International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 2, Issue 4 (July-Aug 2014), PP. 225-230

APPLICATION OF MOBILE AGENTS FOR SECURITY USING MULTILEVEL ACCESS CONTROL

Apoorva Upadhyay
Department of Computer Science Engineering
Shri Ram Institute of Technology
Jabalpur, India
apoorva14u@gmail.com

Mahendra Rai
Department of Computer Science Engineering
Shri Ram Institute of Technology
Jabalpur, India
mahendrakumarrai@gmail.com

***Abstract*— in distributed computing environment, Mobile agents are mobile autonomous processes which operate on behalf of users (e.g., the Internet). These applications include a specialized search of a middleware services such as an active mail system, large free-text database, electronic malls for shopping, and updated networking devices. Mobile agent systems use less network bandwidth, increase asynchrony among clients and servers, dynamically update server interfaces and introduce concurrency. Due to software components, security of mobile agent is essential in any mobile agent based application. Security services such as Confidentiality, Integrity, Authentication, Authorization and Non-Repudiation are discussed and combat with by the researchers. This work is proposing a new technique for access control area of security for the mobile agents and it will be implemented using an example of shopping cart data sharing for multiple levels.**

Keywords- Mobile Agents, Access Control, Authentication, Attacks, Security, Use of Mobile Agents in Shopping Cart

I. INTRODUCTION

A mobile agent is Associate in nursing freelance piece of code with autonomy and quality options. A mobile agent will migrate from one host to a different autonomously to resume its execution. Here autonomy means that to require call Associate in Nursing to execute an action while not direct user or human interaction.

One of the most blessings of victimization mobile agent is – it reduces network traffic load perceptibly because it doesn't need any continuous affiliation or communication between the server and therefore the consumer. Besides, use of mobile agent makes access of remote resource additional economical and versatile. Agent will adapt dynamically to Associate in nursing atmosphere and might operate in heterogeneous environments. It is strong and fault tolerant. Although origin of the term 'Agent' was within the field of 'Artificial Intelligence', it's gained plenty of potential within the field of network watching, analysis and Intrusion Detection or hindrance System. Besides these, the mobile agent also can be used for info retrieval, server configuration backup, dynamic package readying etc. The autonomous agent concept has been proposed for a variety of applications on large, heterogeneous, distributed systems (e.g., the Internet). Mobile agent systems have many advantages over traditional distributed computing environments. Due to the problems with security of Mobile agents, they have limited popularity.

Mobile agent's square measure composed of code, knowledge and state. Agents migrate from one host to a different taking the code, knowledge and state with them. The state info permits the agent to continue its execution from the purpose wherever it left within the previous host. For instance, a mobile agent may be migrated from the house platform with the task of shopping for Associate in nursing plane ticket for its owner. The agent would visit all the identified hosts of airline firms, one once another, to go looking for the foremost reasonable price tag, and so purchase one for its owner. When the agent moves to consequent host, it summarizes the present state, execution pointer on the present state, etc., in order that it will begin finding out affordable tickets on consequent host. The state of the agent can contain a collection of doable tickets to be thought-about for purchase. Once the agent has finished its search, it's going to come to the host wherever it found the most affordable or best price tag and buy it.

While agents cast round the web, they're exposed to several threats and will even be a supply of threat to others. Electric sander and Tschudin gift two forms of security issues that have to be solved. The primary is host protection against malicious agents. The second is agent protection against malicious hosts. Several techniques are developed for the primary quite drawback, like watchword protections, access management, and sand boxes, however the second drawback appears to be tough to unravel. It's typically believed that the execution atmosphere (host) has

full management over capital punishment programs; so, protective a mobile agent from malicious hosts is tough to realize unless some tamper-proof hardware is employed. for instance, Yee planned Associate in Nursing approach during which a secure coprocessors employed that executes crucial computations and stores crucial info in secure registers.

