Asian J. of Adv. Basic Sci.: 2(3), 75-82
ISSN (Online): 2347 - 4114
www.ajabs.org

Privacy & Security of Mobile Cloud Computing

Teg Singh

Deptt. Of BCA & PGDCA Govt. Degree College Bilaspur (H. P.)
Email ID: tejuit9@gmail.com

ABSTRACT: The Indian government, like governments elsewhere in the world, has chosen mobile device as preferred platform to engage with citizens while offering various e-Governance services. Likewise there is huge market for mobile based e-Commerce applications across the globe. However uptake of these services is challenged by the security and privacy concerns of the end user. The limited processing power and memory of a mobile device dependent on inherently unreliable wireless channel for communication and battery for power leaves little scope for a reliable security layer. Thus there is a need for a lightweight secure framework that provides security with minimum communication and processing overhead on mobile devices. The security and privacy protection services can be achieved with the help of secure mobile-cloud application services. Taking support from a proximate cloud a security service could be devised for a mobile device which works as an interface and adaptively provides optimum security solutions based on communication channel capacity, available system resources both hardware and software and user-defined parameters. We plan to explore and experiment with available options to recommend security and privacy enhancing approaches that may meet the security need for mobile application using automated sensing of the context.

Key Words: Mobile Security, Adaptive Security, m-governance, m-commerce, Privacy and Security.

INTRODUCTION

Mobile Cloud Computing (MCC) is combination of two terms, mobile computing and cloud computing. Mobile computing is provision of applications on mobile devices. Cloud computing refers to getting paid services either in the form of infrastructure, platform or software through internet based cluster of distributed servers. Mobile cloud computing is provision of mobile applications using cloud to give more power to mobile devices towards computing, in spite of resource limitations in mobile devices. Mobile cloud computing is a concept that has been in use since 2009 and is still evolving.

There are various known challenges in the field of MCC viz. handover delay, bandwidth limitation, task division for offloading, reliability, integrity of data delivered, scalability of MCC without degradation in performance or change in infrastructure, security of data in mobile device within a cloud and in the communication channel, identity privacy, location privacy, etc. These challenges are the biggest obstacles in growth of mobile cloud computing. According to the literature[1 & 2] 74% of IT Executives and Chief Information Officers are not willing to adopt cloud services due to the risks associated with security and privacy. In MCC the security threats are likely in various segments viz. mobile device, communication channel or the cloud itself. So one has to provide protection from these threats by having secure cloud application services in mobile devices and cloud, secure routing protocols in communication channel and secure virtualization in cloud architecture. According to review of the current approaches in MCC[3], the security framework for MCC is divided into two categories; Data Security framework and Application Security Framework. Data Security frameworks are compared on the basis of their basic theory – mathematical principle or cryptographic principle, data protection –protection of data created or manipulate on device or data created or manipulate on cloud, data integrity, scalability, assumption of components-fully trusted, semi trusted or distrusted, data access automated or semi automated and authentication of originator of file. Application security framework can be compared on the basis of application type, security features like data security, integrity, identity privacy, location privacy, and authentication, secure data access to management or secure routing, assumption of component trust levels, scalability of framework. Each security framework must be viewed with its security strength and resource

usage. In security strength we take care of confidentiality, integrity, authentication parameters. In resource usage we consider memory usage, processing time and network overhead parameters[4].
In this paper, section 2 reviews the related literature on cloud computing, MCC and various security aspects of mobile and cloud computing. Section 3 deals with the overall architecture of the proposed plan elaborating on need of cloud computing in 3.1, features of mobile cloud computing in 3.2, objective in 3.3. Section 4 describes the possible validation approaches to test the design objective. Section 5 lists out the challenges involved in the research objectives whereas section 6 concludes the paper highlighting the possible outcome of this research work.

