

DEVELOPMENT OF A TWO-LEVEL MOBILE AGENT SECURITY MODEL USING ADVANCED ENCRYPTION STANDARD ALGORITHM

Adegbite G.A, Awokola J.A and Ajala F.A
Department of Computer Science and Engineering,
Ladoke Akintola University of Technology, Ogbomosho, Nigeria.
gbabenson4luv@yahoo.com

ABSTRACT

Intelligent Mobile Agent has drawn a tremendous amount of attention from researchers in internet computing recently as it promises to provide an elegant and efficient way of solving complex distributed problems, as well as offering a new approach to human-computer-interaction. Security is in fact a significant concern with mobile agent based computing as the agent itself is vulnerable to malicious hosts and the host must protect itself from rogue agents. Existing security models developed to address the above issues were based on a one-level security method whose security cannot be satisfactorily evaluated and guaranteed. The fact that the security of a mobile agent system can be improved by the use of a two-level security technique, form the major focus of this research work.

This work proposes the development of a two-level security model which will implement the closed network and agent tampering prevention techniques for first and second level respectively. Advanced Encryption Standard (AES) Algorithm that uses a 192-bit encryption key will be adopted to provide security for confidential information. The performance of the proposed mobile agent security model will be evaluated using network performance and security measures.

This research work is expected to develop an improved mobile agent security model with a better performance with respect to response time, average round trip time and fault tolerance than the existing one-level security model.

1.0 INTRODUCTION

The progress in web technologies promotes the progress of electronic services. E-services have a tremendous growth in the recent years due to the advancements in Internet technologies (*Subalakshmi et al*, 2013). E-service is an interactive, Internet-based customer services and content-centered, determined by the customer and incorporated with associated organizational customer support practices and technologies with the goal of spiraling the service provider and customer relationship (*Rust and Kannan*, 2003).

Moreover in Internet, the real power of computers is realized through distributed, open, dynamic and heterogeneous systems which can interact, span organizational boundaries, and operate effectively within rapidly changing circumstances. In the context of addressing such requirements, agent technologies have been developed with the aim of providing solutions for the emergent problems and for managing the complexity that arise in this

arena (Luck *et al*, 2012). Software agents are used to implement highly modular e-services that are inter-operable, flexible, co-operative and autonomous.

The desire for more cost efficiency and less sub-optimal business processes drives the employment of agent technology in e-Business. The basic intelligent property of agents lies in the autonomy of operation, coordination and negotiation between agents for communication that leads to efficient problem solving. Such emerging agent technology has been applied in almost many fields like shopping, healthcare, online hotel booking (Subalakshmi *et al*, 2013).

However Security is the major concern in any network. The key dimensions of e-commerce security such as Access Control, Privacy/Confidentiality, Authentication, Non Repudiation, Integrity and Availability (Yasin *et al*, 2012), are very important in this work because the proposed mobile agent security model will target an online shopping scenario. Therefore, issues such as encryption, authorization, authentication, and non-repudiation should be addressed in a mobile agent system (Subalakshmi *et al*, 2013). Moreover, a secure mobile agent system must protect the hosts as well as the agents from being tampered by malicious parties.

Encryption algorithms play a big role in providing data security against malicious attacks where encryption time, memory output byte and battery power are the major issue of concern (Seth and Mishra, 2011). Advanced Encryption Standard Algorithm provides a balance with the least memory usage compared to Data Encryption Standard and RSA algorithms. Hence, AES is the most suitable algorithm for providing security in applications that will run on mobile devices. Advanced Encryption Standard algorithm also has a minor encryption time difference compared to Data Encryption Standard algorithm which has the least encryption time (Seth and Mishra, 2011). Because of the aforementioned advantages of the Advanced Encryption Standard algorithm, this work will use Advanced Encryption Standard (AES-192) algorithm to develop a two-level security model for a mobile agent system.