A. SECURITY ISSUES AND THREATS

Security of mobile agent is essential in any mobile agent based application. Besides security of agent platform is also important. To discuss the security aspects of a mobile agent system we have considered the following security services: Confidentiality, Integrity, Authentication, Authorization and Non-Repudiation.

1. Confidentiality

Confidentiality ensures that, data and code carried by an agent is not accessible by unauthorized parties (unauthorized agent or unauthorized agent server).

2. Integrity

Integrity guarantees that agent's code and baggage cannot be altered or modified.

3. Authentication

Authentication enables a mobile agent to verify its identity to an agent server as well as an agent server to a mobile agent. Without authenticity an attacker could masquerade an agent's identity and could gain access to resources and sensitive information.

4. Authorization

Authorization ensures that an agent can access the resource or information only those are allowed for it to access.

5. Non-Repudiation

Non-repudiation assures that the agent-server or the mobile agent cannot repudiate the actions it has performed.

Threats in a Mobile Agent system can be categorized as:

• Threats from mobile agent to agent server

• Threats from agent server to mobile agent

• Threats from mobile agent to mobile agent

6. Threats from Mobile Agent to Agent server

Potential threats from a mobile agent to an agent server can be listed as: illegal access to services and resources of agent server, steal or reveal of secret information from server, denial of service, damage of software and data, penetrate virus/worms and finally action repudiation.

7. Threats from Agent server to Mobile Agent

Similarly an agent might face some threats from an agent server those can be listed as: illegal access to mobile agent's resources, steal code and valuable information carried by agent, reveal private or sensitive action performed by mobile agent, damage of code and baggage, execute agents code incorrectly, sending agent to unintended destination, cheat agent with false information and information or action repudiation.

8. Threats from Mobile Agent to Mobile Agent

Finally an agent could face threats from another agent. These threats are stealing agent information, convey false information, render extra messages, accusing processor time, denial of service, information or action repudiation and unauthorized access.

Main focus of this work is on ACCESS CONTROL, which is as per above discussion is to protect the host server from mobile agents or intended mal activities by the agent server on the remote host. The proposed work will be an enhancement to the RBAC with improvements so that better Access Control can be provided to the users.

B. ROLE BASED ACCESS CONTROL (RBAC)

Core RBAC includes sets of five basic data elements called users (USERS), roles (ROLES), objects (OBS), operations (OPS), and permissions (PRMS). The RBAC model as a whole is fundamentally defined in terms of individual users being assigned to roles and permissions being assigned to roles. Figure below indicates a flow diagram for RBAC based processing happening at the remote host in respect of the mobile agent travelling to it. This diagram shows the interactions between the various data elements of the RBAC.

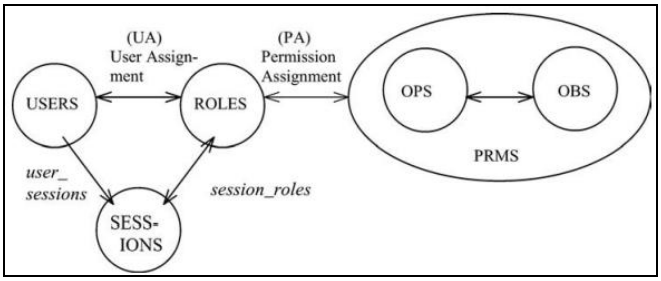

Fig 1: Flow Diagram of RBAC

This work is proposing RBAC over the networked system where communication has to be performed between the two different companies with certain access rights to be given to

each other on mutual agreement basis. The proposed work shall be implemented using an example shopping cart application where two companies want to provide limited access for the online sale of their items through other companies. This work will provide communication by authenticating and authorizing the needs of one company using mobile agents.

This paper discusses the introduction of the mobile agents their pros and cons and application areas in section I. Section II discusses the basis of the proposed work and discusses the work done by the various researchers in the area of security of the mobiles. Problem statement has been formed from the studies and has been discussed in the section III. Section IV elaborates on the proposed system and algorithms to be used in this work. Section V gives the results and discussion of the work implemented to indicate the security enhancements achieved from this work. At the end conclusion has been drawn and possible enhancements to the proposed work has been addresses.