Mobile Cloud Computing: The application of cloud is possible in many domains. One of the domains of our current interest is that of mobiles. Hence, we will be focusing on utility of cloud computing environment for mobile usage and how can a cloud add value to the overall functionality and performance of mobile devices? According to Khan et al [3] as depicted in figure 2, MCC is a service that allows resource constrained mobile users to adaptively adjust processing and storage capabilities by transparently partitioning and offloading the computationally intensive and storage demanding jobs on traditional cloud resources by providing ubiquitous wireless access.

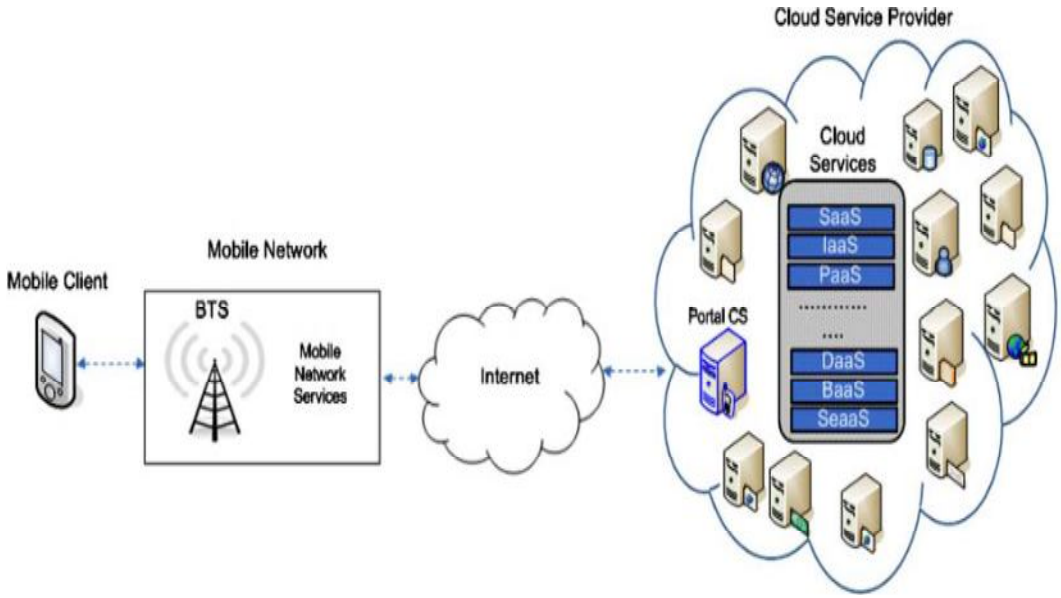

Figure 1: Mobile Cloud Computing Architecture

Some of the limitations of mobile devices which drive use of Cloud Computing for mobile devices are:

- Limited battery
- Low storage
- Less security
- Limited processing power
- Unpredictable Internet connectivity
- Less energy

Related Work: Security and privacy issues of MCC have been discussed by many researchers. J. Oberheide et al.[5] proposed Cloud AV platform, malware detection system for mobile device by moving detection capabilities to network service or cloud. Zhang et al.[6] present security framework for elastic mobile application model by dividing an application into easily configurable weblets. Xiao and Gong[7] proposed scheme for mobile cloud environment to generate a dynamic credential for mobile user for their identity protection from hackers. Wang and Wang[8] have proposed privacy preserving framework for mobile devices while using location based scheme by spatial cloaking. Huan et al.[9] presents framework –

