Networks Security on Mobile Computing – A Survey

T.Chithambaram.

Research Scholar, School Of Computer Science,
Engineering and Applications Bharathidasan University, Trichy.
E-mail: chithambaram1102@gmail.com
Phone Number: 9751679126.

M. DuraiRaj

Assistant Professor, School Of Computer Science,
Engineering and Applications Bharathidasan University, Trichy.
E-mail: durairaj.bdu@gmail.com
Phone Number: 9487542202

ABSTRACT — Mobile cloud computing alleviates the limitations of resource-constrained mobile devices. Mobile cloud computing is gained popularity among mobile users of 998 million in 2014. Mobile Cloud computing is a collection of large group of interconnected networks. This includes personal computers, network servers; mobile computing can be classified in to two types as public and private cloud. Mobile cloud computing describe both a platform and type of application. A cloud computing platform need provisions, configures, reconfigures and depravations servers. The security issues begin to grow and raised there are number of loopholes and challenges that still exist in the security of mobile cloud computing. The security threats have got a hurdle in the rapid adaptability of the mobile computing paradigm. Significant efforts have been committed in research organizations and academia to build secure mobile cloud computing environments and infrastructures. In cloud computing, top cloud services challenges are security, availability and performance. The cloud computing security issue is always the key factor and it is ranked one. This paper presents a survey about the mobile cloud computing security issues and challenges focusing on the cloud computing.

Keywords: Mobile Cloud Computing, Network Security, Privacy, Encryption Algorithm, Cryptography.

1. INTRODUCTION

Mobile Cloud computing is a form of distributed computing technology. It's development of distributed processing, parallel processing and grid computing. Its most basic concepts is that automatically split a huge amount of calculation program into numerous smaller subroutines through the network, and then handed over to the operation system that consists of several servers. After calculating and analyzing it will process the results and return them the user [1, 2]. In spite of the hype achieved by mobile cloud computing, the growth of the mobile cloud computing subscribers is still below expectations due to the risks associated with the security and privacy. To have an in deep understanding of Mobile Cloud Computing and its network security, it is necessary to get the complete grasp on mobile cloud computing. Where user is able to rent software and hardware infrastructure and computational resources as per user basic Computing concept, technology and architectures have developed and consolidated in the last decades. Cloud Computing let you access all your application and documents from anywhere in the world, It easier for group members in different locations to collaborate. Cloud computing is not network computing. And it is a lot bigger than that. The mobile cloud computing (MCC) is Internet-based data, applications and related services (computing) obtain or retrieve from a storage device; as of information on accessed through Smartphone's, laptop computers, tablets and other portable devices [1, 2].

Mobile cloud computing is different from mobile computing. The devices run cloud-based network application rather than written specifically to run on a particular processor. User subscribes a cloud services and access remotely stored applications and their associated data over the Internet. [6].

The mobile devices run a mix of Web-based and native apps. However, the trend is increasingly toward the mobile cloud. According to ABI Research, the number of mobile cloud computing subscribers is reached 998 million in 2014. [3, 4]. In cloud computing, top cloud services challenges are security, availability and performance. The cloud computing security issue is always the key factor and it is ranked one [5].

In this paper, the resent articles published on mobile cloud computing technologies and security issues are briefly reviewed. The articles reviewed in this work are collected from Elsevier and IEEE journals. This paper also summarized cloud service delivery models, deployment model and some of the mobile computing technologies.

2. CLOUD SERVICE DELIVERY MODELS

The concept of cloud services development encompasses several different types of development; the cloud comprises three major components: clients, data centers and distributed servers. Data center is defined here as the collection of servers hosting different applications, whereas distributed servers are the elements of a cloud that are present on internet hosting different applications [6,11].

There are three service layers models are available. They are:

2.1 Infrastructure as a service (IaaS):

In this model the cloud providers offers the cloud services like hardware resources, storage and network infrastructure services. The virtualization is the base of this model.

Infrastructure as a service (IaaS) to deploy their applications, cloud users installs operating system images and their application software on the cloud infrastructure.

