Security Measures and Threats on Mobile Cloud Computing: Issues and Direction

Aradhana[1], Samarendra Mohan Ghosh[2]
[1]*Department of Computer Science and Engineering,* [2]*Dr. C. V. Raman University Bilaspur, C.G.*

Abstract- Mobile cloud computing migrates process to other server that executes some events on the behalf of user and or applications .This consist of various security issues like authentication, code integrity, access control, availability, anti tempering and trust management. So, to design and developed the security mechanism for mobile cloud computing. It requires strategic planning and awareness of growing the security threats and measures. In this paper, we bring out the some security issues and direction related to mobile cloud computing against threats during computation offloading on clouds.

Keyword- Mobile Agent, Computation Offloading, Security, Code Obfuscation, Encryption

I. INTRODUCTION

Mobile agents are the mobile code on cloud environment. The concept of mobile code is the dynamic installation of code on a remote host. Complexity of execution demands resources. It is to be multimedia base application like 4D animated series are being growing demanded on mobile phones. Even requirements of software and hardware upgrade every months. So that mobile devices have poor resources, less secure. Resource poorness is major obstacle for advance applications. The concept of computation offloading is new ability to gain high computation speedups with small communication delays. In last few years, this idea has received more interest because of the significant rise in the sophistication of mobile applications, the availability of powerful clouds. By identifying the off loadable tasks at runtime, recent work [1, 2,3,4,5 and 6] has aimed to generalize this approach to benefit more mobile applications.

The security issues of mobile devices are different from the security issues of traditional Computer systems. These are following factor that shows the difference between these two computing devices: Mobility, Strong Personalization, Strong Connectivity, Technology Convergence and Resource con-strains.

Mobile Agent has some hidden security problem in these phases:-

- **Transferring Phase:** The agent transfer from host to another platform.
- **Running Phase:** The agent's code in another platform during computational offloading.

This approach of mobile agent is new and attractive interaction of computation, it arises significant challenges in terms of data and code security during the offloading. This paper analyses the security issues and points to direction related to mobile agents. Most agent systems considered four elements for their security: -

A runtime environment (usually the Java Virtual Machine) for host protection.

Code signing to prove that the agent has not been tampered with other

Host authentication to prove that the agent is about to move to the intended host,

Establishment of a secure channel over which the agent can migrate.

II. OVERVIEW OF RELATED EXISTING WORK

Cloud computing migrates the computation and the resources from one location onto another recourses. The cloud system resource is open, as neither the application nor the user knows the location of the resource. According to Buyya et al. [7] the cloud computing has the following definition "Cloud is a parallel and distributed computing system consisting of a collection of interconnected and virtualized computers that are dynamically Copyright (c) IARIA, 2015. ISBN: 978-1-61208-388-9 103 CLOUD COMPUTING 2015 : The Sixth International Conference on Cloud Computing, GRIDs, and Virtualization provisioned and presented as one or more unified computing resources based on Service-Level Agreements (SLA) established through negotiation between the service provider and consumers [8]." Vaquero et al. stated that "clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services) [9]", where the resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization.

III. SECURITY OBJECTIVES ON MCC

Generally a secure software system should meet the following security objectives:-

Accountability (Responsibility): This security objective responsible for individual part of information security. This objective supports the supports non-repudiation, prevention, fault isolation, intrusion detection.

Authentication: It identifies the identity of end users or devices. Authentication prevents from faking or masquerading.

Authorization: It gives the permission of deny access rights to a user, program or process.

Availability: It ensures that data and system can be accessed by correct users within an specific period of time. It affects several attacks like Denial of Service (DoS) or loss of availability.

Confidentiality:-It ensures the transmitted data should be protected from any unauthorized person. Data can only

understand by sender or receiver only. A loss of confidentiality effects data privacy.

Integrity: It has two parts Data integrity and system integrity. In case of Data integrity, Data should not change during transmission. System integrity system should be preventing from unauthorized access.

Non-Repudiation: It happens when the system does not properly end the program or log off. Thus it permits malicious manipulation on the transactions.

IV. ATTACK ON MCC

Threats to security can be fall into four classes:

- Disclosure of information,
- Denial of service,
- Corruption of information,
- Interference or nuisance.

