Mobile Ad-hoc Cloud Architecture and Security

Sonam Agnihotri[1], Nidhi Chahal[2]
[1]*Student of Department of electronics and communication*
[2]*Faculty of Department of electronics and communication*
Chandigarh Engineering College, Landran, Mohali

Abstract- Explosive growth in capabilities of mobile devices and concept of mobile cloud computing together raised a potential technology called mobile ad-hoc cloud. MAC aims to provide more efficient, economic and constant availability of services. In this paper we discussed the various technologies involved in formation of MAC. We analysed the various challenges and threats in the implementation of this technology. This paper discussed the similar works in this area. Finally we proposed a general management architecture in which we introduced and discussed various interfaces, their execution process and their objectives. We also developed a security framework to facilitate prevention measures and defence structure for secure and trusted network of MAC.

Keywords- Mobile ad-hoc cloud, management architecture, security, node management, task distribution

I. INTRODUCTION

The mobile devices are become more proficient in their computing ability as the demand of miniaturisation increases. In this new era, Smartphones and mobile devices have greatly influenced the daily lives of almost every person. The growing capabilities of the mobile devices and cloud computing leads to the rise of mobile cloud computing. Despite of growth in technologies of mobile devices they still lack in some areas like battery power, network bandwidth and processing power. These limitations cause hindrance in the processing of application includes intensive computation. The solution of such difficulties is overwhelmed by using mobile cloud computing. Mobile cloud computing is a process in which mobile devices rely on cloud computing services for both data processing and data storage [1]. The mobile application directs the required data to the powerful and centralized servers in the cloud and receives the results of processed data. MCC have several advantages like increased battery life, improved storage capacities, better processing power, scalability, ease of integration and moreover the MCC provides reliability. Despite of all these advantages MCC faces some limitations. In case of MCC, availability is an important factor. Due to weak network connection or in no service situation the connectivity with the cloud becomes impossible. To overcome the problem of availability a new concept of computing comes into role that is mobile ad-hoc cloud computing. This an approach to club the concept of cloud computing and properties of mobile ad-hoc network. In accordance with the perception of S. Giordano [2] mobile ad-hoc network is self-configuring and completely independent of any authority and infrastructure, which is of great use. Mobile ad-hoc cloud computing is a way to harvest under-utilized resources of mobile devices. Several aspects of mobile cloud computing is been discussed by N. Fernando [3]. Despite of several researches and studies mobile ad-hoc cloud is in early stages. This paper presents the comprehensive survey on MAC including definition, architecture and related work towards same technology, various challenges and threats, management architecture and security framework.

II. TECHNOLOGIES INVOLVED IN EVOLUTION OF MOBILE AD-HOC CLOUD

A. Cloud computing

The importance of Cloud Computing is increasing and it is receiving a growing attention in the technical and industrial communities. A study by Gartner [4] considered Cloud Computing as the first among the top 10 most important technologies and with a better prospect in successive years by companies and organizations. Cloud Computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is distributed in three models [4] that is software as service, platform as service and infrastructure as service

Cloud Computing seems as a computational model along with distribution architecture and the main purpose is to provide secure, quick, convenient data storage and computing service, along with computing resources envisioned as services and distributed over the Internet [5]. The cloud develops collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing [6].

B. Ad-hoc cloud computing

Computational power and storage of many enterprises or organisations are often underutilized. Ad-hoc cloud computing is a way to harvest these sporadically, non-exclusively, under-utilized machines. The ad hoc cloud, is infrastructure software is distributed over resources harvested from machines already in use [7]. Ad-hoc cloud computing is a cost effective adaption of cloud services. Ad-hoc cloud is beneficial in many aspects. Number of machines need to be purchased is less, no special infrastructure is required for resilience such as battery backup, cooling systems and redundant power. Power consumption is less in ad-hoc cloud.