2.2 Platform as a service (PaaS):

In this model the cloud service providers provide application development platform for the developers. It also deliver a set of APIs for the developers to develop and launch Their own customized applications. It is not needed to install development tools on local devices and machines. The development environment is offered as a service. The developer uses the building blocks of the vender's development environment to create his own custom application.

2.3 Software as a service (SaaS):

This model facilitates the customers to access the applications hosted on the cloud. Instead of installing the applications on their own machines, the users' access the applications installed is the mobile cloud using their own browsers. Software as a service, or SaaS, is probably the most common type of cloud service development. With SaaS, a single application is delivered to thousands of users from the venders servers. Customers no need to pay for owning the software rather, they pay for using it. Access an application via an API accessible over the web.

3. THE TYPES OF CLOUD APPLICATION DEPLOYMENT MODELS

The cloud computing has three different new deployment models and each model has its own benefits and trade-offs. There is also another model called community models. There are briefly described in this section [1, 2, 4, 5, and 11]. There are different kinds of services provided by the cloud for the cloud users.

There are four types of cloud deployment model

- Public cloud
- Private cloud
- Community cloud
- Hybrid cloud

Private cloud: A term that is similar to, and derived from, the concept of Virtual Private Network (VPN), is applied to Cloud Computing. The Private Cloud delivers the benefits of Cloud Computing with the option to optimize on data security, corporate governance and reliability.

Public cloud: This cloud is available to all the external users through internet who can register with cloud and can use cloud resources on a pay-per-use model. This cloud is not secure like private cloud because it is accessible to the internet users. Public cloud refers to Cloud Computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet.

Community cloud: A community cloud is established among several organizations that have similar requirements and seek to share their computing infrastructure in order to realize some of the benefits of the Public Cloud.

Hybrid cloud: This is a type of private cloud which uses the resources of one or more public clouds. It is a mix of both private and public cloud.

4 MOBILE CLOUD COMPUTING, METHODOLOGIES AND TOOLS

4.1. Mobile Cloud Computing

(MCC) is a combination of cloud computing, mobile computing and wireless networks to bring rich computational resource to mobile users and network operators, as well as cloud computing suppliers. The ultimate goal of MCC is to enable execution of high mobile applications on a plethora of mobile devices; with a high user experience [11]. MCC provides business opportunities for mobile network operators as well as cloud providers. In The mobile cloud computing (MCC) has been inherited from cloud computing MCC which incorporates cloud computing properties with the mobile computing environment. Due to its attractive business model and the increased number of mobile phone smart-phone, tablet pc etc users in the world, the MCC is

proving to be a potential future technology. It has also attracted the attention of many businessmen and entrepreneurs as a prospective and lucrative business opportunity.

From mobile user prospective, MCC is an amazing improvement because it diminishes the mobile resources issues like, limited battery power, slow processing power, low internet bandwidth, small storage space and less energy consumption [7].

4.2. A Mobile Cloud Computing Scenario

The mobile cloud computing (MCC) is Internet-based data, applications and related services (computing) obtain or retrieve from a storage device; as of information on accessed Smartphone's, laptop computers, tablets and other portable devices.[1,2].

Mobile cloud computing is the differentiate from mobile computing in general because the devices run cloud-based network application rather than written specifically to run on a particular processor. User subscribes a cloud services and access remotely stored applications and their associated data over the Internet. [6].

Mobile cloud computing refers in the cloud usage of cloud computing in same combination of mobile devices. It is a same combination between mobile network and cloud computing, there distributing optimal services for mobile users. Cloud computing exists when tasks and data are kept on the internet rather than on individual devices, providing on-demand access. Applications are run on a remote server and then sent to the user [2, 5].

5. METHODOLOGIES AND TOOLS

5.1. Encryption algorithm:

The primarily purpose of encryption is to protect the confident of digital data stored on computer systems or transmitted the web or other computer internet. Modern encryption algorithms play a vital role in the security assurance of IT systems and communications as they can provide not only confident, the following keys components of security:

- Authentication **:** The origin of a message can be verified.authentication
- Integrity **:** proof that the contents of a message have not been changed since it was sent.
- Nin-repudiation : The sender of a message cannot deny sending the message.