MobiCloud to enhance the functionality of MANET and cover security aspect in terms of risk management and secure routing. G. Portokalidis et al.[10] proposed scheme for threat detection in a smart phone with Mobile Cloud Computing. H.Zhang and X Mingjun[11] proposed distributed spatial cloaking protocol for location privacy. P.Zou et al[12] propose Phosphor, a cloud based mobile digital right management scheme with Sim Card by designing License state word. R.Chow et al.[13] present policy based cloud authentication platform using implicit authentication for solving privacy issues. Itani et al.[14] proposed an energy efficient framework for mobile devices by using incremental message authentication code to ensure integrity of mobile users. Jia et al.[15] presents proxy re-encryption (PRE) scheme and identity based encryption (IDE) scheme to achieve secure data service. Huangs et al.[16] proposed secure data processing framework for MobiCloud addressing issue of authentication on cloud. Hsueh et al.[17] Proposed authentication mechanism to ensure security and integrity of mobile users files stored on cloud server. Yang et al.[18] extended the public provable data possession scheme with Diffie Hellman Key Exchange, Bilinear mapping and Merkle Hash Tree (MHT). Chen et al.[19] present security framework for location based grouped scheduling services for identity privacy and authentication. Ren et al.[20] proposed three schemes; encryption based, coding based and sharing based to ensure the confidentiality and integrity of user's file stored at cloud. Zhou and Huang[21] proposed a privacy preserving framework by offloading the processing and storage intensive encryption and decryption on cloud based on Cipher text Policy attribute. Current research initiatives seem to address only one or two parameters of security from the comprehensive set of authentication, integrity, confidentiality and privacy. These research approaches favor static security algorithms without considering changing demand for security, quality of service, and resource usage of mobile users.

Architecture of the model proposed to be explored:

Cloud Computing: The Cloud Computing is gaining popularity with its main advantage of reducing the computational burden of the client and thus reducing the complexity and other infrastructure requirements at the client end. However, it is important to realize that the market is still deprived of cloud service providers because of following important issues:

- Data replication
- Consistency
- Limited scalability
- Unreliability
- Unreliable availability of cloud resources
- Portability
- Trust
- Security
- Privacy

The commonly accepted definition of Cloud computing is an IT service being provided to users on demand and being paid for depending upon amount of usage. It can also be termed as a dynamic service being provided to users that can 3 add on to the available capacity and capabilities of user entity. Some of the key services of Cloud Computing as depicted in Figure 1 are:

- Infrastructure as a Service (IaaS)
- Data storage as a Service (DaaS)
- Communication as a Service (CaaS)
- Security as a Service (SecaaS)
- Hardware as a Service (HaaS)
- Software as a Service (SaaS)
- Business as a Service (BaaS)
- Platform as a Service (PaaS)