Ad-hoc cloud works on a cloudlet approach in which the ad-hoc cloud is a cloud elements, modeller, broker and dispatcher which explain the creation, management and destruction of cloud elements along with that it maintains the quality of system. The concept of A. McGilvery [8] explains the secure cloud jobs running on unreliable cloud clients through V.BONIC. The architecture includes ad-hoc server for job submission and a job distribution from ad-hoc client to guest.

C. Mobile cloud computing

Mobile cloud computing is a technology to attain rich experience of variety of application and services on smart phones. Mobile cloud computing follows the concept of offloading the mobile data to the outside infrastructure. The data storage and processing of the data takes place out in the cloud and result are reverted back to the mobile phones. Christensen [9] explained MCC as powerful combination of SMD capabilities of offloading data and secure processing of cloud computing which offers mobile users to access application and computations over internet. Mobile devices with low capabilities can relish the application indulge with high computational as all the complicated modules can be processed in cloud.

General architecture of MCC is defined by T. Dinh [10] in which mobile devices are connected with central processor through base stations and central processor are further linked with cloud. The request and information is transmitted to the central processor through servers providing network to the mobile user. The request is then forwarded to the cloud through internet. The cloud controllers process the request and provide the service accordingly.

III. RELATED WORK

Researchers in mobile ad-hoc cloud presented their work differently. Shila [11] presented automatic mobile cloud management framework which consist of autonomic cloud element. Autonomic cloud element virtualizes physical resource according to the autonomic control loop which includes monitor, analyse, plan and execute. Each cloud element communicate with each other through embedded common interface. The author presented autonomic cloud elements required to manage the system but lack information on implementation details of various interface. Mobile ad-hoc cloud is still in its early age and due to its highly dynamic nature security becomes a primary concern. K. Murlidhar [12] presents the general requirement for their model 'cloud on the fly' and vision the potential benefits of the model. They proposed the framework to implement the cloud on cluster theory and explained how the model is cost and energy efficient. The author in paper [13] introduces an anonymous on-the-fly secure data exchange protocol for an environment based on paring based cryptography. They proposed the protocol that ensures the secure communication by protecting the data against different attacks such as man-in-middle, target oriented, message manipulation attack and masquerade. This framework considered a particular scenario and worked in a restricted range of healthcare centre.

VI. CHALLENGES OF MOBILE AD-HOC CLOUD

A. Limited power supply

Due to limited energy power and mobility of the nodes the links between the nodes become unreliable. Mobile devices are battery restricted, which can cause several problems. Knowing that nodes are battery restricted they can be target in such a way so that their battery get exhausted, like sending unnecessarily long computations or asking them to provide unnecessary commands further like in DoS (denial of service attack) [14]. In MANET nodes are reliable on each other for communication for direct or indirect contact. Sudden power drain of the devices can cause failure of tasks and failure of communication link.

B. Selfish behaviour of the node

Selfish behaviour of the node can cause a problem where cooperation of nodes are required to perform a task. Selfish behaviour of the node can be due to power failure or the node is deliberately not participating in the task. Node can deliberately withdraw itself before the completion of task. Except the power failure all is considered as selfish behaviour

C. Signal fading

The large buildings and other infrastructure can cause fading of the signal [15] which can cause lag in the processing of the data or even result in the bad communication strength with the other nodes.

D. Mobility of nodes

Due to high speed of nodes, data transfer can be pending. In case of high mobility of nodes complete transfer of data becomes crucial and complex. Due to mobility of the nodes the topology of the network changes constantly. Constant change of the topology leads to the constant change in the routing information. Constant update of routing information at high speed is mandatory.

E. Scalability of network

Heterogeneous nature of the network and lack of global structure raises the issue of scalability. The parameters like number of nodes joining, number of nodes leaving, device parameter like velocity, battery life, processing power should be known. The routing protocols and the services should be compatible with the scale of the network at every instant of time.

