International Journal of Pure and Applied Mathematics
Volume 117 No. 15 2017, 355-367
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Exploration of the Authenticity and Data Integrity in Cloudlet Environment Using Security Agent

[1]P. Thinakaran, [2]K. Sindhanaiselvan, [3]J. Mannar Mannan and
[4]K. Mahalakshmi
[1]Department of Information Technology,
Karpagam College of Engineering,
Coimbatore, Tamilnadu, India.
thina04@gmail.com
[2]Department of Computer Science and Engineering,
M.Kumarasamy College of Engineering,
Karur, Tamilnadu, India.
sindhanai@gmail.com
[3]Department of Information Technology,
Karpagam College of Engineering,
Coimbatore, Tamilnadu, India.
endeavour6381@yahoo.co.in
[4]Department of Information Technology
Karpagam College of Engineering,
Coimbatore, Tamilnadu, India.
prof.dr.mlk@gmail.com

Abstract

In this IT world, Mobile Cloud computing has become a dynamic area of research. It provides a large space for modern smart phones to get connected through private or public networks. Mobile Cloud Computing is a combination of Cloud Computing and Mobile Computing. Due to the advancement in Cloud computing and Mobile Computing the MCC is in a position to provide a sophisticated environment for mobile applications which makes the public to feel more comfortable with their handheld devices. Due to the widespread traffic in the Wide Area Network, the user benefits in getting of Cloud Services become more and more complicated.

The security in transferring data among the cloud also seems to be in a critical position, with that the level of customer satisfaction is also become crucial. However there are many advantages in using MCC, Cloudlet is introduced to reduce the traffic in the cloud. Cloudlet makes the cloud server to come closer to the handheld devices, by this some disadvantages in using MCC is gets reduced. In this paper we are going to explore the authenticity and the integrity of data in cloudlet environment. For monitoring the data transfer between the cloudlets and smart phones and vice versa. and to tighten up the integrity for the data transferred a Security Agent concept was proposed. The security agent as the middleman takes over the control of the entire workings in the cloudlet environment. In support to the working RSA algorithm concept was implemented to enrich the security for the data. By this the user can offload his/her handheld device applications in the nearby cloud through the LAN and get the work done in a quick span of time with the data integrity.

Key Words: Cloud computing, clone cloud, clone computing, mobile computing, mobile cloud computing, cloudlet.

1. Introduction

For the meticulous working on some mobile applications the user must concentrate on the DIL [1] (disconnected, interrupted, low bandwidth) environment. The user relies on the cloud and mobile computing to provide the required environment to perform their operations within an expected time. Due to the advancement in the smart phones they planned to accomplish their task within a stipulated period of time. But in the reality the computational speed and the capacity of the handheld devices may not match for the customer expectation. This is mainly due to the disconnection of the mobile networks, isolating of more space by many users etc, Even though the users are ready to spend their money for their compatibility, their expectation is not get satisfied with the operations of the mobile applications. Offloading the mobile application computation becomes vital for the effective working of the mobile. Here, the Clone cloud comes in to the act. It duplicates the mobile image and most of the mobile application operations are done virtually in the cloud and send the results to the mobile, so that the mobile can work faster than ever. This computing technology seems to be a greater mile stone for the mobile industry and the user. Henceforth the user gets satisfied with the working of his/her handheld devices. The main limitations of the Clone Cloud are handover delay, bandwidth limitation etc., Even though the clone cloud provides good environment to work, the availability of the mobile signals are depends on the user network. Due to the mobility some time both the base stations and the user cannot assure the same speed of data transmission. To uphold these limitations the cloudlet (a small cloud) get introduced in to the act. The handheld devices use the local area network for their processing between cloudlet. By this the network traffic get reduced and the computation speed of the user applications are also get increased and the user can attain their task. Being more cloudlets are available in the network, users are in a position to identify the appropriate cloudlet before sending the data and he also in a position to check the originality of the data send. Thus in order to solve the mentioned challenges, the authenticity of the cloudlet must be checked before the data is send and the integrity of the data is also verified after it reaches the appropriate cloudlet. This work can be coined by implementing a thirty party auditor, who stands between the user and the cloudlet and transfer the data between them.

