Mobile Cloud Computing Security as a Service using Android

Bhavya Sareen
Department of CSE
CGC, Gharuan
Chandigarh, India

Sugandha Sharma
Department of CSE
CGC, Gharuan
Chandigarh, India

Mayank Arora
Department of CSE
CCET, Panjab University
Chandigarh, India

ABSTRACT
Cloud Computing is from one of the most prominent technologies that are used today. A lot of business is growing using the computational resources on pay per use model. As more and more enterprise applications are shifting to mobile these days security becomes a big issue to be answered. This paper will give a review for how mobile cloud computing is getting in an upper edge. The security concerns are shown in this paper and an security mechanism is proposed which will secure the data on the Smartphone's using the computation of the cloud..

General Terms
Cloud security

Keywords
Cloud Computing, Mobile Cloud Computing, Computation Offloading, Security.

1. INTRODUCTION
Cloud computing is a new way through which we can integrate the technologies we need and create a paradigm which provides on demand services to the users, Through the uses of Cloud Computing user could get the exact amount of computing they need in a pay per use model. Like Amazon EC2 and Google. Cloud computing promises to cut operational and capital costs and let IT departments focus on strategic projects instead to keeping any datacenter running. Benefits of Cloud for new IT companies. Now move on to the mobile cloud computing front the market of Smartphones is increasing day by day according to the IDC a global market intelligence firm the worldwide Smartphone market grew 51.3% in the first quarter of 2013 . China and India are the top 2 ranked countries show the highest usage of Smartphone's. Mobile Cloud Computing is the assemblage of resource rich Cloud with the smartphone through various networks to mobile distributed computing paradigms which have three Heterogeneous of mobile computing. Cloud computing and wireless networks are enhancing the computation capabilities of resource constrained mobile devices to maintain rich user experience

2. BASICS OF CLOUD COMPUTING
Cloud computing is a type of computing that relies on *sharing computing resources* rather than having Local servers or personal devices to handle applications. In the word cloud computing "cloud" is used as a metaphor for "the internet". The phrase *cloud computing* means "a type of Internet-based computing," where different services – such as servers, storage and applications – are delivered to an organization's computers and devices through the Internet.

2.1 Characteristics of Cloud Computing
Cloud computing have five essential characteristics defined by NIST (National Institute of Standard And Technology) [1].

1. On demand self service : A consumer can take the services such as network storage And server time etc as needed automatically. Over the Internet.

2. Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms. Throughout the world.

3. Resource pooling: A pool of resources is present from which resources are allocated and deallocated resources to the user according to their demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction.

4. Rapid elasticity: Capabilities should be provisioned rapidly and elastically. That consumer can take whenever needed by them.

5. Measured service: Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

2. 2 Service Models

1. Software as a Service: This service provides application as a service to the user to run on the cloud infrastructure. The user does not have the Control of cloud infrastructure like network, servers and Operating systems.

2. Platform as a Service: This service provides computing platform for the application and creates an environment for the application which gives programming language, libraries, services and tools. The user does not have the control over the network Storage and operating system but has the control on the deployed application and the configuration settings for the application hosting environment.

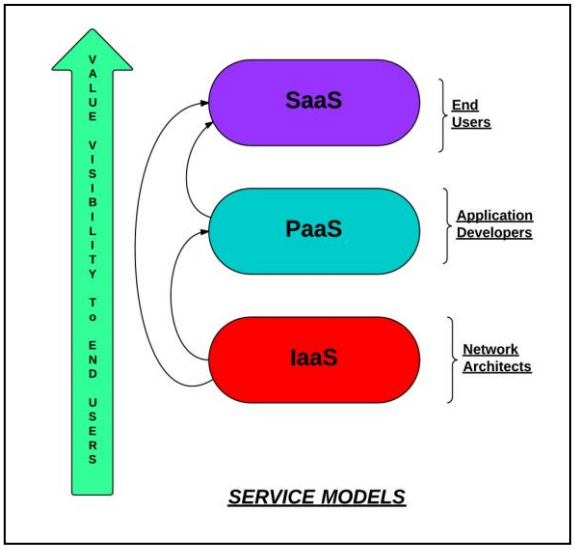

Figure 1. Service Models

3. Infrastructure as a Service: This service gives provision to the user to get control over the processing ,network, storage and other computing resources where consumer can able to deploy and run the arbitrary software which can include operating system and application .