F. No centralized management

A network without central management, high mobility and ad-hoc nature is difficult to protect from attacks [16]. In absence of central management it is difficult to study a similar attack with different pattern. The compassionate attacks in such system can become malignant. The compassionate attacks in such network becomes an opportunity for an adversary node to implement a malicious act.

G. Lack of clear boundaries –

Mobile ad-hoc cloud does not have any clear boundaries. Like in traditional way of computing security measures can be taken at the network layer. But the mobile ad-hoc network is

established at an instant of time and any node is free to leave or join the network. The ad-hoc nature of the system doesn't include the clear boundaries due to which proactive or reactive security becomes questioned at network layer.

V. SECURITY THREATS IN MOBILE DA-HOC CLOUD

A. Malicious node –

In ad-hoc network there can be adversary node within the network. The node can share a set of instruction which can infect the services of the targeted nodes. Malicious acts to tamper the established links can be performed. Threats like data tempering and data leakage are more likely to happen in the scenario where adversary node pretends to be some other trustworthy node.

B. Byzantine failure

This failure occurs when a malicious act is performed by a group of nodes [14]. In such case the malicious act become difficult to identify. In this kind of failure they change the routing protocols to generate the incorrect routing information which offer fake links or even overflow other nodes with routing traffic.

C. Denial of service attack (DoS)

This attack aims at the availability of certain node or even the services of the entire ad hoc networks [17]. This act is carried out in a way to overflow the routing path of the nodes by sending unwanted packets. In mobile ad-hoc environment this act can be performed by sending unnecessarily computations which results in the wastage of time and exhausted battery. Due to exhausted battery the node will be unavailable from the network.

D. Eavesdropping

Unsafe data transfer leads to these kinds of attack. When the data encryption is not proper data can be stolen while it is moving from source to client or it can be heard. This type of threat wither the confidentiality of the data.

VI. MANAGEMENT ARCHITECTURE FOR MOBILE DA-HOC CLOUD

We propose a management framework for mobile ad-hoc cloud in which we subdivided cloud in sub-clouds. Each sub-cloud has number of nodes. On the basis of node configurations and battery life the load balancer will divide the nodes into sub-clouds. Each sub-cloud is intact with an interface which provides communication among sub-clouds. We considered nodes as host nodes and client nodes, the nodes which offer their services are considered as host nodes and the nodes willing to use the services are considered as client nodes.

Our model distribute the job to the sub-cloud in way that respects the factors like computational power of the sub-cloud in terms of MIPS and current load on the sub-cloud. Management unit includes different components that is node manager which follows a particular protocol for node selection, load balancer, cloud repository, task manager, and application manager, along with management and security policies. The proposed framework is shown in figure 1.

A. Cloud repository

All the other components of the management unit are connected with cloud repository. Important data from every component will be stored by cloud repository, and every element can receive important and necessary information from the repository.

B. Node manager

Node manager decides the eligibility of the node to join the system. Factors like battery life, computational power of the host node or the computation power required by the query requested by the client node, estimated time that can be devoted by the host client to the system or calculated time for a query requested by client node to get processed and other security policies effects the selection of node for participating in MAC formation. The information like battery life, configuration of the mobile device, computational power required by the query reaches the management unit through the mobile cloud application installed in the device. Mobile cloud application intact Service level agreement which reflects the management policies, security criteria, QoS and cloud service performance metrics. Node manager automatically updates the number of nodes present in the system by monitoring the number of nodes joining and leaving the system. The eligibility criteria for node selection will include the minimum battery life, minimum processing power of the node, maximum length of the query requested by the client node and minimum estimated devoted time in the system. These eligibility criteria for node selection improve the failure of task due to battery life and provide better traffic management on the network.

C. Application manager

Each mobile node should be equipped with an application to facilitate its participation in MAC formation. The application will help the participant to understand the various requirement, important information and security policies of the system. The trusted data received by the mobile nodes will be maintained by the application manager. All the updates necessary by the node will be frequently updated by the application manager. The information like present load on the node, estimated time that nodes can devote to the system, battery life of the node and other important information required by the system will be provided by application manager. Application manager act as interface between mobile nodes and system.