II. EXITING WORK

The work of the various authors have been the base to understand the possibilities in the area of the security of the mobile agents and details used in this work as the base work is as follows:

Xu Xiao-long [1] it presents Information Retrieval System based on MobileMultiAgents (IRSMMA) that improves the performance of existing Information Retrieval System (IRS). The system brings security threats like fake malicious host pretending to be real ones, malicious mobile agents and generation of fake information. Mobile Multi Agent Security Architecture (MMASA) is introduced in this work. In this work X.509 certificates is used whereas SSL has been used on transport layer, IDE algorithm for encryption of MAs and RSA for key encryption. MD5 for message digest and PKI with RSA for digital signature has been applied using Java Authentication and Authorization Services.

Rossilawati Sulaiman [2] it presents a Multi-Agent based SecurityMechanism (MAgSeM) to enhance the traditional non-agent based system. It is claimed that Agents are interactive, autonomous, extensible and mobile which allow the agent to perform task with minimal interaction with user. JavaAgentDevelopment (JADE) has been used to develop MAgSeM and FIPA-ACL (Agent Communication Language) is used to implement agent communication.It applies Cryptographic protocols for encryption. Secure channel security with SSL and symmetric key AES are used. PKI to encrypt via RSA algorithm and SHA1for hash function is used to incorporate security. This work has been elaborated on access control.

Vieira-Marques [3] it presents the Information Gathering System (IGS) for secure integration of distributed, inter-institutional medical data using agent technology. It improves the performance of existing Virtual Electronic Payment Record (VEPR). This system needs to ensure that only authorized staff can access the information and data moving through network is secure. Proposed mobile agent system is based on JADE framework and FIPA-ACL for agent communication. It uses X.509 certificates and Secure Assertion Markup Language (SAML). Hash-Chains scheme has been proposed in this work. This work proposes to create digital envelope using public key cryptography signatures, symmetric keys and code encryption. It uses role based access control (RBAC) to manage user's role policies and uses Extensible Access Control Markup Language (XAMCL) to ensure interoperability of the system access control policies.

A. Secure Image Mechanism

One way to provide security to mobile agent and to protect the partially processed data is to introduce a SIC (Secure Image Controller) in the system. When a Mobile Agent head towards an Agent Server it looks up the itinerary table to check whether the host is trusted or not. If the host is not trusted then the Mobile Agent goes to SIC (Secure Image Controller). SIC generates an image (a version) of the agent and sends the image to the untrusted host rather sending the original one. After completion of execution the agent image is compared with the original agent by the SIC. If the verification is failed SIC just drop the returned image of agent and use the original agent to complete the rest of the task [1]. Advantage of this method is, in this way an agent can be sent to an untrusted host and verify it. By using SIM eavesdropping and alteration attack can be prevented. But there is no solution to protect the agent server from malicious agents. There is also no solution for Authorization, Access Control and Non-Repudiation service.

B. Protecting Mobile Agent Through Tracing

Geovanni Vigna has proposed a schema to detect any possible undesired modification of a roaming agent by any malicious site using cryptographic traces [2]. Cryptographic Traces are nothing but log or history of operations done by agent during its life time. An agent program is checked against an assumed history of the agent's execution. The agent owner can check whether the agent has performed its tasks correctly or not from the log file. But in this method the agent system must maintain a large log file and special mechanisms are needed to reduce the log size.

C. Partial Result Encapsulation

In this procedure Symmetric Key Cryptography is used. Bennet Yee proposed this idea to protect the intermediate state of partial result of an agent after being executed on a server. When an agent moves from a host its state and result is encrypted with a symmetric key to produce MAC (Message

Authentication Code) on the message. This authentication code is used to verify any types of modification of the agent's partial result [3]. Problem of this method is to maintain and generate a large scale of symmetric keys.