2.3 Deployment Models

1. Private Cloud: The cloud infrastructure is provisioned by the single organization which has all the control to operate it and that company may have multiple users and it may be managed by a single organization which keeps all the information confidential and exists on the premises of that single organization only

2. Public Cloud: The cloud infrastructure is provisioned for open use by general public .It May be owned managed by some business, academic or government organization .it exist on the premises of the cloud provider.

3. Hybrid Cloud: This cloud is the combination of both private and public cloud where an organization owns the Cloud and the Cloud is deployed in its premises .A part of the Cloud is dedicated for the organization .Private usage and some is open for general public.

4. Community Cloud: The cloud infrastructure is provisioned by the specific community of users from the organizations of similar type It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off Premises.

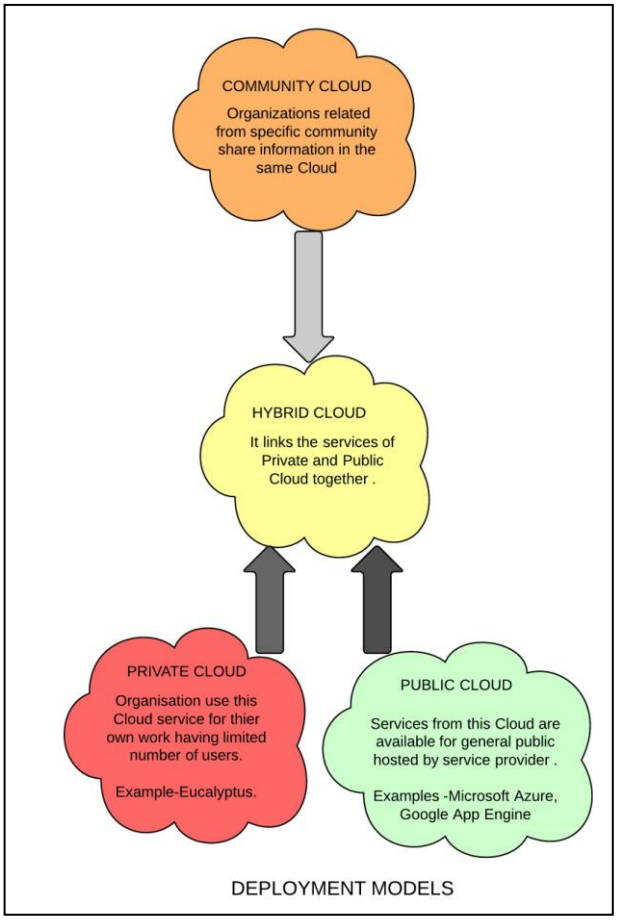

Figure 2. Deployment Models

3. MOBILE CLOUD COMPUTING

Use of Smartphones is increasing to such extent as they provide all facilities which laptop does. Users prefer using Smartphone's and tablets instead of laptops. A report from Cisco shows that the traffic from mobile devices will lead to get 60 percent of the total global IP traffic by 2016. Some of the applications related to image processing .natural language processing are compute intensive, which need resources i.e. larger memory as well as more processing power which results in exhausting the battery of smartphones, limiting the usage of such application by the users. [2] describes an architecture on how mobile cloud computing works .Mobile Cloud Computing is used where all the resources are provided by the cloud it takes the data from mobile device and process it with its resources, stores the result which is then given back to mobile devices, saving the resources of mobile devices and its battery.[16,17] have all the clear idea about resource rich Cloud Computing which helps mobile device to transfer the data and processing on to the Cloud which constitutes storage, server, processing power , software . Besides this security is also important to be maintained in this model [3] explains the five reasons in which care is to be for Mobile Cloud Computing. [4] Describes the future of mobile cloud computing, where It is beneficial and a detail for which is explained in [5] future scope of Mobile Cloud Computing. [6] discussed the security issues takes place in the Cloud premises which is taken into consideration for the proposed Architecture.