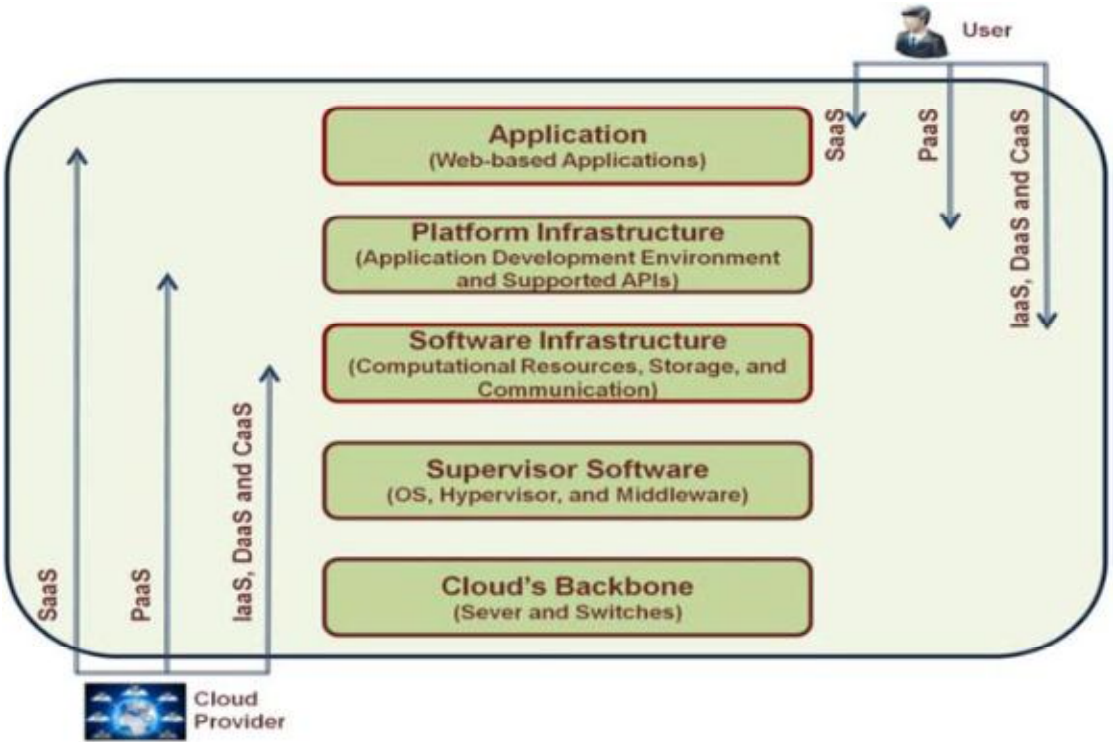

Figure 2: Layered Architecture of Cloud Computing

M-governance and E-Governance: M-Government is a subset of e-Government. E-Government is the use of information and communication technologies (ICTs) to improve the activities of public sector organizations. In the case of m-government, those ICTs are limited to mobile and/or wireless technologies like cellular/mobile phones, and laptops and PDAs (Personal Digital Assistants) connected to wireless Local Area Networks (LANs). M-Government
can help make public information and government services available "anytime, anywhere" to citizens and officials. M-Government should not be seen as something brand-new: for example, wireless technology has always been an important part of law enforcement. Only today, police officers are as likely to use a laptop wirelessly connected to the Internet as the good old two-way radio. When officers spot a suspicious vehicle they can directly search databases that provide information on who owns the vehicle, if it has been reported stolen or has been reported at a crime scene, and if the owner is wanted by police or has jumped bail. Health and safety inspectors can now file their reports from the field in real time using a Pocket PC or handheld terminals, eliminating paper forms and the need to re-enter the data collected when they get back
to the office. On the other hand, citizens are able to save time and energy by further accessing the Internet and government networks through mobile phones and other wireless devices. In Malaysia, for example, citizens can verify their voting information, such as the parliamentary and state constituencies where they are to vote, using SMS (Short Message Service). Alternatively, citizens can request that real-time information is
sent to their mobile phone, PDA(Personal Digital Assistants), or pager as an e-mail or text message. As another example, the California state government has established a Web page where citizens can register to receive wireless PDA (Personal Digital Assistants) and cell phone notification services for energy alerts, lottery results, traffic updates and articles from the Governor's pressroom. M-Government is not only about efficiency but it also allows for citizen activism. In Philippines, citizens are able to help enforce anti-pollution laws by reporting smoke-belching public buses and other vehicles via SMS. SMS is also being used to get citizens involved in the fight against crime and illegal drugs. M-Government is not a replacement for e-government, rather it supplements it. While mobile devices are excellent access

devices, most of them, particularly mobile phones, are not suitable for the transmission of complex and voluminous information. Despite the emergence of more sophisticated handsets, mobile phones do not have the same amount of features and services as PC-based Internet applications. For example, SMS limits messages to 160 characters, whereas email allows a nearly infinite quantity of characters and multimedia content. Even PDAs or Pocket PCs that support email have display and other limitations. Internet-connected PCs are still the preferred device to take part in online political discussions, 295 Towards Next Generation E-Government to search for detailed public sector information, and to transact most types of e-government service. Mobile applications also rely on good back office ICT infrastructure and work processes: government networks and databases, data quality procedures, transaction recording processes, etc. m-Government is particularly suited for the developing world where Internet access rates are low but mobile phone penetration is growing rapidly, particularly in urban areas. Globally, the number of mobile phones has surpassed the number of fixed/wired phones. This is also the case in many individual nations, including 49 middle-income and 36 low-income countries. Among these countries are Burkina Faso, Chad, Honduras, Indonesia, Jordan, Mexico, Mongolia, Nigeria, Philippines, Saudi Arabia, and South Africa.

