Special Issue | August 2017 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

All India Seminar on

Futuristic Trends in Telecommunication Engineering & Telecom Panorama – Fundamentals and Evolving Technology, with Particular Reference to Smart City on 5th – 6th August 2017

Organized by

The Institution of Engineers (India) Jabalpur Local Centre

Secure Data Transfer for Mobile and Smart Devices in Mobile Cloud Computing Environment based on Cloudlet Approach

Dr. Mukta Bhatele
Professor
Department of Computer Science & Engineering
Gyan Ganga Institute of Technology & Sciences
Jabalpur (M.P.), [INDIA]
Email: mukta_bhatele@rediffmail.com

Anshita Khare
M. Tech. (CSE)
Gyan Ganga Institute of Technology & Sciences
Jabalpur (M.P.), [INDIA]
Email: khareanshita13@gmail.com

Abstract**—***Mobile Cloud Computing (MCC) is the combination of cloud computing, mobile computing and wireless networks to bring rich computational resources to mobile users, network operators, as well as cloud computing providers. A Mobile Cloud Computing model based on cloudlet approach with secure data transfer using Hybrid Cryptosystem technique is proposed in this paper. Cloudlet, which is a local Cloud Data Center located in common areas, communicates with mobile devices. Random Way Point (RWP) for mobility mechanism has been used in this proposed model. Infrastructure as a service will be provided by cloudlets to the mobile nodes that will be connected to it. Various workload sizes after performing the encryption using hybrid cryptosystem will be offloaded to the cloudlet. After this, the cloudlet will perform the tasks of the mobile devices and will send the computation results back to the clients. Thus, this proposed model will provide us secure data transfer, mobility management, reduced end to end packet delay and better system scalability.*

Keywords:— *Mobile Cloud Computing, Cloudlet, Random Way Point, hybrid cryptosystem, Wi-Fi Connection.*

1. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is defined as a network that has many free or autonomous nodes, often composed of mobile devices, that can arrange themselves in various ways and operate without strict top-down network administration. Mobile Cloud Computing (MCC) is the combination of cloud computing, mobile computing and wireless networks to bring rich computational resources to mobile users, network operators, as well as cloud computing providers. MCC uses the computational augmentation approaches (computations are executed remotely instead of on the device) by which resource-constraint mobile devices can utilize computational resources of varied cloud-based resources.

Cloudlet is one of the cloud based resource namely proximate immobile entity. It is a new architectural element that extends today's Cloud Computing infrastructure. Cloudlet supports resource-intensive and interactive mobile applications by providing powerful computing resources to mobile devices with lower latency. The critical point is to make data transfer secure when mobile device offloads its data to the cloudlet and receives the result from it. To study the behaviour of the mobile cloud computing model in terms of performance to find out the benefits and drawbacks in order to achieve an appropriate solution for the secure data transfer is the proposal of this research paper. This mobile cloud computing model consists of an enterprise cloud in addition to the cloudlets. It provides infrastructure as a service for mobile cloud applications. The mobile user gets connected to the cloudlet by Wi-Fi. We have proposed a new ad-hoc cloudlet network model over using enterprise cloud to find out the solution of data transmission security. It also measures the ability of the proposed model to react to the network topology change with the help of the contextual information of the mobile devices. For security purpose, this model will utilize the hybrid cryptosystem so that mobile device and cloudlet will exchange their data in encrypted form. Thus, the security of the data will be achieved. The remainder of this paper is organized as follows; Section 2 presents the related work and Section 3 depicts the proposed architecture. Section 4 describes the additional components of the cloudlet. Finally, we conclude the paper in section 5.

2. LITERATURE REVIEW

Mobile Cloud Computing has been defined in various ways in many literatures. In [4], the definitions of Mobile Cloud Computing have been divided into classes. The first refers to carry out data storage and processing outside mobile devices. Mobile devices are simply terminals in Cloud Computing, only intended to provide convenient way to access the services in the cloud. By this, the storage and computing limitations of mobile devices are avoided. In this way, the centralized maintenance is beneficial for MCC. Now the second class of definitions refers to computing where data storage and processing are also carried out on mobile devices. This introduces the concept of the Ad-hoc Mobile Cloud. This kind of Ad-hoc cloud network is advantageous in special cases such as battle field, disaster management etc.