D. Sandboxing

The main goal of sandboxing is to protect the agent platform from a malicious mobile agent. Typically a sandbox provides a controlled set of resources for a guest program to run. While the guest program runs in the restricted environment its movement and activities are observed. If it does not show anything unusual and executes the tasks it supposed to do, then the program is considered safe for the actual environment and is allowed to execute there [6].

E. Signed Code

This method provides a way to secure mobile agent using Digital Signature. This sign may be provided by either the creator of the agent or the owner or by some third party. Authenticity, Non-Repudiation and Integrity of an agent can be ensured by this technique. For Authorization and Access Control, Attribute Certificate can be associated with the signed code [6]. This method requires a CA (Certificate Authority). So it is not applicable for an ad hoc network where there is no central trusted party.

III. PROBLEM STATEMENT

It is a mobile agent based information retrieval system which relies on the security of the mobile agent to be ensured before data delivery to it. It addresses two major concerns, security and performance. In example implementation it uses online shopping carts. In security, it addresses the major points such as malicious agents, access control mechanism, secured data transfer over the network etc. At all no interaction with the user Secured transaction with proper access control has been proposed and implemented using the java technology. Key based authentication One Time Pad Security Encryption technique is used to provide high security and performance. It applies role based access control (RBAC) to manage user's role policies. We have various rules created and applied to achieve access control is strictly applied.

IV. PROPOSED FRAMEWORK

The work in this paper proposes to implement the security of the mobile agent data communication using authentication, access control & consistency applied over the shopping cart system. The framework of the complete work flow is shown in the figure 2. It has 7 Process Agents which are performing the various tasks to actually port the information with high security through Mobile Agent.

1. User Authentication & Information Agent (UAIMA). It is responsible for authenticating to end user for purchasing the shopping cart items. It keeps all information related with item purchased and end user login.

2. User Requirement Processing Agent (URPA). URPA just stays on the first server, responsible for managing the local information such as the identity and retrieval inclinations. URPA is also able to learn from the database about the items lacking in quantity and correct the inclination parameters to meet the current requirement.

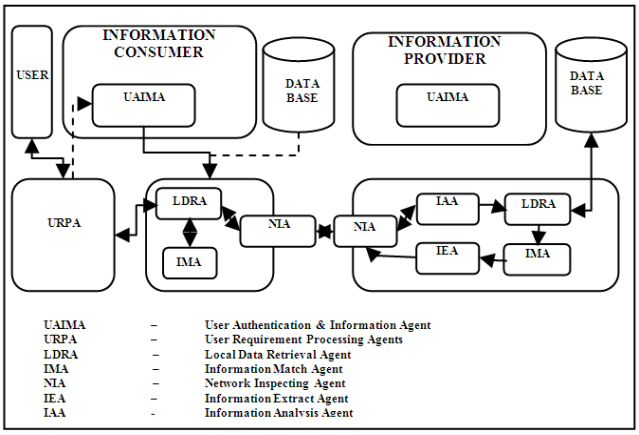

Fig 2: Framework for the proposed system

3. Local Data Retrieval Agent (LDRA). It is used to help URPA to access the items which are lacking in quantity at local system to be sent the same to other host.

4. Information Matching Agent (IMA). IMA stays on the information retrieval server host, with responsibility for receiving queries provided by LDRA from hosts, searching and finding the matching information from the index database with internal retrieval algorithm, and then feeding retrieval results sorted.

5. Network Inspecting Agent (NIA). NIA is another kind of mobile agent in this system, which is sent by the information retrieval server and traveling among network nodes to investigate the running conditions of websites automatically. NIA is used to detect the collapse or service termination of websites and report to the information retrieval server.

6. Information Extract Agent (lEA). lEA stays on the information store host, which can analyze web pages, extract the valuable information and format them as the following format :<Subject, Abstract, Main content, Links, URL, Update time>, which is encapsulated in DT A and sent to the information retrieval server.