4. RELATED WORK

Mobile cloud computing contains two factors by the combination of which this model works mobile network and cloud computing. Through the mobile network all the data or computation is being transferred to the cloud. And cloud stores that data in its storage and if any computation task arrives which smartphones is not capable of executing due to lack of battery power and resources in mobile phones then it is transferred to resourceful cloud which does the execution.[19] consider the problem with the traditional smartphone application which are not capable to be compatible with the Cloud features and offloading is also not supported by these application so for compute intensive problem the Mobile Cloud architecture is defined which helps to identify offloading decisions entities and the application model for Mobile Cloud. Security is also an essential measure to keep in mind as all the storage and computation work is shifting on the Cloud. Thus concerning the privacy of an individual and an organization subscribing Mobile Cloud computing. [11] describes a framework where offloading is done by the application on the cloud which have unlimited resources to use and complete the work in less time as possible .[13] computational offloading survey is shown to best describe this process .As per the trend all the work is being shifted on the mobile devices which are able to provide all the facilities which laptops and personal computer provide. And the mobile devices are having an advantage over them as they are easy to carry and portable, but through this growth in usage of mobile device for all the confidential work the liabilities will also come. Situations may arise where the confidential data may get leaked or compromised if the phone got lost, thus making the mobile device highly vulnerable. Moreover, these are other security issues in context with the Cloud as the Cloud is being used for storage and computations [7] Gartner defined seven cloud computing security risks which an organization should address before getting switched to a cloud computing model.

The seven Security Issues are:-

1. Perquisite User Access – User should spend time to know all about the providers from which it is seeking to get services and emphasis on their regulations before assigning some trivial applications.
2. Regulatory Compliance – Users are accountable for security of their data as they can choose between service providers that allow audits by third party organization that checks the security level and service providers that do not.
3. Data Location – Certain contracts are made by the service providers according to which user will get no right or idea of where their data is kept in which country or under which jurisdiction.
4. Data Segregation – The information from the various organizations may be stored in the same hard disk which is in encrypted form mechanism to segregates data should be employed.
5. Recovery – Providers should have some disaster recovery mechanism to keep the user data safe and recoverable.
6. Investigative Support – If the user sense any faulty activity from the service provider side it should not take long time to start the investigation process.
7. Long Term Viability –Service provider should give long term viability as if they went out of business or bought by another organization. The user's data should be retracted to them safely.

In[8] Lakshmi Subramanian et al. shows the security aspects of the smartphones how they can get infected thorough infection channels like Bluetooth ,Sms and internet and what are the threats that lead smartphones to leak all the confidential information and then the Security functions to secure the information .on the basis of which an architecture is proposed which reflect the malware to reach towards smartphone by doing scanning through antivirus on cloud only which also reduces the power consumption of smartphone as all the scanning work will be done on cloud for all the applications and data sending or receiving done on smartphone. [9] A mobile cloud data processing framework is described which contains three components : Trust management gives control to the user to access data by authenticating the identity of the individual ,Multi-tenant secure data management manages the data in two form one is normal data which is secured by the cloud data encrypting key generated by the cloud storage service provider and another is critical data secured by the key generated by user only and ESSI data Processing model show the data flow and then the normal data is sent to the public cloud storage directly but critical data is kept in the secure storage .[15]shows the augmented execution for smartphones by the help of CloneCloud architecture which means holding a clone of smartphone over cloud . [14] shows the work done where they define the smartphone gives pc like experience and to enhance this experience and an virtual image of the smartphone is created over the mobile cloud and user can use it to store data and do computation which will save the resources and processing time of the smartphone.

5. SECURITY ISSUES

In this area of mobile cloud computing security issues arises in two different parts one belongs to mobile phones and mobile network security and another is security on Cloud i.e. cloud security.

Mobile Phone and Mobile Network Security:-

Mobile phones have applications which can get malicious attack and reveal all the data stored through them in the mobile device and that kind of malware can come from the internet through mobile network. So to protect mobile device from these attacks antivirus are provided which scans all the application and data stored in phone to check the any kind of malware present but the drawback here is shortage of resources and excessive consumption of power which reduces the battery of smartphones only by running antivirus scan as all resources gets busy in doing the scanning task which led to the low battery situation.