In [10], the author surveyed the existing work in mobile computing through the prism of cloud computing principles. They also highlighted research challenges in the area of mobile cloud computing. Mobile Community Cloud Platform (MCCP) as a cloud computing system has been proposed. It can leverage the full potential of mobile community growth. An analysis of the core requirements of common mobile communities has been provided. The design of cloud computing architecture that supports building and evolving of mobile communities has been presented [5]. In [6], An architecture based on virtual machine (VM) technology has been proposed. It rapidly instantiates customized service software on a nearby *cloudlet* and then uses that service over a wireless LAN. The mobile device typically functions as a thin client with respect to the service.

In [5,7,8,9,10], analysis of running an application for mobile on a remote resource rich server has been done. While the mobile device performs in the vein of a thin client connecting over to the distant (enterprise) server through 3G. The asymmetric encryption technique is used to protect the user's sensitive data (i.e. data- which is stored on the device or the data when transferred through a network.) It is sure that the user sensitive data will be sent only to the intended person who can decrypt the encrypted message (using the private key). In [12], the current research efforts towards Mobile Computing have been reviewed. The author presented several challenges for the design of MCC services. A concept model has been proposed to analyze related research work. Then, the recent MCC architecture, application partition and

offloading, and context-aware services have been surveyed. In [15], the author explored energy efficiency of mobile devices when transferring data securely over various communication networks including high-speed 4G networks such as LTE and Wibro.

A new platform is described in [2], known as Hyrax. It has been derived from Hadoop that supports cloud computing on Android smart phones. Hyrax allows client applications to conveniently utilize data and execute computing jobs on the networks of smart phones and heterogeneous networks of phones and servers. Hyrax allows applications to use distributed resources abstractly, oblivious to the physical nature of the cloud. In [3], CloudExp, a modeling and simulation environment for cloud computing has been introduced. It can be used to evaluate a wide spectrum of cloud components such as the processing elements, data centers, storage, networking, web-based applications. In [14], a large scale BANs system in the presence of cloudlet-based data collection is presented. The objective is to minimize end-to-end packet cost by dynamically choosing data collection to cloud using cloudlet based system.

Many literatures [1,10,11,13], presented location management in wireless network. In [1], mobility support and management in mobile cloud computing systems has been focused based on the cloudlet approach. The cloudlets will be placed in many common areas, such as coffee shops, universities and airports. A mobile user is able to use the services of the nearest cloudlet that covers limited area to provide the services such as storing, processing, content delivery. But, proper information about the mobile device's recent location if it is moving away from the range of the cloudlet is required to achieve this goal. A possible technique can be the infrastructure based methods- that uses technology such as Wi-Fi with GPS. It becomes a key point to monitor the context of current user's location, when the cloudlet's user going out of the range. In such case, connection should be dynamically adapted for the contexts to keep the job progress while any moves of cloudlet members. For keeping the connection on to the mobile device, an ad-hoc network among the cloudlets will be created. So that the mobile device users will offload their workloads to the cloudlets and receive the computation results while moving from the network of one cloudlet to another. In [17], comparison of the performance of multi-hop wireless ad-hoc network routing protocols has been done. It was concluded that Destination-Sequenced Distance Vector (DSDV) is good with low mobility. Temporally-Ordered Routing Algorithm (TORA) has large overhead. So it fails to converge with more sources. Dynamic Source Routing (DSR) is very good at all the rates of speed, but has large packet overhead. Ad-hoc On Demand Distance Vector (AODV) is almost as good as DSR, but has more transmission overhead. In [18], Ad-hoc On Demand Distance Vector (AODV) is a Reactive Routing Protocol that acts in response on demand. AODV is an advancement of Dynamic Sequence Distance Vector protocol. It facilitates multi-node, dynamic routing and self-starting in MANET environment . It never generates close loop in the routing table of any mobile node because of the idea of generated sequence number counter. AODV Sequence numbers provide as time stamps protocol and agree to mobile nodes to compare how new packet information reached to other nodes in the MANET architecture.

3. THE PROPOSED MODEL ARCHITECTURE

The work undertaken focuses on the secure data transfer in ad-hoc mobile cloud computing network based on cloudlet approach. All the cloudlets have the same role i.e. to provide the services to the mobile users.

3.1 Problem Analysis

A cloudlet is a resource rich server placed in common regions to provide the services to the thin clients (mobile nodes) when required.

