Analysis on security threats of mobile ad -hoc cloud

Sonam Agnihotri
Student of Department of electronics and communication
Chandigarh Engineering College, Landran, Mohali

Nidhi Chahal
Faculty of Department of electronics and communication
Chandigarh Engineering College, Landran, Mohali

Abstract: In this paper we talked about the challenges, security threats and security criteria for mobile ad hoc cloud. The network uses the properties of MANET for communication and implementation of ad-hoc cloud. The ad-hoc environment and mobile nature of the system leads to many challenges. We discussed the various possible threats, security criteria and security measures against threats which can make the system better and trustworthy.

Keywords – Mobile ad-hoc cloud, security, privacy, challenges

I. INTRODUCTION

The importance of Cloud Computing is increasing and it is receiving a growing attention in the scientific and industrial communities. A study by Gartner [1] 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 [1] that is software as service, platform as service and infrastructure as service.

Another mode of cloud computing is ad-hoc cloud computing influenced by the underutilized resources. The computational power and storage resources of many workplaces, educational institutes and big enterprises are under-utilized. Ad-hoc cloud provides a way to harvest resources from these under-utilized, non-exclusive and sporadically available resources [2]. Users of ad-hoc cloud belongs to highly shared environment of resource. The ad-hoc cloud computing is an effective way to reduce overall power and cost.

In mobile ad-hoc networks (MANET) mobile nodes self-organise them-selves to create a mobile network [3]. These mobile nodes comprise of laptops, smartphones or any other mobile device. The mobile nodes can communicate directly or indirectly to any other node in their own radio range. Each node in mobile ad-hoc cloud is free to join and leave, so the topology of the network keeps on changing.

Mobile ad hoc cloud is a concept of using computation power of smartphones in ad-hoc environment to implement ad-hoc cloud computing as discussed by K. Murlidharan [4]. These day's everyone wants to access all the services and applications on mobile devices. However all the devices are not same regarding resources. Limitations of weak devices can be overcome through MAHC (mobile ad-hoc cloud). MAHC uses the properties of mobile ad-hoc network (MANET) to detect nearby nodes so as to access its computational and storage power. Mobile nodes changes the cloud dynamically as the nodes are not dedicated to the cloud. Though the primary purpose of node is different they offer some time for ad-hoc structure. A local ad-hoc cloud formed with the help of smartphones is powerful enough to provide the computational services. A framework of mobile ad-hoc cloud is discussed in [9]. This framework includes source handler, job handler and cost handler. A resource handler is responsible for finding the clients in its range and collecting parameters like processor, battery life, location, velocity and processing price of the potential resource. A job handler is responsible for partitioning the data and distributing the data according to the potential of the clients in the network. Keeping the track and scheduling mechanism is also handled by job handler. A cost handler is responsible for estimating the cost and selecting the device depending upon the information provided by resource handler. Figure (1) shows the basic architecture of mobile ad hoc cloud. Due to ad-hoc and mobile nature of the cloud, security and privacy becomes the most important parameter. Further paper is organised as follow. Section 2 discuss the challenges of MAHC. Section 3 discuss security threats. Section 4 discuss security criteria. Section 5 discuss security measures for mobile ad-hoc cloud. Section 6 presents conclution.

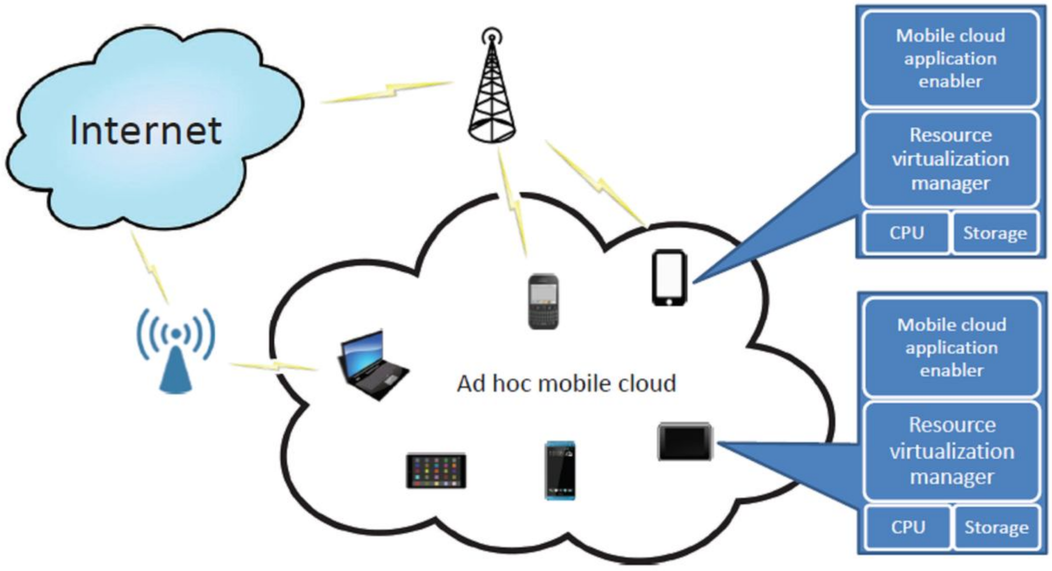
Internet
Ad hoc mobile cloud
Mobile cloud application enabler
Resource virtualization manager
CPU
Storage
Mobile cloud application enabler
Resource virtualization manager
CPU
Storage