Cloud Based Security Issues:-

Cloud provides storage and computation and the data stored on the cloud needs security. [13] Describe the cloud security front in three main points. First is to keep the information stored in the cloud secure which means the data stored by user could not be accessed by the third party .so for that the data is stored in encrypted form on the cloud but that data is also known to the cloud provider in an unencrypted form as encryption is performed by the cloud providers only so they should be trustworthy

Second is the execution of the desirable code which doesn't contain any virus or malware in the code only that code should be executed sometimes at the time of development of the code some malicious content can be introduced. So for that software must be revalidated to maintain assured validity. Problem arises when stream of executables is introduced which can quickly spread malicious payload on cloud computing environment.

Third is the information stored and services provided by the cloud to the user should always be available when needed. For the replication of data is done which lead to issues of data management to ensure consistency. And every time the services are updated can lead to inconsistency or failure. If an older service is used when the newer one is available to that.

In [18] user authentication is done through profiling technique when user requests for the access control. Authentication is not provided by specifying the Id/Password and then on the basis of OTP because this can also be now fetched by hackers through key logging attack or SSL strip attack.

Securing Information on Mobile Cloud –
The cloud security mechanisms can be used to enhance the security of the mobile device which is cloud based secure proxy and remote antivirus etc. Remote antivirus does all the scanning for mobile device on the cloud and protect device to get infected from any malware attack. To store the information on the Cloud and ensuring the security of the Information the following three factors should be kept under consideration:-

1. Integrity: The information stored on the cloud by the user through mobile device should be integrated. User should know where the information is kept and who can access it and every access should be authorized so no leakage of the confidential information can be done.

2. Authentication: Authorized access Is the main issue when mobile client access the information stored on Cloud every access should be authenticated so that user can access information related to them only no unauthorized access should be permitted and this is done by several authentication mechanisms like giving login ids passwords, pins To individual user to verify their identity which permits them to get access to their data securely.

3. Digital rights management: Digital media are getting pirated easily because of their presence on Cloud openly. Media like videos, images, audio and eBooks are illegally accessed so they should be kept in encrypted form so that no piracy of the individual media important to the user can get viral on internet illegally.

6. PROPOSED ARCHITECURE

According to a recent survey only 17% of Enterprise applications are on mobile today. Till 2015 98% Enterprise applications will be on mobile. As more and more applications are becoming mobile the need for securing the data and making use of the resources of the cloud is increasing. It has been showed in another survey that the top 10 reasons of data leakage for an enterprise constitute the loss of a mobile phone resulting in data leakage. It is proposed that this problem could be solved if the data is not kept on the mobile phone.

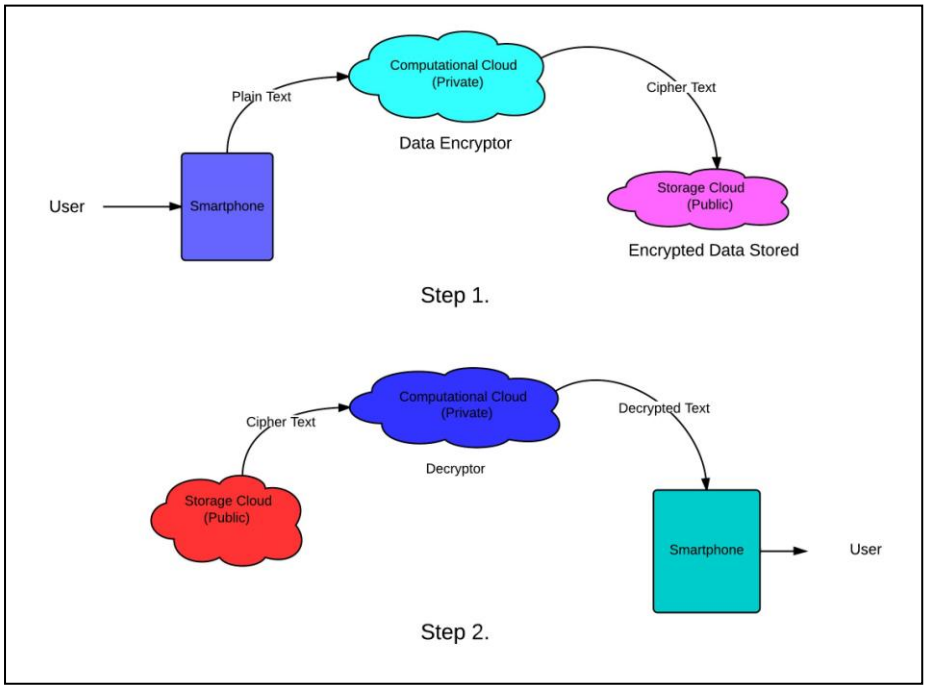

Figure 3. Security Architecture for Smartphone

Instead the data needs to be stored on the Cloud storage which is more secure and the data could be accessed from anywhere. The only issue that needs to be answered is the Trust issue. It is proposed that if the following architecture is used the trust issue for storing sensitive information to a public cloud will be gone.