Figure 1: Insecure Data Transfer Between Cloudlet and Mobile Devices

When the mobile device gets connected to the nearby cloudlet, it offloads its data to the cloudlet to perform the tasks when such kind of requirement occurs. Since the mobile device has limited resource availability, the mobile device gets benefit of the cloudlet. The mobile device will get the result of the task performed even when it goes out of range of the current cloudlet network. But, there is lack of data transfer security. So, the security in data transmission has to be achieved.

3.2 Model Architecture

Each cloudlet is able to establish a connection with other cloudlet using the Ad-hoc On Demand Distance Vector (AODV) routing protocol in this architecture. The cloudlets are capable to provide the services to the mobile devices as per their requirement even when the mobile devices are moving from one network to other network. Figure 3.1 shows the components of the cloudlet network.

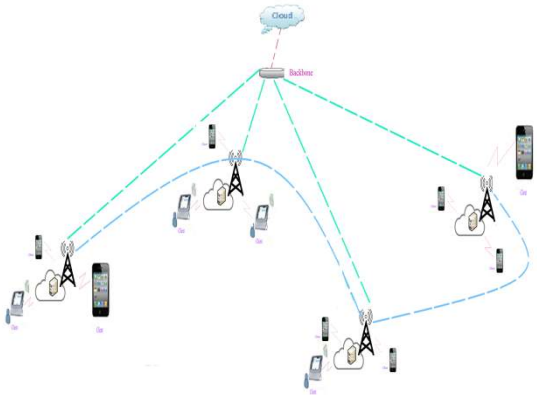

Figure 3.1: Ad-hoc Cloudlet Network

This network includes the following components:

- An enterprise cloud (3G connection).
- Cloudlets are connected to each other in high bandwidth wireless communication (Wi-Max).
- Mobile devices (laptops, smart phones, tablets) connected to a cloudlet in high bandwidth wireless Communication (Wi-Fi).

The proposed model Architecture consists of number of cloudlets situated in common areas associated with several mobile nodes. Each cloudlet which is a fixed entity, presents services for any around mobile device. All the cloudlets are connected to the enterprise cloud. According to the needs of the mobile devices, they can offload their jobs to be processed by any nearby cloudlet. There will be number of nodes with diversed tasks in the cloudlet network. Each mobile node will be connected to the cloudlet with high bandwidth wireless functionality via wireless links. For the movement of the mobile nodes, Random Way Point (RWP) mobility mechanism has been used.

The routing information will be swapped among the cloudlets by making the use of Ad-hoc On Demand Distance Vector (AODV) routing protocol. Cloudlets will update their routing tables when a mobile node joins or leaves the cloudlet network. Only those mobile nodes will be registered by the cloudlet, that will request to the cloudlet to offload their workload.

There are two kinds of situations that can take place. In the first situation, the mobile node will remain in the same cloudlet network to which it offloaded its job. Then, the cloudlet after processing the job will send the result to the intended mobile node. This is also called the traditional approach. In the second type of situation, the mobile node offloads its data to the cloudlet to be processed and leaves the network while the cloudlet is processing its job. Thus, the mobile node goes out of the range without receiving the result. This

cloudlet will perform the computation and stores the result, if it does not find the mobile node in its network range which made the request. The mobile node reaches in the range of another cloudlet's network range. When the node requires the offloaded job results, then in which cloudlet's network it is present, it requests to that cloudlet for the result. This cloudlet after updating its routing table, sends to the other cloudlets. The other cloudlets will check the mobile node ids if they have any stored result of the mobile nodes' id which are present in received routing table. Now the cloudlet which stored the result of the mobile node request will respond to the cloudlet with the result. Then, the mobile node will receive the result from the corresponding cloudlet. An additional component for secure data transfer is to be added in the cloudlet.

4. ADDITIONAL COMPONENTS OF THE CLOUDLET

There are three additional components of the cloudlet have been assumed : Security handler, job handler, and context handler as in Figure 4.1. Since the main focus is on the secure data transfer issue in mobile cloud computing model, this model is based on the security handler part with respect to other components' benefits.

Figure 4.1: Additional Components of the Cloudlet.

Security handler

- Creates secure connections between the mobile devices and cloudlet.
- Performs encryption of the data that has to be transferred.

Context handler

- Maintains connections and communicates with the mobile devices.
- Monitors the mobile nodes entering or leaving the coverage area.