2. Related Fields

Due to the emergence of the offloading concepts the cloudlet shares one of the best components in the mobile cloud computing environment. In this chapter we are going to discuss about the primary concepts which are intimate for the offloading operations.

Mobile cloud computing is a technology which emerges from combination of cloud computing and mobile computing for the smooth operations of the mobile applications in this cyber world. From another perspective MCC can also be a

combination of mobile computing with the wireless networks. In 2010, Google CEO Eric Schmidt explained mobile cloud computing that 'based on the cloud service development, mobile phones will become a complicated and evolve to be a portable super computer in the future' [2]. Some distinct characteristics of hosted applications makes the mobile cloud different from other types of computing.MCC tries to overcome the fundamental limitations (like bandwidth, battery life etc.,)faced by the mobile in its environment[4]. It also finds difficult to maintain same range of connectivity across different mechanism [5]. Mobile applications when using the mobile cloud seems to be more sensitive on network latency than the regular cloud or mobile computing. MCC maintains the cross platform functionality effectively and gives an enrich experience to the end user. Henceforth the end user experience is treated with the high priority and it should not be let down due to some network latency. So.MCC must be in such a position to support distance matrices. Due to the limited energy in handheld devices, the mobile cloud should take some responsibility of doing some complicated functions on the cloud itself. Due to the advancement in the smart phones, nowadays, mobile cloud computing is becoming the disruptive force for other technologies. The main constraint for the mobile device is their own resources. Normally the capacity of the smart phones will differ from device to device. The capacity includes its processing power, operating system, memory, screen size, sensing technology etc., Due to the advancement in the innovation in this environment the mobiles technology gets its update in daily. The handling of some complicated applications will limit the computing capability of the mobile resources. In some environment, the smart phones still faces a limitation when it is compared with the computing capacity of PCs and Laptops. Due to the development of interactive applications, sensing technology the battery gets drained adequately. Nowadays the mobile users face this as a serious problem. It is a time to take constant steps to get out from these limitations. By B. Chun, Clone Cloud system is initiated [3] in 2011. The main functionality is to transfer the some function of the smart phone to the cloud with the help of device configuration using virtual machine migration technology. With this technology the smart phones can offload its complicated application process to the clone cloud for the effective operation and time consumption. By this activity the half or even full process of the mobile phones is get reduced and the operations are carried over in the distributed environment. The battery life and the capabilities of the mobile phones can also expand[13] By this transfer of the application the user can get the same feel of working in a smart phone with no time delay. Figure 1 shows the clone cloud system model. Being the Clone cloud work directly with the cloud server the mobile process seems to be healthier than the previous workings. The users get the good feel for using the handheld devices like smart phones, PDAs etc. Even though with the limited processing energy the mobile phone can complete some unforeseen workings.

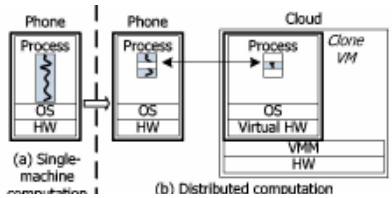

Fig. 1: Clone Cloud System Model [3]

3. Cloudlet

In this cloudy world, there is an enormous difference between the using of the mobile cloud for mobile apps than using the normal cloud. Nowadays mobile apps predominantly depend on mobile cloud. Mobile cloud seems to be a safe arena for the implementation of mobile apps. With the usage of mobile cloud the reliability and fault tolerant will gets increased for the mobile apps. To overcome the drawbacks faced by the mobiles devices than PCs and laptops like processing time, battery usage etc., and mobile cloud gets into the act. In MCC, when the user or the developer plans to run the cross platform mobile application, they purely depend only on the cloud for all the functionality. Mobile cloud exposed the usage of real data when ever and where ever it is required by the mobile user. Flexibility of using data becomes a counterpart by using the mobile cloud. by this the apps can be deployed remotely. With a help of the clone cloud, MCC off-load the workings of some mobile applications by having a maximum process in the cloud itself. By this the performance of the mobile is get increased. There may be some limitations in working with the clone cloud. Even though the processing of the mobile applications increased comparatively in clone cloud there are some disadvantages prevails in clone cloud. They may be handover delay, bandwidth limitation etc.During transient of the user, a well know fact is that the data transmission speed between the smart phones and the base stations is not in a consistent manner i.e. it will change according to the situation. Consequently, the Clone Cloud will not be available if mobile users walk in the signal's blind zone. To reduce these types of problems in the clone cloud, the user wants to share the workings of the smart phones applications in a server near to their network. Sharing the mobile applications in the big cloud and communicating through the huge WAN creates many troubles.

