46-53 (2009)

[7] Rawal, C. and M. Sharma. Implementation of soft handover in 3G using OPNET. *Optimization, Reliabilty, and Information Technology (ICROIT), 2014 International Conference*. **20**(14): 208-211 (2014)

[8] Lucio, G., M. Paredes, E. Jammeh, M. Fleury and J. Reed. Opnet modeler and ns-2: Comparing the accuracy of network simulators for packet-level analysis using a network testbed. WSEAS Transactions on Computers, **2**(3):700-707 (2003)

[9] Ioannidis, S., A, Keromytis, S. Bellovinand J. Smith. *Implementing a distributed firewall. Proceedings of the 7th ACM conference on Computer and communications security*, **2**(1):190-199 (2010)

[10] Wool, A. A quantitative study of firewall configuration errors. *Computer*, **37**(6):62-67 (2004)