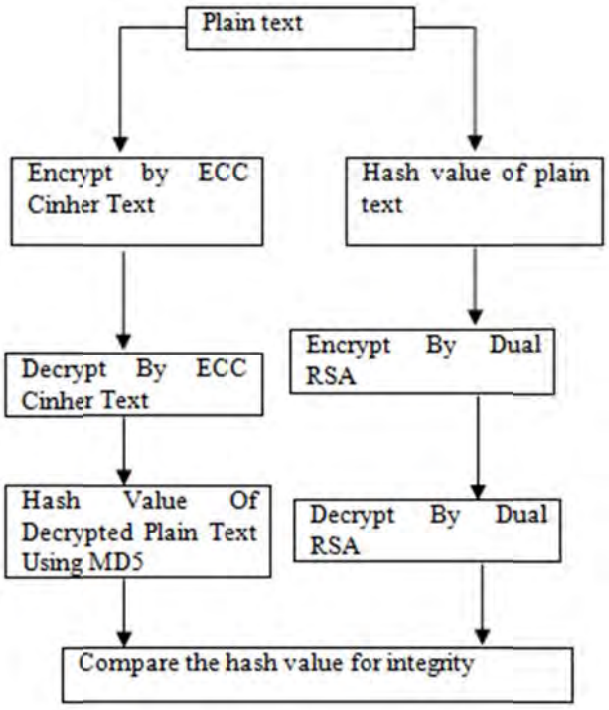

Fig. 2. Encryption Security Protocol Architecture [14].

The arrival of the Diffie-Hellman key exchange and RSA algorithms, government and their armies were the only real users of encryption. However, Diffie-Hellman and RSA led to the broad use of encryption in the commercial and consumer realms to protect data both while it is being sent across a network (data in transit) and stored, such as on a hard drive, smart phone or flash drive (data at rest). Devices like modems, set-top boxes, smartcards and SIM cards all use encryption or rely on protocols like SSH, S/MIME, and SSL/TLS to encrypt

sensitive data. Digital rights management systems, which prevent unauthorized use or reproduction of copyrighted material, are yet another example of encryption protecting data [12, 14].

5.2 Mobile cloud computing security algorithms:

RSA- is an algorithm for public-key cryptography, involves a public key and a private key.

MD5- (Message-Digest algorithm 5), a widely used cryptographic hash function with a 128-bit hash value, processes a variable-length message into a fixed-length output of 128 bits.

AES- In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard [11].

6. REVIEW OF RELATED WORKS

This study is based on existing literature, highlights the current state of the work proposed to secure mobile cloud computing infrastructure. Proposed an energy efficient integrity verification scheme for mobile clients to verify the integrity of the files stored on a cloud server using an incremental message authentication code. The proposed scheme offloads most of the integrity verification jobs on a cloud service provider and trusted third party to minimize the processing overhead on the mobile client. The cloud service provider redirects the stored files towards the coprocessor when instructed by a mobile client. The coprocessor computes incremental MAC o n received files for integrity verification. The reviews of literature carried out in this work are described below.

Kuyoro S. O, et. al. [1] highlighted key security considerations and challenges which are currently faced in the Cloud computing security. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

Rajesh Piplode, et. al [2] highlighted that the cloud computing vulnerabilities, security threats cloud computing faces and presented the security objective that need to be achieved. On one hand, the security-sensitive applications of a Cloud computing require high degree of security on the other hand, cloud computing are inherently vulnerable to security attacks.

Deyan Chen, et. al [3] presented a dynamic load balancing algorithm called load balancing Min-Min (LBMM) technique which is based on three level frameworks. This technique uses Opportunistic Load Balancing algorithm which keep each node busy in the cloud without considering execution time of node. Because of this it causes bottle neck in system. The key to privacy in the cloud environment is the strict separation of sensitive data from non-sensitive data followed by the encryption of sensitive elements. According to the analysis for data security and privacy protection issues above, it is expected to have an integrated and comprehensive security solution to meet the needs of defense in depth. Regarding privacy protection, privacy data identification and isolation are the primary tasks. They should be considered during the design of cloud-based applications.