Cloudlet is a concept which is introduced to offload the mobile applications workings through a near LAN network. It is appear to be a small cloud located nearby the mobile users[8] and their smart phones are get connected through LAN network which in turn connected with the clouds located far away [7]. Cloudlet seems to be an architectural element that comes from the combination of cloud computing and mobile computing [12]. Cloudlet is seems to be a resource enriched trusted computer(s) connected on the trusted network, by which it has the excellent connectivity in the network [6]. The software are run in the cloudlet and the handheld devices are become a thin client during the

processing. In general cloud, the user wants to communicate with the available WAN network, which sometime decreases the processing capacity of the smart phones and the user are not in a position to uphold the actual ability of the devices what they have. So the process of some applications which uses more GUI functionality like video games faces the same type of the problem. Due to the centralized ownership in handling all the applications in the cloud seems to be more composite. So cloudlet decentralized the ownership according the requirement of the user.

4. Cloudlet Architecture

The cloudlet works under a 3 tier architecture in which first layer from the base is a mobile device which are connected with the individual cloudlet which is works as a second layer, the third and the final layer is the central core i.e. the base cloud. This architecture explains the way by how the smart phones off load its working to the next cloudlet layer. The mobile phones get connected with the nearest cloudlet through the LAN network within turns get connected with the central cloud.

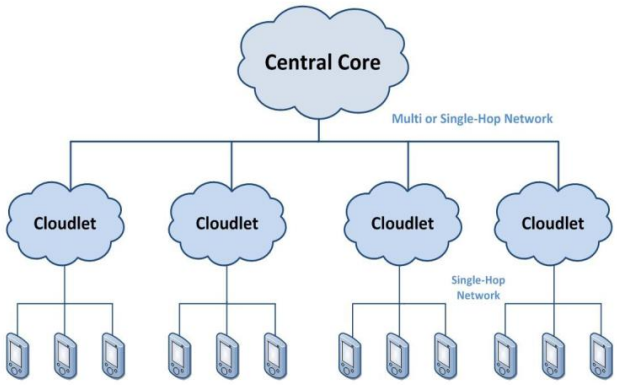

Fig. 2: 3 Tier Architecture: Mobile Device, Cloudlet , Central Core(Cloud)

The central core is from any one of the Microsoft cloud, Google data centre or any private based cloud centers. Due to the nearest communication or single – hop network this architecture reduce the latency [9] and also lowers the battery consumption by using the Wi-Fi. Cloudlet works on the concepts of Virtual Machine (VM). The client can offload its workings with the cloudlet through a virtual machine. The virtual machine works like a original or dedicated machine to gives the same experience to the user. Disconnect of the network may not be possible in the cloudlet because the mobile application can locate to the different cloudlet and tries to complete its work in short span of time[10].