Job handler

- Partitions the application and data set required into separated subtasks.
- Returns the result of each subtask to the owner of the job or to the destination cloudlet.

To achieve the data transmission security, hybrid cryptosystem is to be used. So that the user's data can be protected. Hybrid Cryptosystem protocol makes the use of multiple ciphers of different types together, each to it's best advantage. One common approach is to generate a random secret key for a symmetric cipher, and then encrypt this key via an asymmetric cipher using the recipient's public key. In this paper, we are making the use of cloudlet approach. It is based on the client server model, where a mobile device will act as a client and the cloudlet will act as the server.

The secure data transfer will be achieved by the following steps:

- The mobile node, that has to access the cloudlet so as to offload its workload on it, sends request to the cloudlet.
- The cloudlet generates a public /
- private key pair for the client.
- The server also has a few public / private key pairs.
- The cloudlet sends its own public key and the public / private key pair generated for the client to the user.
- Thus the user will get registered to the cloudlet.

The user will now encrypt the symmetric key by using the public key of the cloudlet and the workload that has to be offloaded will be encrypted by the symmetric key.

Both encrypted key and data will be sent to the cloudlet.

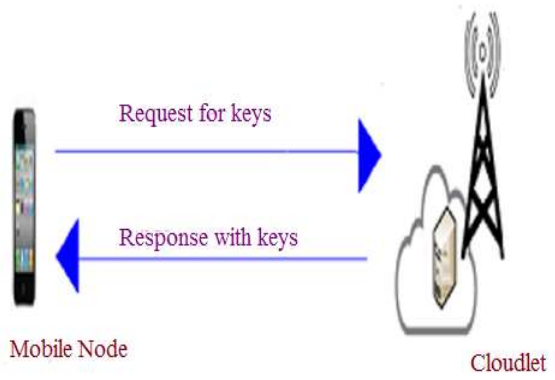

Figure 4.2: Registration of the Mobile Node.

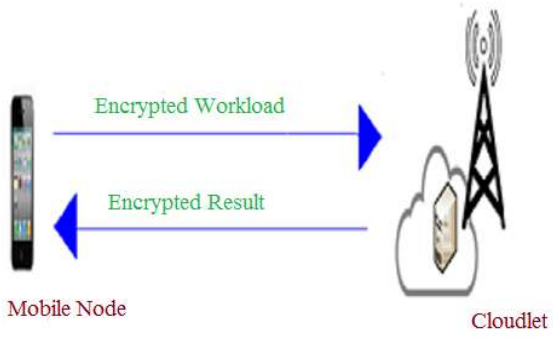

Figure 4.3: Secure Data Transfer between the Mobile Node and Cloudlet.

- The cloudlet will decrypt the encrypted symmetric key with it's private key.
- With the help of this symmetric key the encrypted offloaded data will be decrypted.
- The cloudlet now performs the requested tasks.
- The cloudlet sends the result to the mobile node after processing the requested job.
- Cloudlet will encrypt it's symmetric key by using the public key of the user and processed data will be encrypted by this symmetric key.
- Both encrypted key and data will be sent to the user.
- The user will receive the result and decrypt it.
- Secure data transfer will be achieved in this way.

5. CONCLUSION

The proposed model presents secure data transfer in Mobile Cloud Computing scenario which makes the use of cloudlet as service provider. Random Way Point (RWP) and Ad-hoc On Demand Distance Vector (AODV) routing protocol have been used for mobility management and communication among cloudlets respectively. The mobile device encrypts the workload with the help of hybrid cryptosystem and offloads the encrypted data to the cloudlets to perform its task. The cloudlet returns the processed data to the mobile user in encrypted form. Thus, the model achieves secure data transfer between mobile device and the cloudlet.

REFERENCES:

[1] Mohammad AL-Rousan, Elham AL-Shara, Yaser Jararweh, "AMCC: Ad-hoc based Mobile Cloud Computing Modeling". The International Workshop on Ntworking Algorithms and Technologie for IoT (NAT-IoT2015). Procedia Computer Science 56(2015)580-585. URL:www.sciencedirect.co.

[2] Marinelli, E.E.. Hyrax: cloud computing on mobile devices using mapreduce. Tech. Rep.; DTIC Document; 2009.