7. Information Analysis Agent (IAA). IAA stays on the information retrieval server, which communicates with the

DTA and receives web pages' information and running status from information store hosts. IAA then processes such information and puts the web pages' information into the index database or updates the information stored in it.

V. PROPOSED ALGORITHM

According to literature review presented by Rui A. Martins et.al, Mobile Agents have increasing penetration in the market for data transfers and due to enhanced application areas, their security is becoming a major issues. They require attention for all the fields of security such as Authentication, Confidentiality, Integrity, and Access Control.

This work is proposing a new technique for access control area of security for the mobile agents and it has been implemented using an example of shopping cart data sharing for multiple levels.

Initially two or more web applications have been developed for implementation of shopping cart using J2EE. A socket based system is run to connect the two web applications for transfer of data between the servers. A user makes the specific demand for the products to purchase from an interface provided. User demands are used to generate Mobile Agents for retrieving information spread around the web i.e. other web application. Each server authenticates the mobile agents using an internal key generated by the proposed system. Data demands and response are encrypted resulting in high confidentiality between the web applications under communication. Various access levels for the different category of mobile agents for providing deep levels of data to them has been created.

The work applies Malicious Agents, various Mobile Agents needs of different Access Levels, total time required by a mobile agent in collecting complete information etc.

VI. RESULTS & DISCUSSIONS

This paper provides various researched solutions to some agent security issues, such as data confidentiality, code integrity and access control and authorization, but only shows what solutions are out there for each specific problem and do not propose a specific and unified solution.

Table 1: Processing Time of mobile agents incurred during the execution processes.

MOBILE AGENT TRANSACTION OCCURRENCE	PROCESSING TIME IN MS
1	714
2	676
3	741
4	430
5	585
6	170
7	176
8	117
9	155
10	182
11	303
12	153
13	120
14	290

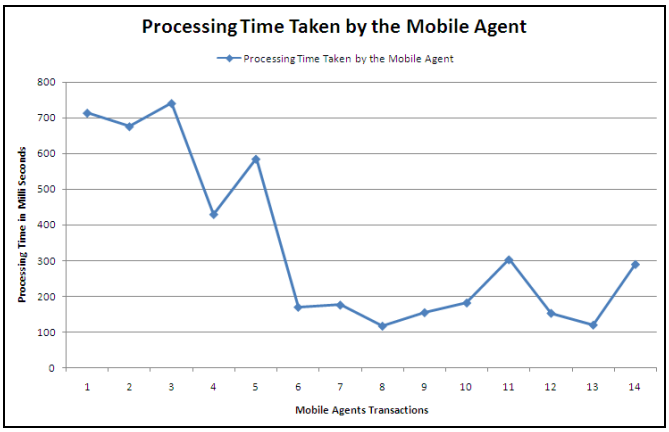

Fig 3: Graph Showing Processing Time Taken by the Mobile Agent

Inference: From the readings and graphs it is seen that the initial time taken in processing by the mobile agent is higher but it reduces and averages to around 200 ms after 5 occurrences. This behaviour is expected because the initially the Mobile Agent code is loaded in memory and database queries are executed and buffers are made for the same, whereas after some occurrences these times are reduced and only processing time is required majorly. The slight variations in later executions are also expected as the network latency and load on server will affect the processing time.