Shahzad, et. al [4] presented a complete understanding of MCC by explaining the architecture, advantages and applications. This paper is mainly focused on highlighting the issues and challenges of MCC like, data security, infrastructure security and communication channel security. The main idea behind this research is to identify these issues and challenges because they are preventing the mobile users to take on cloud services.

Soeung-Kon, et. al [5] discussed the different security issues that arise about how safe the mobile cloud computing environment. This paper have discussed security issues concerning mobile cloud computing. Securing mobile cloud computing user's privacy and integrity of data or applications is one of the key issues most cloud providers are given attention. Since mobile cloud computing is a combination of mobile networks and cloud computing, the security related issues are then divided into two categories: mobile network user's security; and mobile cloud security.

Shih-Hao Hung, et. al, [6] proposed a framework to execute mobile applications in a cloud-based virtualized execution environment controlled by mobile applications and users, with encryption and isolation to protect against eavesdropping from cloud providers. On the system level, the design is for the workload migration framework, so that the system has better flexibility to allocate workload on local processing elements or virtual processing elements on cloud servers, depending on network connectivity and core utilization. As a result, the computation resources can be better utilized.

Swarnpreet Singh, et. al [7] discussed opportunity for the development of mobile applications since it allows the mobile devices to maintain a very thin layer for user applications and shift the computation and processing overhead to the virtual environment. A cloud application needs a constant connection that might prove to be an Achilles heel for the cloud computing movement.

Abdullah Gani, et. al [8] described that the network intensive computing environment such as MCC necessitates the optimal use of networks resources in order to establish a seamless connectivity between SMDs and the cloud. Also limited battery life feature of SMDs requires minimum energy consumption in accessing the services of computational clouds. The consolidation of network terminal, cross-layer information, multi- packet casting, computing capability of network terminal and intelligent network selection algorithm appears to be an

optimum solution for achieving seamless service continuity in order to facilitate seamless connectivity. Also incorporation of distributed mobility management can be an optimum solution for providing seamless connectivity. The development of such communication system between SMD and the cloud will reduce the developmental constraints and facilitate smooth function of mobile cloud computing setup,

Hoang T. Dinh, et. al [9] provided an overview of mobile cloud computing in which its definitions, architecture, and advantages have been presented. The applications supported by mobile cloud computing including mobile commerce, mobile learning, and mobile healthcare have been discussed which clearly show the applicability of the mobile cloud computing to a wide range of mobile services. Then, the issues and related approaches for mobile cloud computing (i.e., from communication and computing sides) have been discussed.

N Sriram , et. al [10] proposed a novel secure and verifiable cloud computing for mobile system using multiple servers. This method combines the secure multiparty computation protocol and the garbled circuit design with the cryptographically secure pseudorandom number generation method of Blum et al. This method preserves the privacy of the mobile client's inputs and the results of the computation, even if the evaluator colludes with all but one of the servers that participated in the creation of the garbled circuit. Further, this method can efficiently detect a cheating evaluator that returns arbitrary values as output without performing any computation. This paper also presented an analysis of the server-side and client-side complexity of this system.

M.Rajendra Prasad, et. al [11] presented the Mobile Cloud Computing will provide a full commercial environment for applications, providing an easy way for smaller developers to monetize their services as well as new routes to market. Crucially, Mobile Cloud Computing will eliminate the commercial and technical fragmentation that has thus far proven to be a barrier to successful collaboration between application providers and operators on a global scale.

Huajian Mao, et. al [12] presented the Wukong, a cloud-oriented file service for mobile devices. Wukong characterizes itself with several unique features. It provides a standard POSIX compliant interface so that existing applications can be deployed on this service directly or with few modifications. It supports multiple heterogeneous storage services, and has a capability to support new or unforeseen services. It introduces negligible overhead while providing an easy way to access cloud services in mobile devices.