There are a variety of ways to examine in greater detail these classes of threats as they apply to agent systems. Here, we discuss the security threats on agent model to identify the possible source and target of an attack. Based on mobile agent and platform of execution we distinguished four categories of threats:-

- Agent-to-Platform attack
- Agent-to-Agent attack
- Platform-to-Agent attack
- Other-to-Agent attack

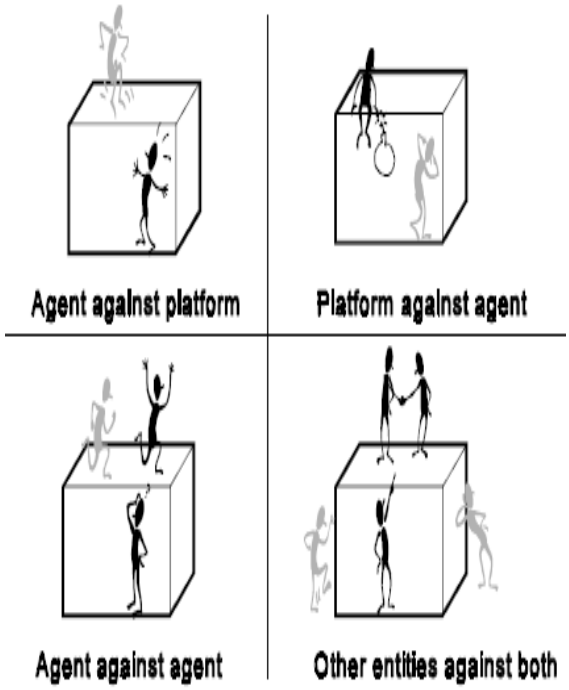

Fig.1: Classes of threats against mobile agent

Agent-to-Platform attack: Mobile agent corrupts the Execution Platform. The attacks such as Masquerading, Denial of Service and Unauthorized Access comes under this treat.

Agent-to-Agent attack: Mobile Agent attacks to another Agent inside the host they may change and modify the original code. Attacks such as Masquerade, Denial of Service, Repudiation and Unauthorized access are used to perform Agent-to-Agent attack.

Platform-to-Agent attack: A Platform attacks the security of the Mobile Agent. This includes attacks such as Masquerading, Denial of Service, Eavesdropping and Alteration.

Other-to-Agent attack: All types of attack which Mobile Agent may suffer during its travel through the network or visiting a host. This may include masquerading, denial of service, unauthorized access.

V. SECURITY THREATS ON MCC

Security concern of cloud is fall on two broad categories first is security issue faced by cloud providers and second is their end users. so that the responsibility is shared and implement the security on both ends. This environment has many advantages but It has also some drawbacks and security issues .It can arise during offloading the computation (SaaS) services. Here we describe some security threats facing cloud users. Cloud Security Alliance (CSA) did survey on related issue and find the following threats:

1. Tracing and hacking our sensitive information by attackers.
2. Unauthorized use of network used by
3. Data leakage in cloud environment
4. Lacking of skilled hands and experts
5. Data loss on cloud environment
6. Data Segregation from other recourses
7. Security culture among different providers
8. Evolving threats may target clouds.
9. Hardware and software modification
10. Interruptions on software
11. Software theft
12. Misuse of infrastructure
13. Privacy concerns

VI. SECURITY ISSUES IN MCC

In case of strong mobility of mobile agent all its code, data and state are exposed to the mobile agent platform in which it migrates for execution of operation. Because of this mobile agent faces more severe security risks. Following are possible attacks by malicious platforms:

1. Leak out/ modify mobile agent's code
2. Leak out/ modify mobile agent's data
3. Leak out/ modify mobile agent's execution flow
4. Denial of Service(DoS)
5. Masquerading
6. Leak out/ Modify the interaction between a mobile agent and other parties