Figure 1: Mobile ad hoc cloud architecture

II. CHALLENGES OF MOBILE AD-HOC CLOUD

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) [5]. 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.

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

Signal fading-
The large buildings and other infrastructure can cause fading of the signal [6] which can cause lag in the processing of the data or even result in the bad communication strength with the other nodes.

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.

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.

No centralized management –

A network without central management, high mobility and ad-hoc nature is difficult to protect from attacks [7]. 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.

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.

III. SECURITY THREATS IN MOBILE AD-HOC CLOUD

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.

Byzantine failure –

This failure occurs when a malicious act is performed by a group of nodes [5]. 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.

Denial of service attack (DoS) –

This attack aims at the availability of certain node or even the services of the entire ad hoc networks [8]. 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.

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.

IV. SECURITY CRITERIA FOR MOBILE AD-HOC CLOUD

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) [9].

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.

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.

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 [10]. 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.

V. SECURITY MEASURES FOR THREATS IN MAHC

The security criteria like availability, integrity, confidentiality needs some strong communication structure to be achieved. Powerful encryption algorithm can prevent the attacks like eavesdropping. Once the data is sent to the potential client for processing the originator loses complete control of the data. Malicious node can modify or delete the data. The processing data should be highly encrypted which makes the modification of data challenging. Malicious nodes can even send viruses, to protect the devices from viruses sandboxing of the system can be done. Sandboxing is the technique in which the processing of the task from the other device will be separated from the host device. Sandboxing restricts the resources of host device and prevents any impact on the host device due to processing of task from other device. Antivirus software in the devices can protect the device from malicious activity. Certificates and cryptographic techniques in traditional cloud computing helps in establishing trustworthy environment, one such structure can help in trustful sharing of services in ad-hoc cloud.

Rating mechanism can help in avoiding selfish behaviour of the node in the network as discussed in [11]. A promising cloud element should be rewarded with good rating. The element performing evil tasks or misleading the network should be rated with less points. This system will help in recognising the malicious nodes, then such nodes will not be allowed to join any mobile ad-hoc cloud.

VI. CONCLUTION

The mobile ad-hoc cloud aims at exploiting the full potential of mobile devices. These days every person wants to access most of the application on smartphones. Mobile ad-hoc cloud is cost effective and power saving model. In first section we reviewed the architecture of mobile ad-hoc cloud. In second section this paper discussed the challenges due to mobile nature and ad-hoc environment of mobile ad-hoc cloud. We have gone through the various possible threats due to absence of proper communication structure. In the end we discussed the current solution and security techniques which help in protect the mobile ad-hoc cloud.

During the study we find some areas on which a lot of work can be done in future like creating a better architecture for mobile ad-hoc cloud and better security framework.

REFRENCES

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

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

[3] Corson, M. Scott, Joseph P. Macker, and Gregory H. Cirincione. "Internet-based mobile ad hoc networking." *IEEE internet computing* 3, no. 4 (1999): 63-70.

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

[5] Amitabh, Mishra, M. Ketan, and Nad Karni. "Security in Wireless Ad Hoc Networks, The Hand Book of Ad hoc Networks." (2003): 479-490.

[6] Grilli, Gianluca. "Data dissemination in vehicular networks." *PhilosophiDoctor (PhD) dissertation in Computer Science and Automation Engineering* (2010): 181-190.

[7] Papadimitratos, Panagiotis, and Zygmunt J. Haas. "Securing mobile ad hoc networks." *Book The Handbook of Ad Hoc Wireless Networks* (2002).

[8] 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.

[9] Cloud Security Alliance (2012) SecaaS implementation guidance, category 1: identity and Access managament. https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf

[10] Fernando, Niroshinie, Seng W. Loke, and Wenny Rahayu. "Mobile cloud computing: A survey." *Future Generation Computer Systems* 29, no. 1 (2013): 84-106.

[11] Shila, Devu Manikantan, Wenlong Shen, Yu Cheng, Xiaohua Tian, and Xuemin Sherman Shen."AMCloud: Towards a Secure Autonomic Mobile Ad Hoc Cloud Computing System." *to appear*