The architecture providing the solution to the above described issues is explained as follows. As shown in above Fig.3 it is proposed that if the data is encrypted before sending it to the storage cloud the data will be of no use of the cloud service providers.

It is proposed that the data being stored to the cloud will be encrypted using a computational cloud before storing the data to the cloud storage. By doing this the data being stored will not be plain text data i.e. won't be in readable format but will be cipher text which will be of no use for anyone except the one having the decryption key. As shown in the figure the data originates from the Smartphone, but is indented to be stored in the cloud storage. To ensure that the data is not compromised or misused the data needs to be encrypted. The Encryption could be done on the phone itself but it will result in resource exhaustion. As the Smartphone's have limited memory and processing power the encryption will be an extra overhead. The solution to this problem is that the compute intensive encryption process be offloaded to the cloud i.e. a computation cloud could be used to encrypt the plain text into cipher text. The computational cloud will not be able to misuse the data because we will make an application for encryption and deploy it on the cloud leaving no point where the data could be compromised. When the data will be needed again it will be decrypted in the same format i.e. on the computational cloud.

An application is designed based on the proposed architecture to encrypt text and image using AES. An AES Encryption and decryption application is also made for the Smartphone to measure the time taken for encryption and decryption of the text as well as image on the Smartphone and cloud hypervisor. This is done to show the speedup in the encryption/decryption using the proposed scheme. Thus making the data on the Smartphone secure will not cost much to the user in terms of energy and time by using the Cloud as a computational backup. Table I shows the results obtained by encrypting the text and image both on the Smartphone and cloud hypervisor which will do the comparison between the mobile device and virtual machine and the availability of resources will help to execute these operation by taking less time .

As it could be seen while encrypting a single word i.e. the first case almost 17x speedup is achieved. In case of an image i.e. the case 4 almost 20x speedup is achieved while encrypting an image of 600kb. As the size of data will increase, it would become difficult for the phone to encrypt such huge amount of data. Such process will eat up the battery of the smartphone. In the above table while the image was being encrypted for almost 8 seconds the smartphone was not responding while encrypting as the processor was utilized by the encryption process. Using this mechanism makes the smartphone more responsive to the user's demands making it much more suitable to the user using the smartphone for work i.e. running the enterprise applications.

Table I. Shows the Results Obtained Through Encryption Done Over Smartphone And Virtual Machine.

Text And Image	Time Taken For Encryption in virtual machine (in millisecs)	Time Taken For Encryption in smartphone (in millisecs)
1. Hello	1	17
2.1234-2345-3456-4567-5678-6789-6790-1235-1267.	6	36
3. Portability storage space and battery life are the main characteristics of smartphone's .	11	56
4. Image a1.jpg	498	8643

After encrypting the text and image decryption is performed to check the time taken by the smartphone and cloud hypervisor individually for decryption. Hence concludes the comparison of both. As it could be seen the decryption process is taking much less time than the encryption process the speedup is also not as good as the encryption process. Hence concludes the comparison of both. As it could be seen the decryption process is taking much less time than the encryption process the speedup is also not as good as the encryption process. It is seen that the more compute intensive the problem the more is the benefit of offloading it to the Cloud. A maximum of 7x and a minimum of 3x speedup is achieved in case of decryption. Yet offloading it will make a significant change in the smartphone's battery life and the smatphone's performance.

Figure 4 here shows the results obtained where it can be seen that it will take a lot of time to encrypt an image on Smartphone and virtual device as the size of data increases the time taken also increases. But here the benefit is that it will take less time on the virtual machine than Smartphone to perform encryption on the data.