VII. SECURITY MECHANISMS FOR MOBILE CODE

The security mechanism for mobile code can be divided into two broad categories

1. Detection
2. Prevention

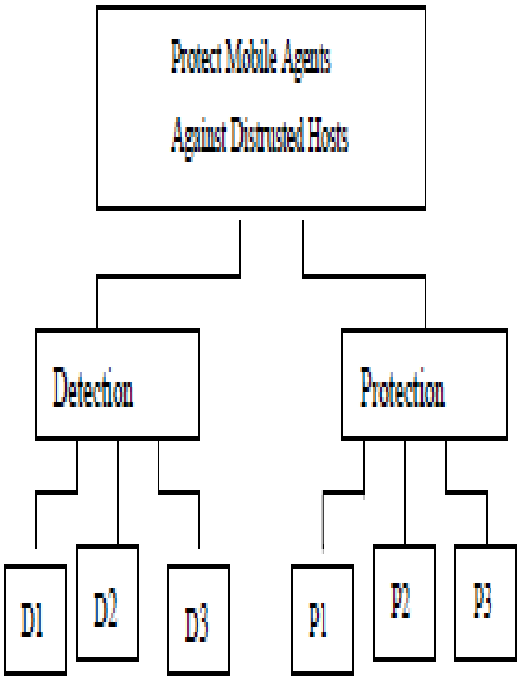

Fig.2: Security Mechanism

Detection Mechanism

Detection of Agent tampering: this includes solutions to detect unauthorized modifications of code, state or execution flow of a mobile agent. These detection mechanisms are further subdivided depending on whether they:

D1: detect manipulation automatically or require a suspicion.

D2: detect manipulation during execution of a mobile agent or after it has terminated.

D3: detect all possible manipulations of mobile agent or only some of them.

Prevention Mechanisms

The mechanisms here try to make it impossible or very difficult to access or modify code, state or execution flow of a mobile agent. These are further subdivided into:

P1: prevent attacks on the entire agent or only parts of it.

P2: rely on some trusted functionality or no trust at all.

P3: prevent attacks permanently or only temporarily.

VIII. REASONS FOR BUILDING TRUST IN MCC

For building the secure framework for MCC we measure the following two parameters of security in mobile cloud computing:

(1) Authentication of agent platform,

(2) Security in code offloading.

The security of these three parameter not only provide the authenticity, integrity and confidentiality to mobile computing in the cloud, but also provide flexibility, mobility, scalability and performance For computation offloading, the code and data collected by mobile devices is executed and stored on cloud services. The agents of mobile application could be instantiation on the cloud environment and to supplement the functionalities of the device. During the offloading confidentiality and authenticity of this execution is a concern much attention.

A secure computational offloading framework is proposed to address this concern. For providing the security on computation by owner provides the encryption keys as aforementioned. The critical part of computation is encrypted with keys used by the owner. Hence, access to critical data needs the authorization of the owners. The limitation of encryption/decryption method of information on cloud computing is key management from both ends information for that we send and store the key in the cloud the key. The problem in this technique is key outflow from channel or cloud so that information is not confidential.

We analyze that code obfuscation method is better than encryption because it also transform the information in intellectual form without using key. Code obfuscation provide information to better security and information will be more complex than encryption, including improved software security, tamper prevention, and intellectual property protection. As obfuscation results more complex and become more obfuscate and mitigation and detection are not impossible.

IX. CONCLUSIONS

In this paper, we bring out the security issues which affecting the computational on mobile cloud computing. We first list various threats found during computation offloading on cloud. Finally we summarized the proposed mechanisms that ensure providing the better security on mobile cloud computation offloading using code obfuscation method rather than encryption/decryption methods also discuss the limitation of encryption /decryption during offloading. We observe that securing the information using Obfuscation method is more robust, complex and difficult than encryption/decryption method.

X. REFERENCES

[1]. R. K. Balan, D. Gergle, M. Satyanarayanan, and J. Herbsleb. Simplifying cyber foraging for mobile devices. In ACM MobiSys, 2007.

[2]. B. Chun, S. Ihm, P. Maniatis, M. Naik, and A. Patti. Clonecloud: elastic execution between mobile device and cloud. In EuroSys, pages 301–314, 2011.

[3]. E. Cuervo, A. Balasubramanian, D.-k. Cho, A. Wolman, S. Saroiu, R. Chandra, and P. Bahl. Maui: making smartphones last longer with code offload. In ACM MobiSys, 2010

[4]. M. S. Gordon, D. A. Jamshidi, S. Mahlke, Z. M. Mao, and X. Chen. COMET: code offload by migrating execution transparently. In USENIX OSDI, pages 93–106, 2012.

[5]. F. Xie, Y. Peng, W. Zhao, D. Chen, X. Wang, and X. Huo, "A risk management framework for cloud computing," in Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on, 2012, vol. 1, pp. 476–480.

[6]. W. Liu, "Research on cloud computing security problem and strategy," in Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, 2012, pp. 1216–1219.

[7]. H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," Computer Software and

Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual , pp. 393–398.

[8]. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, no. 6, Jun. 2009, pp. 599–616.

[9]. L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, 2009, pp. 50–55.