[3] Jaraweh Y., Jarrah M., Kharbutli M., Alshara Z., Alsaleh, M.N., Al-Ayyoub, M.. Cloudexp: A comprehensive cloud computing experimental framework. *Simulation Modelling Practice and Theory* 2014;49(0):180 – 192.doi:http://dx.doi.org/10.1016/j.simpat.2014.09.003.

[4] Communications, Z.. Zte corporation. a survey of mobile cloud computing. 2011.

[5] Kovachev, D., Renzel, D., Klamma, R., Cao, Y. Mobile Community cloud computing: Emerges and evolves. In: *Mobile Data Management (MDM), 2010 Eleventh International Conference on*. 2010 p. 393–395. doi:10.1109/MDM.2010.78.

[6] Satyanarayanan, M., Bahl, P., Caceres, R., Davies, N.. The case for vm-based cloudlets in mobile computing. *Pervasive Computing, IEEE* 2009;8(4):14–23. doi:10.1109/MPRV.2009.82.

[7] Jararweh, Y., Tawalbeh, L., Ababneh, F., Dosari, F.. Resource efficient mobile computing using cloudlet infrastructure. In: *Mobile Ad-hoc and Sensor Networks (MSN), 2013 IEEE Ninth International Conference on*. 2013, p.373–377. doi:10.1109/MSN.2013.75.

[8] Quwaider, M., Jararweh, Y. Cloudlet-based efficient data collection in wireless body area networks. *Simulation Modelling Practice and Theory* 2015;50(0): 57–71.URL: http://www.sciencedirect.com/science/article/pii/S1569190X14001099. doi:http://dx.doi.org/10.1016/j.simpat.2014.06.015;

[9] Jararweh, Y., Tawalbeh, L., Ababneh, F., Khreishah, A., Dosari, F.. Scalable cloudlet-based mobile computing model. *Procedia Computer Science* 2014;34(0):434 – 441. URL: http://www.sciencedirect.com/science/article/pii/S1877050914009065. doi:http://dx.doi.org/10.1016/j.procs.2014.07.051; the 9th International Conference on Future Networks and Communications (FNC'14)

[10] Bajad, R.A., Srivastava, M., Sinha, A.. Survey on mobile cloud computing. *International Journal of Engineering Sciences & Emerging Technologies* 2012;1(2):8–19.

[11] Fernando, N., Loke, S,W., Rahayu, W. Mobile cloud computing: A survey. *Future Generation Computer Systems* 2013;29(1): 84–106.URL: http://www.sciencedirect.com/science/article/pii/S0167739X12001318. doi:http://dx.doi.org/10.1016/j.future.2012.05.023;

[12] Guan, L., Ke, X., Song, J.. A survey of Research on mobile cloud computing. *Computer and Information Science, ACIS International Conference on* 2011;0:387–392.

[13] Altamimi, M., Naik, K.. The concept of a mobile cloud computing to reduce energy cost of smart phones and its systems. In: Kranzlmller, D., Toja, A., editors. *Information and Communication on Technology for The Fight against Global Warming*; vol. 6868 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg. ISBN 978-3-642-23446-0; 2011,p. 79–86. URL: http://dx.doi.org/10.1007/978-3- 64223447-7- 8. doi:10.1007/978-3-642-23447-7-8.

[14] Quwaider, M., Jararweh, Y..Cloudlet-based for big data collection in body area networks. In: *Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for*. 2013, p. 137–141. doi:10.1109/ICITST.2013.6750178.

[15] Hong, J.a., Seo, S., Kim, N., Lee, B.D.. A study of secure data

transmissions in mobile cloud computing from the energy consumption side. In: *Information* Networking *(ICOIN), 2013 International Conference on*. 2013, p. 250–255. doi:10.1109/ ICOIN.2013.6496385.

[16] Broch J., Maltz D.A., Johnson, D.B. Hu,Y.C. Jetcheva, J.. A Performance comparison of multi-hop wireless ad-hoc network routing protocols. In: *Proceedings of the 4th Annual ACM/ IEEE International Conference on Mobile Computing and Networking*; Mobi-Com '98. New York, NY, USA: ACM. ISBN 1-58113-035-X; 1998, p. 85–97. URL: http:// doi.acm.org 10.1145/288235.288256. doi:10.1145/288235.288256.

[17] Ahmad A., Huda M., Mohd Kaleem A., Maurya R.. Mobile Ad-Hoc Networks: AODV Routing Protocol Perspective. International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE) *Vol. 4, December 2015.*