Critical Issues for m-Government Applications:

Privacy and Security: While all traffic on the Internet is subject to interception, some hackers are spying on corporate wireless networks from outside buildings, where they can scan e-mail and documents. Wireless networks broadcast signals over the public airwaves so they are vulnerable. Privacy and security issues must be addressed in the planning phase, and may impact the timing or selection of a specific type of wireless service. Specific programs have been developed and released on the Internet to facilitate access to 802.11b networks using the Wired-Equivalent Privacy (WEP) encryption system. AirSnort and WEPCrack are tools that can be used to grab passwords and other sensitive data. Additional security protocols are being developed for 802.11 networks, and some vendors are offering enhanced security features in specific products.

Accessibility: As government entities pursue plans to provide access to m-Government information and services via text to wireless access devices, they should also facilitate making the information more accessible for all citizens via the Web and other communications technologies. The new Voice Extensible Markup Language protocol is being developed to make information on Web sites accessible to disabled and other users by telephone. This technology could make Web site information accessible by voice commands. 296Manish Kumar and Omesh Prasad Sinha / M-Government – Mobile Technology for e-Government The World Wide Web Consortium's draft VoiceXML 2.0 standard integrates markup languages for common dialogs, grammar, speech synthesis and natural language semantics.

Research Objective: Our research objective is to propose and develop a system in which security protocols can be decided for a mobile entity dynamically in a cloud. For this, we will be focusing on not just the mobile security parameters but also on the cloud security related issues and respective parameters. As suggested by Khan et al [3], the security and privacy protection services can be achieved with the help of secure cloud application services. Figure 3 describes the security services necessary at various layers of the supporting cloud. In addition to security and privacy, the secure cloud application services provide the user management, key management, encryption on demand, intrusion detection, authentication, and authorization services to mobile users. There is a need for a secure communication channel between cloud and the mobile device. The secure routing protocols can be used to protect the communication channel between the mobile device and cloud.