5. Data Authenticity and Integrity on Cloudlet

In mobile cloud computing the data security plays a dominant role. The mobile cloud is in a position to safe guard the sensitive data stored by the users. The MCC should take more steps to protect the data stored by the users. In the mobile world, the mobile apps depends on the mobile cloud to destruct the pitfalls in mobile network latencies, unreliability connectivity etc.,The cloudlet is an emerging computing platform where the application can execute over the linked small cloud servers through the LAN network rather than the big cloud. Due to the cloudlet functionality the user's handheld devices can offload the typical application execution in the cloudlet and make the mobiles as a thin client. The cloudlet can be defined as the process of utilization of computing resources over the known network. Even though it provides a better functionality than the regular cloud, there are some pitfalls in the security provided to the data. So there must be some substantiate measures for the data transfer in the cloudlet [11]. Two basic works to be done for the better workings of the cloudlet are i) authenticity and ii) integrity. Authenticity is finding the right cloudlet for the transfer of the data for the computation and the second one is the checking the reliability of the data sends to the cloudlet for computation. Encryption and Decryption concepts should be implemented while transferring of the data from cloudlet to the client or vice versa. In cloudlet environment the local cloud and the handheld devices must become a companion and should establish a know environment before passing or offloading or sharing the applications among them for the operations. The cloudlet must know that the data received is from the right device and the mobile device is also should be in a position to judge its application is offloaded to the right cloudlet which is more suitable for its operations. After this genuine check only the expected operations can be done in a quick succession so that the latency is reduced and the proper or expected output can be achieved. In this paper we have proposed a concept called Third Auditor / Security Tactic Agent, who is solely responsible for the workings of the judging the right cloudlet for the mobile application before offloading the process and also responsible for the integrity of the data send to the cloudlet. Cloudlets may be of many for the each available domains. For e.g. many Cloud Service Providers (CSPs) may provide a cloudlet for each required domain. So the user can easily communicate with their domain specific cloudlets. The Security Agent is going to be the authority for the communication of data between the user and the required cloudlet. To regularize the working activity the security agent will maintain a Allotment Table, which in turns going to regulate the allotment of data communication between the cloudlet and the user.

Table 1: Allotment Table

S.NO	Cloudlet Unique ID	Cloudlet Name	Domain Name	User Unique ID	MAC Address	Time slot

As shown in the **Table 1** the SA will create a table with the mentioned fields for the operations in the cloudlet environment. As the first level, in the allotment table, the security agent will maintain the list of cloudlets according to their domain specific and also gives a unique id for the cloudlet. Then when the handheld device (PDA, Mobile etc)., is planned to send or offload its application , It should communicate with the security agent by sending a message that they are ready to communicate with the appropriate cloudlet. The security agent maps the MAC address of the device and also checks the availability of the cloudlet as per its requirement specific. After the identification of the proper cloudlet, security agent sends the MAC address of the handheld devices and cloudlet unique id to the cloudlet and the handheld devices respectively. The cloudlet allocation for the handheld devices is done dynamically according to the availability of the cloudlet.

The security agent maintains all its allotment in the allotment table as mentioned. It also fix the time frame for the completion of the allotted task. By this action the latency can also be cross verified By this activity of the security agent , the handheld devices know which cloudlet it is communicate or it offload its application for the computation and vice versa. By this activity the cloudlet and the handheld devices become a companion for sharing of their resources. As at this level the security agent's foremost perception of authenticity is maintained. In case of any miscommunication or unexpected interrupt during the process the security agent hold the key role to select the cloudlet dynamically and it does the above mentioned working without wasting the time. The workings is mentioned in Fig3

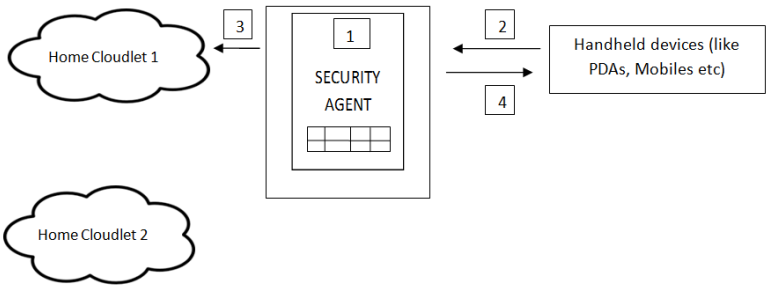

Fig. 3: Security Agent Data Authenticity

Working Architecture as the First Level-Security Agent Data Authenticity

1. Security agent creates the allotment table and maintains the available cloudlet details and gives unique ID. and also checks the availability of the cloudlet as per the required domain by the handheld devices.

2. Hand held devices sending their ready status to offload the application to the security agent. The security agent maps the MAC address of the handheld devices and save it in the allotment table.
3. The Security agent sends the MAC address of the handheld devices to the cloudlet
4. The Security agent sends the cloudlet unique id to the handheld devices.

As the second level for checking the integrity of the data transferred between the handheld devices and the cloudlet the RSA encryption and decryption technique was introduced. This entire activity is monitored by the security agent. After allotting the respected cloudlet to the applications, the security agent creates the dynamic public key and sends it to the handheld devices. The handheld devices in turns encrypt the data with the public key and send it to the respective cloudlet. Being the unique id of the cloudlet is maintained by security agent, it is easy for the handheld devices to send the encrypted data to the particular cloudlet.