Nazanin Aminzadeh, et. al [13] surveyed the crucial intrinsic restrictions of mobile devices and storage augmentation issues in three domains of mobile computing, cloud computing and MCC to devise a taxonomy of issues as the motivation for the emergence of effective and efficient MSA approaches in MCC. A number of approaches leverage data partitioning whereas other approaches exploit data replication, cache management, or SOA. Based on a review of the credible MSA approaches, the paper proposes a taxonomy of cloud-based storage.

S. Subashini, et. al, [14] described that though there are extreme advantages in using a cloud-based system, there are yet many practical problems which have to be solved. Cloud computing is a disruptive technology with profound implications not only for Internet services but also for the IT sector as a whole. Still, several outstanding issues exist, particularly related to service-level agreements (SLA), security and privacy, and power efficiency. As described in the paper, currently security has lot of loose ends which scares away a lot of potential users. Until a proper security module is not in place, potential users will not be able to leverage the advantages of this technology.

Zaheer Ahmad, et. al, [15] emphasized that the security may be added in the form of additional authentication processes and management, which should not interfere with existing (U)SIM authentication, however, there is opportunity to expand the use of the (U)SIM to create an attack resistant foundation for the added security. Virtualization has received a lot of attention on Smart phones and there are several hypervisor products, however, the security foundations will be paramount as the powerful capabilities of hypervisors have much in common with types of published malware.

7. RESULTS AND DISCUSSION

In [1], the authors described cloud computing technology and its development from distributed processing, parallel processing and grid computing. Its most basic concepts is that automatically split a huge amount of calculation program into numerous smaller subroutines through the network, and then handed over to the operation system that consists of several servers. In spite of the hype achieved by mobile cloud computing, the growth of the mobile cloud computing subscribers is still below expectations due to the risks associated with the security and privacy.

The cloud computing [2] can be seen as a new phenomenon which is set to revolutionize the direction on the use of Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological and the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception.

This paper [3] work is targeted on mobile service providers, and this work is to improve security with technologies and mechanisms applied in cloud security to minimize the user's security concerns. On the basis of the literature review conducted, this is concluded that MCC is regarded to be a potential technology in coming years but currently there are serious security issues and challenges which limits its adoption among the mobile users.

The method [6] proposed in this was compared with conventional scheme, and this approach not required the developers to redesign their applications, but offers the opportunities for the users to migrate their applications from one mobile device to another quickly. More importantly, the user is in control of the application deployment and migration, so the risk of leaking data to application service providers is saved. Many practical issues were discussed and proposed a technique to address security issues. At the application level, the agents of the framework was collaborated to support application execution in the cloud with techniques, including check pointing, event recording, event replay, application migration, file synchronization, etc.

This method [8] predicted MIH and IMS based interworking schemes which are suitable candidates for seamless connectivity. In brief, the incorporation of identical strategy and development idea of inter- working and mobility techniques to handle the challenges of network intensive distributed mobile computing like MCC and it could be appreciable solution for achieving seamless connectivity.

In [13], the author discussed mobile devices in local resource conservation, computational augmentation, and storage extension through the convergence of mobile and cloud computing. The association and all its inestimable privileges originate multi-dimensional heterogeneity in various domains, including platforms, operating systems, networks, and data structures. The paper concludes that the need for lightweight, energy- and communication-aware MSA approaches is vital for the successful adoption of mobile computing.

This security module [14] should cater to all the issues arising from all directions of the cloud. Every element in the cloud should be analyzed at the macro and micro level and an integrated solution must be designed and deployed in the cloud to attract and enthrall the potential consumers. Until then, cloud environment will remain cloudy [14]. The integrated security model targeting different levels of security of data for a typical cloud model is meant to be more dynamic and localized in nature.

The perspective and confidence will be dominated by the protection of personal data within common use-case scenarios for Cloud storage [15]. While considering data security in cloud, it is likely that there will be still be locally stored data and great care is needed when it is held on removable storage devices such as flash memories and (U) SIMs [15].

The encryption algorithm proposed and described in the literature outlines that decryption process is reverse of the encryption. This algorithm can be used to encrypt the user data in cloud. Since the user has no control over the data once their session is logged out, the encryption key acts as the primary authentication and the number of existing techniques used to implement security in cloud. Different symmetric and asymmetric algorithms were used for devising effective security mechanism. Cloud computing is revolutionizing how information technology resources and services are used and managed, but the revolution always comes with new problem.