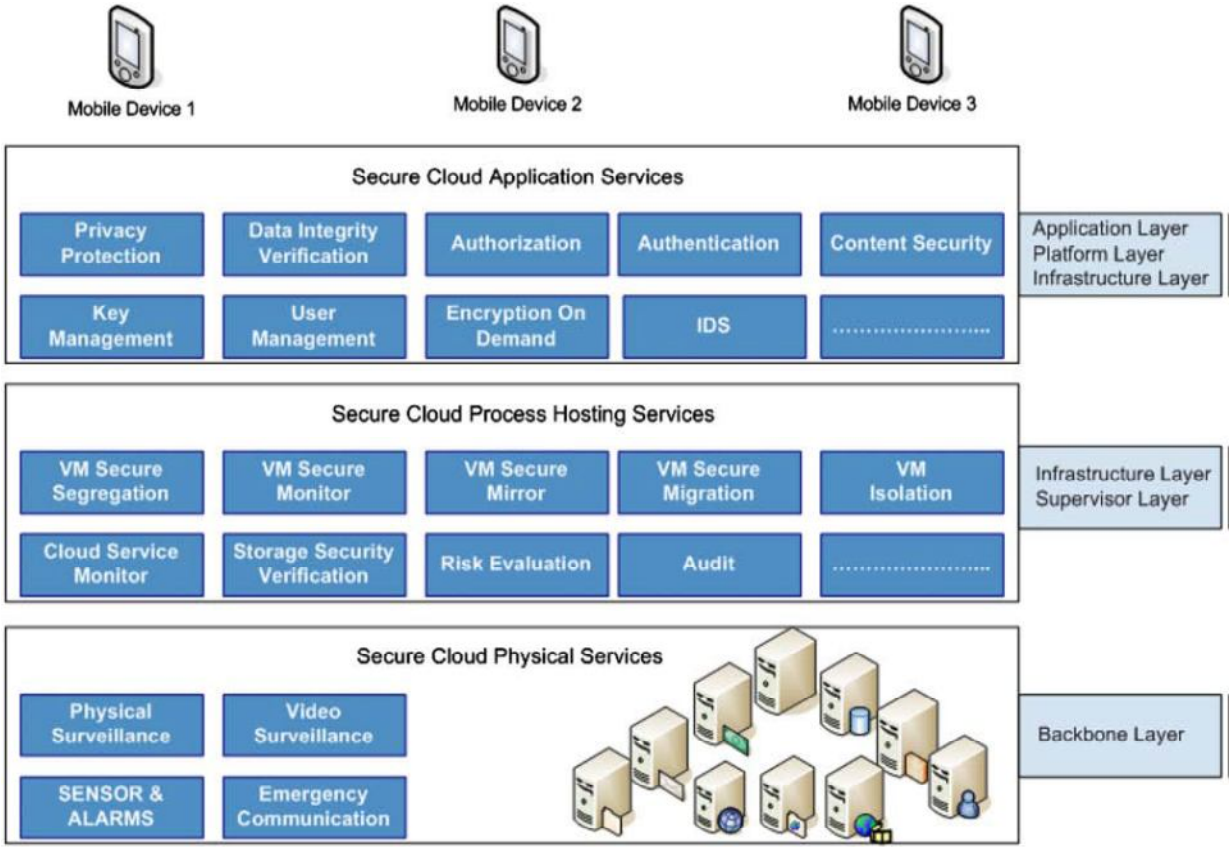

Figure 3: Security services on different layers

The key illustrative areas of proposed research are:

- Preparation of semantic data for security parameters
- Cloud Security attributes
- Mobile Security features and respective parameters
- Security protocols under different security requirements
- Platform Independent Security Architecture.

In the work of Khan et al.[3], frameworks of various aspects of security features have been described in detail. As suggested by Rocha et al.[4], a security service can be devised which works as a middleware with the ability to change the security protocols dynamically between two peers. In their work, domain is of independent mobile users.

We propose to expand this concept to a cloud where a number of mobile users will be acting as members of the cloud and will exchange information within the cloud. For this we need to define various levels of security. A mobile may require different levels of security at different times depending upon the service being used and the sensitivity of the data exchanged with the peer.

CONCLUSION

This paper has attempted literature review of various approaches for effective deployment of secure mobile cloud computing paradigm.

Challenges and possible options have been delineated while we try to explore and characterized an adaptable and dynamic framework providing configurable security interface at the application layer.

Issue connected with validation and testing of proposed solution have also been considered to help us formulate dependable testing and benchmarking of a security firmware in the context of mobile cloud computing.

The fallout of the proposed research is expected to be of interest to both E-governance and E-commerce applications. The challenges in this evolving field of research are many and we plan to proceed in phases with first phase attempting to characterize the problem in formal terms and propose a lightweight mobile interface having limited dynamic capability. Later phase may attempt expanded objectives.