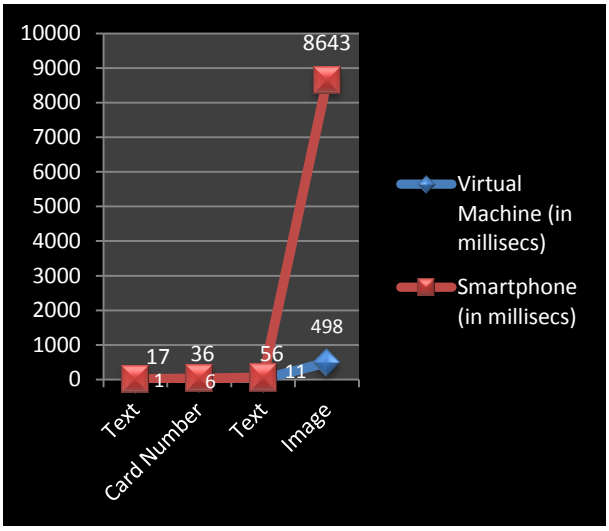

Figure 4. Time taken for Encryption by Virtual Machine and Smartphone

Both the Table I and Table II shows the comparison of time taken in encrypting and decrypting the data on Smartphone and cloud Results shows that it will take less time to do both the operations when done on cloud as compared to Smartphone as it lacks the resource power and takes more time to perform the encryption and decryption on it.

Table II. Shows The Results Obtained Through Decryption Done Over Smartphone And Virtual Machine.

Text And Image	Time Taken For Decryption in virtual machine (in millisecs)	Time Taken For Decryption in smartphone (in millisecs)
1. Hello	1	7
2.1234-2345-3456-4567-5678-6789-6790-1235-1267.	3	11
3. Portability storage space and battery life are the main characteristics of smartphone's .	4	12
4. Image a1.jpg	567	1240

For decryption the data on the virtual device and smartphone separately it will take a lot of time on the Smartphone and less time on the virtual machine. As in the Figure 5. Results obtained from the decryption of the data are shown it achieves 3x speedup by decrypting the text and to decrypt the card number given 4x speedup is attained. This is how it can be assumed in this case also time taken is less on the Virtual machine that Smartphone.

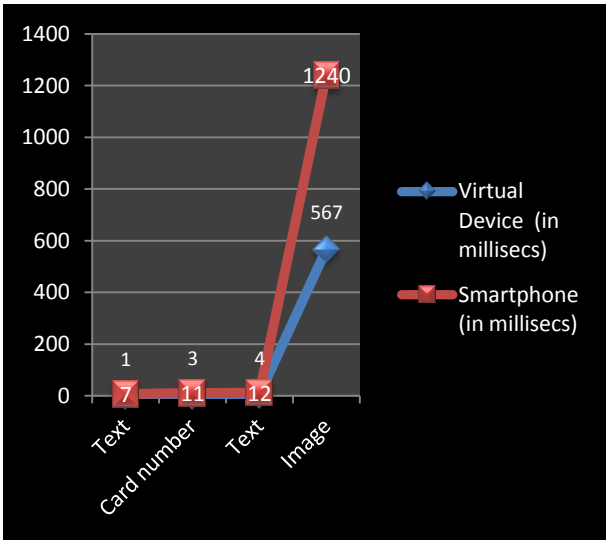

Figure 5. Time taken for Decryption by Virtual Machine and Smartphone

This will lead to arise many constraints on Smartphone's so offloading that work to cloud environment is better which saves time and battery life of the Smartphone [12] shows all the statistics for the cpu utilization and power consumption .And also brings security to the data which is to be kept on the device and confidential for use by an organization or individual. The purpose of the architecture proposed here is also to secure the data stored in Smartphone's by taking the help of the cloud services provided

7. CONCLUSION AND FUTURE SCOPE

Cloud Computing is the model provides many services and now used for security purposes also .As all the smartphone users are opting the services from the cloud for storing their data increasing their usage increases security which is provided by the cloud service providers but what measures can be done to protect the data from the cloud providers also this proposed architecture will help to provide this service to an individual so they can keep their data safe in the way they want to and then by encrypting that data by themselves the data can be send to any public cloud for storage only under any service providers system and can be kept over this proposed scheme will also take a lot to perform as an individual may need his own computation cloud for encryption but this can be done to secure the confidential data as no such scheme is found which do so . As the above mentioned literature survey and related work shows the way to encrypt the data these scheme can also be considered to secure the Smartphone's and by using cloud this will provide and extra power to mobile phones to work faster as than they are right now and this is already being going on many application are their which stores the data from mobile device to cloud but the only issue going on right now is about how much secure that data is on the cloud also these days.