Table 2: Data Transferred with Mobile Agents during the Executions

MOBILE AGENT TRANSACTION OCCURRENCE	LOAD CARRIED BY MOBILE AGENTS IN BYTES
1	40
2	40
3	41
4	41
5	41
6	41
7	40
8	40

9	41
10	41
11	40
12	41
13	40
14	40

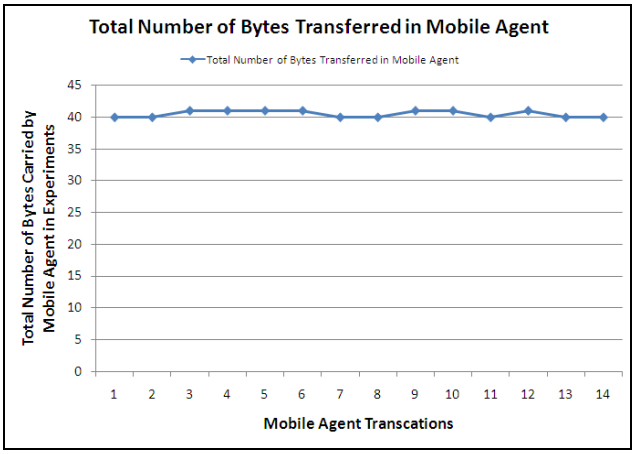

Fig 4: Graph Showing Total Number of Bytes Transferred in Mobile Agent

Inference: From the graph it is seen that the number of bytes being carried by the mobile agent is almost same and difference might be due to different bytes required for the price money of the items purchased.

REFERENCES

[1] Xu Xiao-Long; Xiong Jing-Yi; Cheng Chun-Ling, "The model and the security mechanism of the information retrieval system based on mobile multi-agent,"Communication Technology (ICCT), 2010 12th IEEE International Conference on , vol., no., pp.25,28, 11-14 Nov. 2010 doi: 10.1109/ICCT.2010.5689164

[2] Sulaiman, R.; Sharma, D.; Wanli Ma; Tran, D., "A Multi-agent Security Architecture," Network and System Security, 2009. NSS '09. Third International Conference on , vol., no., pp.184,191, 19-21 Oct. 2009 doi: 10.1109/NSS.2009.78

[3] Vieira-Marques, P.M.; Cruz-Correia, R.J.; Robles, S.; Cucurull, J.; Navarro, G.; Marti, R., "Secure Integration of Distributed Medical Data Using Mobile Agents,"Intelligent Systems, IEEE , vol.21, no.6, pp.47,54, Nov.-Dec. 2006 doi: 10.1109/MIS.2006.120

[4] Rui A. Martins, Manuel E. Correia, Alexandre B. Augusto, "A Literature Review of Security Mechanisms Employed by Mobile Agents", 1Open Federated Environment for Leveraging of Identity and Authorisation, 2012 IEEE

[5] Shilpa Budhkar, Anshita Mishra, Ferdous A. Barbhuiya, Sukumar Nandi, "Security in Mobile Agent Systems with Locator Mechanism", 1st Int'l Conf. on Recent Advances in Information Technology, RAIT-2012, 978-1-4577-0697-4 © 2012 IEEE

[6] M. Vigilson Prem, S. Swamynathan, "Securing Mobile Agent and its Platform from Passive Attack of Malicious Mobile Agents", IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012, ISBN: 978-81-909042-2-3 ©2012 IEEE

[7] Hedi Dhouib, Adlen Loukil, Ahmed Chiheb Ammari and Abderrazek Jemai, "Proactive mobile agent security:A new access control approach based on the risk analysis", 978-1-4673-1107-6 (c) 2012 IEEE

[8] Benjamin Henne, Christian Szongott, Matthew Smith, "Coupled Multi-Agent Simulations for Mobile Security & Privacy Research", 978-1-4673-1703-0 © 2013 IEEE

[9] w. Li, T. Zhao, w. Zang, "Summary-based information retrieval model", Jounal of Software, vol. 19 no.9, pp. 2329-2338, September 2008.

[10] X. Xu, R. Wany, "The Agent-based information retrieval model with multi-weight ranking algorithm", Journal of Electronics & Information Technology, vol. 30 no.2, pp. 482-485, February 2008.

[11] S. Gui, L. Li, Z. Peng, "Network information retrieval method based on information resource catalog system", Geomatics and Information Science of Wuhan University, vol. 33 no.! I, pp. 1202-1205, November 2008.

[12] http://en.wikipedia.orglwiki/InformationJetrieval