REFERENCES

1. Subashini,S. ,Kavitha,V.: A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications 34 (1) 1–11 (2011).
2. 2. Buyya,R.,Yeo C.S.,Venugopal,S., Broberg,J.,Brandic I.: Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems 25 (6) (2009) 599–616
3. 3. Khan,A.,N.,Mat Kiah,M.,L., Khan S.,U.,Madanic,S.A. :Towards secure mobile cloud computing: A survey, Future Generation Computer Systems 1-22 (2012)
4. 4. Bruno P.S.Rocha,Daniel N.O.Costa,RandeA.Moreira,ristianoG.Rezende,Antonio A.F.Loureiro, Azzedine Boukerche : Adaptive security protocol selection for mobile computing, Journal of Network and Computer Applications (2012)
5. 5. Oberheide,J., Veeraraghavan,K., Cooke, E., Flinn, J., and Jahanian, F.. :Virtualized in-cloud security services for mobile devices, in Proceedings of the 1st Workshop on Virtualization in Mobile Computing (MobiVirt), pp. 31-35, (June 2008).
6. 6. Zhang, X., Schiffman, J. , Gibbs ,S., Kunjithapatham, A., Jeong, S.: Securing elastic applications on mobile devices for cloud computing, in Proceeding ACM workshop on Cloud computing security, CCSW ’09, Chicago, IL, USA,(Nov. 2009.)
7. 7. Xiao, S., Gong, W.: Mobility can help: protect user identity with dynamic credential, in: Proc. 11th Int. Conference on Mobile Data Management, MDM ’10, Missouri, USA,(May 2010)
8. 8. Wang, S., Wang, X.S.: In-device spatial cloaking for mobile user privacy assisted by the cloud, in: Proc. 11th Int. Conference on Mobile Data Management,MDM ’10, Missouri, USA,(May 2010).
9. 9. Huan,D., Zhang, X., Kang ,M., Luo ,J.: MobiCloud: building secure cloud framework for mobile computing and communication, in: Proc. 5th IEEE Int. Symposium on Service Oriented System Engineering, SOSE ’10, Nanjing, China,(June 2010).
10. 10. Portokalidis,G.,Homburg,P.,Anagnostakis,K., Bos,H.: aranoid Android: versatile protection for smartphones, in Proceedings of the 26th Annual Computer Security Application Conference (ACSAC), pp. 347-356, (September 2010).
11. 11. Zhangwei ,H. and Mingjun ,X., : Distributed Spatial Cloaking Protocol for Location Privacy, in Proceedings of the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), vol. 2, pp. 468,(June 2010.)
12. 12. Zou,P., Wang,C., Liu ,Z., and Bao ,D.,: Phosphor: A Cloud Based DRM Scheme with Sim Card, in Proceedings of the 12th International Asia-Pacific on Web Conference (APWEB), pp. 459, (June 2010).
13. 13. Chow, R., Jakobsson, M., Masuoka, R., Molina, J., Niu Y., Shi ,E., Song, Z. :Authentication in the clouds: a framework and its application to mobile users, in: Proc. ACM Cloud Computing Security Workshop, CCSW ’10, Chicago, USA,(Oct. 2010.)
14. 14. Itani,W., Kayssi,A., Chehab, A.: Energy-efficient incremental integrity for securing storage in mobile cloud computing, in: Proc. Int. Conference on Energy Aware Computing, ICEAC ’10, Cairo, Egypt, (Dec. 2010.)
15. 15. Jia,W., Zhu ,H., Cao, Z., Wei, L., Lin, X.,:SDSM: a secure data service mechanism in mobile cloud computing, in: Proc. IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, Shanghai, China,(Apr. 2011).
16. 16. Huang,D., Zhou,Z., Xu,L., Xing,T., Zhong,Y:Secure data processing framework for mobilecloud computing, in: Proc. IEEE INFOCOM Workshop on Cloud Computing, INFOCOM ’11, Shanghai, China, (June 2011.)

17. 17. Hsueh ,S.,C., Lin ,J.Y., Lin, M.Y.,: Secure cloud storage for conventional data archive of smart phones, in: Proc. 15th IEEE Int. Symposium on Consumer Electronics,ISCE '11, Singapore, (June 2011.)
18. 18. Yang, J., Wang, H., Wang, J., Tan, C., Yu1, D.: Provable data possession of resource constrained mobile devices in cloud computing, Journal of Networks 6 (7) 1033–1040 (2011).
19. 19. Chen,Y.,J., Wang,L.,C.: A security framework of group location-based mobile applications in cloud computing, in: Proc. Int. Conference on Parallel Processing Workshops, ICPPW '11, Taipei, Taiwan, (Sep. 2011.)
20. 20. Ren,W., Yu,L., Gao,R., Xiong,F.: Lightweight and compromise resilient storage outsourcing with distributed secure accessibility in mobile cloud computing, Journal of Tsinghua Science and Technology 16 (5) 520–528 (2011).
21. 21. Zhou,Z., Huang, D.: Efficient and secure data storage operations for mobile cloud computing, IACR Cryptology ePrint Archive: 185, (2011).
22. 22. Dimitrios Zissis, Dimitrios Lekkas,: Addressing Cloud Computing Issues, Future Generation Systems (28) 583-592 (2012).
23. 23. ISTQB Exam certification .com Webpage-http://istqbexamcertification.com/what-is-validation-in-software-testing-or-what-is-software-validation/
24. 24.Belatrix cloud testing best practices, Belatrix Software Factory-White papers http://www.belatrixsf.com/index.php/outsourcing-case-studies/1318