Based on this review of literature, our work will be extended by developing combination of more than one security mechanisms as a hybrid technology for providing effective security mechanism for mobile cloud computing.

8. CONCLUSION

In this paper, different security mechanism applied in the cloud and effectiveness of these mechanism was discussed. Security and Privacy of data stored in Cloud Computing is an area which has full of challenges and of paramount Importance. Cryptographic techniques were applied to provide secured communication between the user and the cloud. Literatures showed that symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data in cloud storage. The encryption algorithm can be applied by the user to ensure that the data is stored only on secured storage. Based on the review of literatures carried out in this work, this paper proposes a technique for effective security mechanism, which will be our future course of work.

9. REFERENCES

[1] S. O. Kuyoro, F. Ibikunle and O. Awodele, "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), vol. 3, Issue 5, (2011).

[2] Rajesh Piplode, Umesh Kumar Singh " An Overview and Study of Security Issues & Challenges in Cloud Computing ", International Journal of Advanced Research in Computer Science and Software Engineering , Vol 2, Issue 9, September 2012 ISSN: 2277 128X.

[3] Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues inCloud Computing", (2012) International Conference on Computer Science and Electronics Engineering.

[4] Abid Shahzad and Mureed Hussain, "Security Issues and Challenges of Mobile Cloud Computing ", International Journal of Grid and Distributed Computing Vol.6, No.6 (2013),

[5] Soeung-Kon, J. -H. Lee and S. W. Kim, "Mobile Cloud Computing Security Considerations", Journal of Security Engineering, no. 9, (2012) April.
[6] Shih-Hao Hung, Chi-Sheng Shih, Jeng-Peng Shieh, Chen-Pang Lee, Yi-Hsiang Huang, " Executing mobile applications on the cloud: Framework and issues ", Computers and Mathematics with Applications 63 (2012) 573–587. Elsevier Ltd.
[7] Swarnpreet Singh, Ritu Bagga, Devinder Singh, Tarun Jangwal "Architecture Of Mobile Application, Security Issues And Services Involved In Mobile Cloud Computing Environment ", International Journal O Computer Science And Electronics Research.Vol.Issues.Agu(2012).
[8] Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani " A review on interworking and mobility techniques for seamless connectivity in mobile cloud computing: Journal of Network and Computer Applications 43 (2014)84–102 (2014) Elsevier Ltd.
[9] Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang, " A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches", Department of Computer Science and Computer Engineering, La Trobe University, Australia 31 Accepted 30 May 2012,Available online 6 June 2012.
[10] Sriram N. Premnatha, Zygmunt J. Haas, " A Practical, Secure, and Verifiable Cloud Computing for Mobile Systems", The 11th International Conference on Mobile Systems and Pervasive Computing (MobiSPC-2014).
[11] M.Rajendra Prasad, Jayadev Gyani, P.R.K.Murti, " Mobile Cloud Computing: Implications and Challenges ", Journal of Information Engineering and Applications ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol 2, No.7, (2012).
[12] Huajian Mao, Nong Xiao, Weisong Shi, Yutong Lu, "A cloud-oriented file service for mobile Internet devices ", J. Parallel Distrib. Compute. 72 (2012) 171–184 31 October 2011, Available online 11 November (2011) Elsevier Ltd.
[13] Nazanin Aminzadeh, Zohreh Sanaei, Siti Hafizah Ab Hamid, " Mobile storage augmentation in mobile cloud computing: Taxonomy, approaches, and open issues ", Simulation Modeling Practice and Theory (2014) Elsevier Ltd.
[14] S. Subashini, V.Kavitha, "A survey on security issues in service delivery models of cloud computing ", Journal of Network and Computer Applications 34 (2011) 1–11, Elsevier Ltd.
[15] Zaheer Ahmad, Keith E. Mayes, Song Dong, Kostas Markantonakis, " Considerations for mobile authentication in the Cloud information security technical report 1 6 (2011) 123to1 3 0 Elsevier Ltd.