The security agent gives a dynamic private key to the respective cloudlet to decrypt the data send by the handheld devices. The cloudlet with this private key decrypts the data and run the process and also sends an acknowledgement message to the security agent. With this key concept the security agent, mobile device and the cloudlet can confirm that the original data is exchanged among them. The security agent maintains the timings for the each process to complete. As the third level, after completion of the process the cloudlet handover the details to the handheld devices and does the same type of operations as mentioned in reverse. The entire workings are explained in the Fig. 4 and Fig.5.

Working Architecture as Second Level- Sending Encrypted Data from Handheld Devices to Cloudlet

1. Security agent sends the dynamically created Public key to the Handheld devices.
2. Handheld devices encrypting the data with the available public key.
3. Handheld devices -Sending encrypt data to the respective Cloudlet.
4. Security agent sends the dynamically created private key to the Cloudlet.
5. Cloudlet decrypt the data received from the Handheld devices using the private key.
6. Cloudlet sends the acknowledgement to the Security agent, which in turns help the Security agent to maintain the time slot.

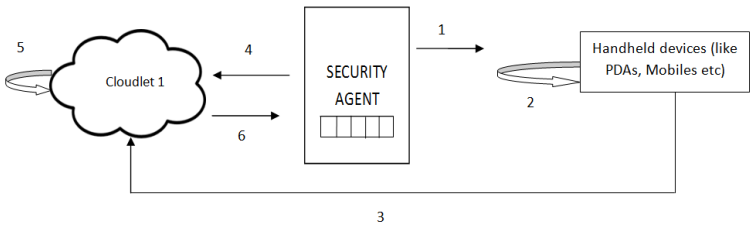

Fig. 4: Sending Encrypted Data from Handheld Devices to Cloudlet1

Working Architecture as Third Level - Sending encrypted data from Cloudlet to Handheld Devices

1. Security agent sends the dynamically created Public key to the Cloudlet.
2. Cloudlet encrypting the data with the available public key.
3. Cloudlet -Sending encrypt data to the respective handheld devices.
4. Security agent sends the dynamically created private key to the Hand held devices.
5. Handheld devices decrypt the data received from the Cloudlet using the private key.
6. Handheld devices send the acknowledgement to the Security agent, which in turns help the Security agent to maintain the time slot.

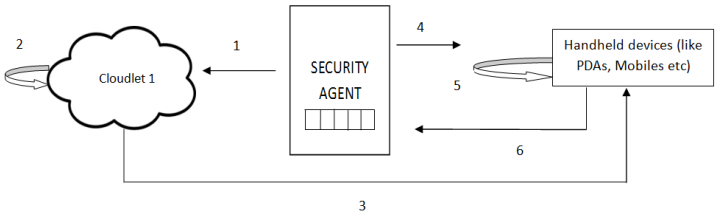

Fig. 5: Sending Encrypted Data from Cloudlet to Handheld Devices

6. Conclusion

Cloudlet is one of the technologies which bring the handheld devices close to the internet. The user can get connected through the LAN network. Due to the nearest connectivity the time duration taken for the operation is seems to be less than that is taken by the general cloud through WAN. Due to the low bandwidth, computation speed, battery power the user can off load the execution of their handheld devices application operations to the nearest cloudlet. Here the user can get the things done with the high speed operation of the cloud with a time slot. So latency problem is also solved. Even though the computation is very quick in the cloudlet, security for the data seems to be the major issue. The cloudlet wants to know from which device it going to connect and vice versa So a companion link should be implemented before sending the data to the cloudlet with the handheld devices and the data should contain a security check. In this paper we discussed about the security agent who stands between the cloudlet and the user. Before sending the data to the cloudlet the agent maintain a allotment table in which the allocation of the work can be regulated. With the RSA encryption and decryption standard the data send between the cloudlet and the user handheld devices are regulated for the integrity. By this the security agent can give two levels of security that is authenticity for the better communication and integrity for the data send over the network. The time allotment for the work can also be monitored through the allotment table. With this the data transferred in the cloudlet environment can attain a safe state.