D. Load balancer

Load balancer estimates the computing power of the system, the host node must provide the cloud management with necessary information about its own configuration and the present load running on the node. With the help of the information from host nodes the load balancer estimate the computing power of the nodes and lead to the formation of sub-cloud and keep on updating the status. This helps to reduce the response time and queuing delay for a query made by the host node.

E. Task manager

Task manger will distribute the task on the basis of the capability of sub-cloud. The task manger will calculate the computation power and time required by the task assigned by

the client node. On the basis of computation power and time required by the task for completion, the task manager will distribute the task to the sub-cloud. Knowledge of the processing power of the nodes and current load on the node helps the task manager with appropriate distribution of the task.

VII. SECURITY FRAMEWORK

At almost every stage of the process security becomes an integral part. Like selection of trusted nodes for setting up of trusted network, distribution of task among the nodes, processing of task allotted by other device. In this section we discussed some important security parameter

A. Protection of location information

In mobile ad-hoc network, allocation of task to a node requires location information of the node which in turn raises the privacy issues. System must provide the proper security of data and location to the node. Improper security regarding location may cause many criminal activities like identity theft, unwanted advertisements, invasion of unwanted parties and many other issues. Node should have full control on sharing of its location, node should know with whom their location information may be shared. The location of the node must be encrypted before sharing.

B. Identification of malicious node-

Secure discovery protocol: In our security framework we introduce an element which will look out the behaviour of node. Application software installed on the mobile node generates the unique identification number according to their unique hardware identification number. Node manager track the behaviour of every node which includes the node joining frequency in formation of the mobile ad-hoc network, time dedicated by the node to the mobile ad-hoc cloud and number of times the node completed the task assigned to it. On basis of this protocol node manager rates the node. Good rating of node allows the node to join the cloud otherwise the node will not be allowed to join the system.

C. Intrusion detection system

As there is no centralized monitoring entity present in mobile ad-hoc cloud each node needs to run its individual IDS. As proposed by Besant Subba [18] Bayesian game theory based IDS can protect the network from malicious nodes through strategically monitoring, it monitors the node which have high malicious value and bad history background which results in low traffic, protect the battery life of mobile node

D. Trusted network

Trusted network can be generated with the help of trusted, secure and cooperative nodes. On the basis of behaviour of the node and history details, each node will be assigned with some trust value. The nodes with higher trust value will be considered as more trusted and secure.

VIII. SECURITY CRITERIA

A. Authenticity

Generally service provider is responsible for providing the securities like identity or access management. But in an environment where users are the service providers than authenticity is a key issue. It is very important to prove identities before joining the network. Authenticity can be achieved through security assertion markup language (SAML).

B. Confidentiality

Confidentiality comes in role when some particular data is only accessible by some confidential nodes. This is a parameter to keep the data secret from all the nodes.

C. *Authorisation*

Authorisation is a process of issuing a certificate to node. This is generally done to provide degree of permission to access a network to the user.

D. Integrity

Integrity identifies the correctness of the message during their transmission. It can detect two types of altering one is malicious altering and other is accidental altering [2]. Data can be deleted or altered due to some malicious act or it can be lost due to some benign failures. Maintaining the integrity of data is really important.

IX. CONCLUSION

Mobile nodes with property of formation of ad-hoc network and cloud computing paradigm envisioned MAC. Mobile cloud computing is an energy efficient and cost effective model. In this paper we reviewed the similar work done in this area and further presented management architecture for MAC. In which we discussed various architectural components and their processing protocols. We also analysed various challenges and threats causing hindrance in the implication of the MAC and developed a security framework. Presented security framework focuses on necessary prevention techniques corresponding to threats and defence structure towards secure management architecture. Lots of research is still needs to go by researchers in this new paradigm as many of its capacities are not covered entirely.