8. REFERENCES

[1] Mell Peter, Grance Timothy "The NIST Definition of Cloud Computing" NIST Special Publication 800-145 in September 2011 .

[2] Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang" A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches" Wiley,pp. 1-38.

[3] Fabrizio Capobianco" Five Reasons to Care about Mobile Cloud Computing" International Free and Open Source Software Law Review Vol. 1, Issue 2, pp. 139-142.

[4] Gupta Pragya, Gupta Sudha" Mobile Cloud Computing: The Future of Cloud" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 1, Issue 3, September 2012 , pp. 134-145.

[5] Niroshinie Fernando, Seng W. Loke, Wenny Rahayu" Mobile cloud computing: A survey" www.elsevier.com/locate/fgcs June 2012 , pp. 85-106.

[6] Hamlen Kevin, Kantarcioglu Murat, Khan Latifur, Thuraisingham Bhavani "Security Issues for Cloud Computing" International Journal of Information Security and Privacy, 4(2), April-June 2010, pp.39-51,

[7] J. Brodkin(2008,Jun) . "Gartner :Seven Cloud Computing Security Risks " available :http://www.infoworld.com/d/security-central /gartner-seven-cloudcomputingsecurity-risks-853 page=0,1 Mar. 13,2009.

[8] Lakshmi Subramanian , Gerald Q. Maguire Jr. ,Philipp Stephanow "An Architecture To Provide Cloud Based Security Services For Smartphones" 2011 KTH Royal Institute Of Technology Stockholm,Sweden

[9] Dijang Huang ,Zhibin Zhou, Le Xu,Tianyi Xing ,Yunji Zhong "Secure Data Processing Framework For Mobile Cloud Computing" Arizona State University , IEEE INFOCOM 2011 Workshop on Cloud Computing.

[10] Brent lagesse "Challenges In Securing The Interface Between The Cloud And Pervasive Systems" Cyberspace Science And Information Intelligence Research Computational Sciences And Engineering, Oak Ridge National Laboratory.

[11] Mayank Arora, Mala Kalra and Dr. Sarabjeet Singh. "ACOF: Autonomous Computation Offloading Framework for Android using Cloud", In proc of IEEE 2nd International Conference on Information Management in the Knowledge Economy, 2013

[12] Power tutor application. Feb 2013. Available: http://ziyang.eecs.umich.edu/projects/powertutor.

[13] Kumar Kartik · Liu Jibang · Yung-Hsiang Lu · Bhargava Bharat" A Survey of Computation Offloading" For Mobile Systems" Springer April 2012.

[14] Eric Y. Chen , Mistutaka Itoh "Virtual Smartphone Over IP" NTT Information Sharing Platform Laboratories, NTT Corporation 3-9-11 Midori-cho, Musashino-shi, Tokyo, 180-8585, Japan.

[15] Byung-Gon Chun, Petros Maniatis "Augmented Smartphone Applications Through Clone Cloud Execution " Intel Research Berkeley 2009, pp. 1-5.

[16] Shaoxuan Wang and Sujit Dey, Senior Member, IEEE "Adaptive Mobile Cloud Computing to Enable Rich Mobile Multimedia Applications" IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 15, NO. 4, JUNE 2013,pp.870-883,

[17] Yi Xu And Shiwen Mao, Auburn University "A Survey Of Mobile Cloud Computing For Rich Media Applications" Auburn University, IEEE Wireless Communications • June 2013, pp. 46-53.

[18] Hoon Jeong, Euiin Choi "User Authentication Using Profiling In The Mobile Cloud Computing"Department Of Computer Engineering,Hannan University,Ojung – Dong 133,Daeduk- Gu ,Daejeon Korea 2012 AASRI Conference On Power And Energy Systems published by Elsevier ,pp. 262-267 .

[19] Atta ur Rehman Khan, Mazliza Othman, Sajjad Ahmad Madani, *IEEE Member*, and Samee Ullah Khan, *IEEE Senior Member"* A Survey of Mobile Cloud Computing Application Models*"* IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 1, FIRST QUARTER 2014, pp. 393-412.