References

[1] Lewis G., Echeverría S., Simanta S., Bradshaw B., Root J., Tactical cloudlets: Moving cloud computing to the edge, Military Communications Conference (MILCOM) (2014), 1440-1446.

[2] Marrapese B., Google ceo: a few years later, the mobile phone becomes a super computer. [Online]. Available: http://www.itnews-blog.com/it/21320.html

[3] Chun B., Ihm S., Maniatis P., Naik M., Patti A., Clonecloud: Elastic execution between mobile device and cloud, Proceedings of the sixth conference on Computer systems ACM (2011), 301–314.

[4] Change R., Gao J., Gruhan V., He J., Roussor G., Tsai W., Mobile Cloud Computing Research–Issues, Challenges, and Needs, 7th International Symposium on Service-Oriented System Engineering (2013).

[5] Allam H., Nassiri N., Rajan A., Ahmad J., A critical overview of latest challenges and solutions of Mobile Cloud Computing, Second International Conference on Fog and Mobile Edge Computing (FMEC) (2017), 225-229.

[6] Satyanarayanan M., Gahl P., Cacores R., Davis N., The Case for VM-Based Cloudlets in Mobile Computing, IEEE Pervasive Computing 8(4) (2009), 14-23.

[7] Koukoumidis E., Lymberopoulos D., Strauss K., Liu J., Burger D., Pocket cloudlets, ACM SIGPLANNotices 47(4) (2012), 171–184.

[8] Verbelen T., Simoens P., De Turck F., Dhoedt B., Cloudlets: Bringing the cloud to the mobile user, Proceedings of the third ACM workshop on Mobile cloud computing and services ACM (2012), 29–36.

[9] Cuervo E., Balasubramanian A., Cho D.K., Wolman A., Saroiu S., Chandra R., Bahl P., Maui: making smartphones last longer with code offload, Proceedings of the 8th international conference on Mobile systems, applications, and services. ACM (2010), 49–62.

[10] Bahtovski A., Gusev M., Cloudlet Challenges, 24th DAAAM International Symposium on Intelligent Manufacturing and Automation (2013).

[11] Ioana L., Juric O., Krivale L., Aloso G., Calling the Cloud: Enabling Mobile Phones as Interfaces to Cloud Applications, I Bacon J.M., Cooper B.F.(eds) Middleware, Lecture Notes in Computer Science (2009).

[12] Jaiswal A.S., Thakare V.M., Sherekar S.S., Performance based Analysis of Cloudlet Architectures in Mobile Cloud Computing, International Journal of Computer Application, National Conference on Recent Trends in Information Security (2015).

[13] Lima D., Miranda H., Taïani F., Towards a new model for cyber foraging, Proceedings of the 13th Workshop on Adaptive and Reflective Middleware (2014).

[14] RAJESH, M. "A SYSTEMATIC REVIEW OF CLOUD SECURITY CHALLENGES IN HIGHER EDUCATION." The Online Journal of Distance Education and e-Learning 5.4 (2017): 1.

[15] Rajesh, M., and J. M. Gnanasekar. "Protected Routing in Wireless Sensor Networks: A study on Aimed at Circulation." Computer Engineering and Intelligent Systems 6.8: 24-26.

[16] Rajesh, M., and J. M. Gnanasekar. "Congestion control in heterogeneous WANET using FRCC." Journal of Chemical and Pharmaceutical Sciences ISSN 974 (2015): 2115.

[17] Rajesh, M., and J. M. Gnanasekar. "Hop-by-hop Channel-Alert Routing to Congestion Control in Wireless Sensor Networks." Control Theory and Informatics 5.4 (2015): 1-11.

[18] Rajesh, M., and J. M. Gnanasekar. "Multiple-Client Information Administration via Forceful Database Prototype Design (FDPD)." IJRESTS 1.1 (2015): 1-6.

[19] Rajesh, M. "Control Plan transmit to Congestion Control for AdHoc Networks." Universal Journal of Management & Information Technology (UJMIT) 1 (2016): 8-11.

[20] Rajesh, M., and J. M. Gnanasekar. "Consistently neighbor detection for MANET." Communication and Electronics Systems (ICCES), International Conference on. IEEE, 2016.