X. REFERENCES

[1] Fan, Xiaopeng, Jiannong Cao, and Haixia Mao. "A survey of mobile cloud computing." zTE Communications 9, no. 1 (2011): 4-8

[2] Basagni, Stefano, Marco Conti, Silvia Giordano, and Ivan Stojmenovic, eds. Mobile ad hoc networking. John Wiley & Sons, 2004.

[3] Fernando, Niroshinie, Seng W. Loke, and Wenny Rahayu. "Mobile cloud computing: A survey." Future generation computer systems 29, no. 1 (2013): 84-106.

[4] Pettey, Christy. "Gartner identifies the top 10 strategic technologies for 2011." Gartner http://www. gartner. com/it/page. jsp (2011).

[5] Kovachev, Dejan, Dominik Renzel, Ralf Klamma, and Yiwei Cao. "Mobile community cloud computing: emerges and evolves." In Mobile Data Management (MDM), 2010 Eleventh International Conference on, pp. 393-395. IEEE, 2010.

[6] Marinelli, Eugene E. Hyrax: cloud computing on mobile devices using MapReduce. No. CMU-CS-09-164. Carnegie-mellon univ Pittsburgh PA school of computer science, 2009.

[7] Kirby, Graham, Alan Dearle, Angus Macdonald, and Alvaro Fernandes. "An approach to ad hoc cloud computing." arXiv preprint arXiv:1002.4738 (2010).

[8] McGilvary, Gary A., Adam Barker, and Malcolm Atkinson. "Ad hoc cloud computing." In Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on, pp. 1063-1068. IEEE, 2015.

[9] Christensen, Jason H. "Using RESTful web-services and cloud computing to create next generation mobile applications." In Proceedings of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications, pp. 627-634. ACM, 2009.

[10] Dinh, Hoang T., Chonho Lee, Dusit Niyato, and Ping Wang. "A survey of mobile cloud computing: architecture, applications, and approaches." Wireless communications and mobile computing 13, no. 18 (2013): 1587-1611.

[11] Shila, Devu Manikantan, Wenlong Shen, Yu Cheng, Xiaohua Tian, and Xuemin Sherman Shen. "Amcloud: Toward a secure autonomic mobile ad hoc cloud computing system." IEEE Wireless Communications 24, no. 2 (2017): 74-81.

[12] Muralidhar, K., and N. Geethanjali. "Implementation of Ad Hoc Cloud Computing through Mobile Devices to Facilitate "Cloud on the Fly" Model." (2016).

[13] Rahman, Sk Md Mizanur, Md Mehedi Masud, M. Anwar Hossain, Abdulhameed Alelaiwi, Mohammad Mehedi Hassan, and Atif Alamri. "Privacy preserving secure data exchange in mobile P2P cloud healthcare environment." Peer-to-Peer Networking and Applications 9, no. 5 (2016): 894-909.

[14] Mishra, Amitabh, and Ketan M. Nadkarni. "Security in wireless ad hoc networks." In The handbook of ad hoc wireless networks, pp. 499-549. CRC Press, Inc., 2003.

[15] Grilli, Gianluca. "Data dissemination in vehicular networks." Philosophiæ Doctor (PhD) dissertation in Computer Science and Automation Engineering/University of Rome, Tor Vergata (2010).

[16] Papadimitratos, Panagiotis, and Zygmunt J. Haas. "Securing Mobile Ad Hoc Networks." (2004).

[17] Ismail, Mohd Nazri, Abdulaziz Aborujilah, Shahrulniza Musa, and AAmir Shahzad. "Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach." In Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, p. 36. ACM, 2013.

[18] Subba, Basant, Santosh Biswas, and Sushanta Karmakar. "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation." Engineering Science and Technology, an International Journal 19, no. 2 (2016): 782-799.