2.0 RELATED WORKS

This computing paradigm, which exploits code, data and state mobility, raises many new security issues that are quite different from conventional client/server systems. Agent servers that provide an execution environment for the agents to execute can be attacked by malicious agents. Similarly agents could be carrying sensitive information about their owners and should be protected from tampering by malicious hosts. The data collected by the agent from one host should also be protected from tampering by another host in the itinerary (Ahuja and Sharma, 2012). The various categories of security threats of a mobile agent system are classified into the following categories:

1) Agent-To-Platform category represents the set of threats in which agents exploit security weaknesses of an agent platform and launch attacks to an agent platform. This set of threats includes masquerading, denial of service and unauthorized access (Jansen and Karygiannis, 2000; Jansen, 2001):

2) Agent-To-Agent category represents the set of threats in which agents exploit security weaknesses of other agents or launch attacks against other agents. Many agent platform components are also agents themselves (Ahuja and Sharma, 2012). This set of threats includes masquerading, unauthorized access, denial of service and repudiation (Jansen and Karygiannis, 2000; Rizvi *et al*, 2010).

3) Platform-To-Agentcategory, represent the set of threats in which platforms are not trusted, to which agents migrate. This set of threats includes masquerading, denial of service, eavesdropping, and alteration (Jansen and Karygiannis, 2000; Jansen, 2001).

2.1 EXISTING MOBILE AGENT SECURITY MODEL

A number of solutions have been proposed to protect agents against malicious hosts. These can be divided into three types: agent-tampering detection, closed network and agent-tampering prevention(Kannamal and Iyengar, 2007).

Existing mobile agent security models are based on a one-level security technique which implements one of the three aforementioned security solutions.

2.1.1 CASE STUDY

The Shopping Consultant Agent System (SCAS) is a web-based mobile agent system that provides users with information on the products in an electronic marketplace. It is written in the Java programming language, on top of the Java Agent Development Environment (JADE). SCAS enables mobile agents to retrieve product information in an electronic marketfor users. An electronic market consists of hosts that sell products on the network. Each seller maintains a database of details of products available at that host. SCAS allows users to specify a set of products and the corresponding quantities they want to buy (Kannammal and Iyengar, 2007). An agent is created for the user, which will collect price details from hosts in the e-marketplace. The itinerary of the agent is determined before the agent is launched. After the agent visits all hosts specified in its itinerary, it returns to its sender and reports the prices.

This model is a one-level model which implemented only the principle of a closed network. In this model, a key server was introduced which provides a public key infrastructure for agents and hosts in the system. It stores the public key of participating hosts and mobile agents. It also provides the public key details to registered Launcher Agent and Remote Agents. This, in effect, establishes a closed set of hosts registered and known to the Key Server. The architecture of the security model with Key server as a component is shown in Figure 2.2. As indicated, the major components of SACS are client browser, Launcher Agent, Key Server, Remote Server, Hosts and Mobile Agent.

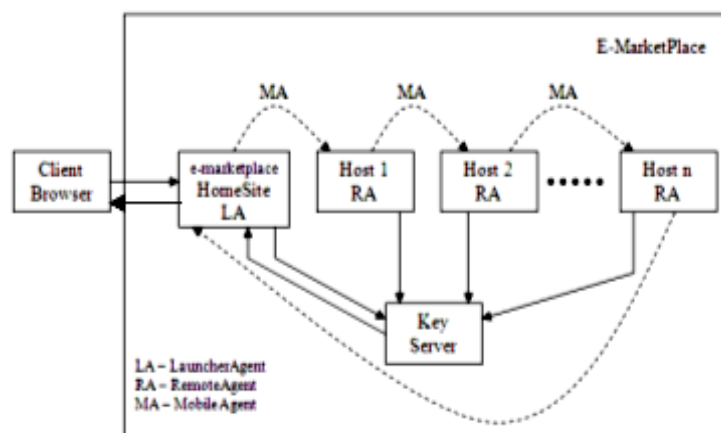


Figure 2.1: Architectural Components of Existing System Security Model

(Kannammal and Iyengar, 2007)

3.0 METHODOLOGY

This proposed model shown in figure 3.1 will implement a two-level security approach:

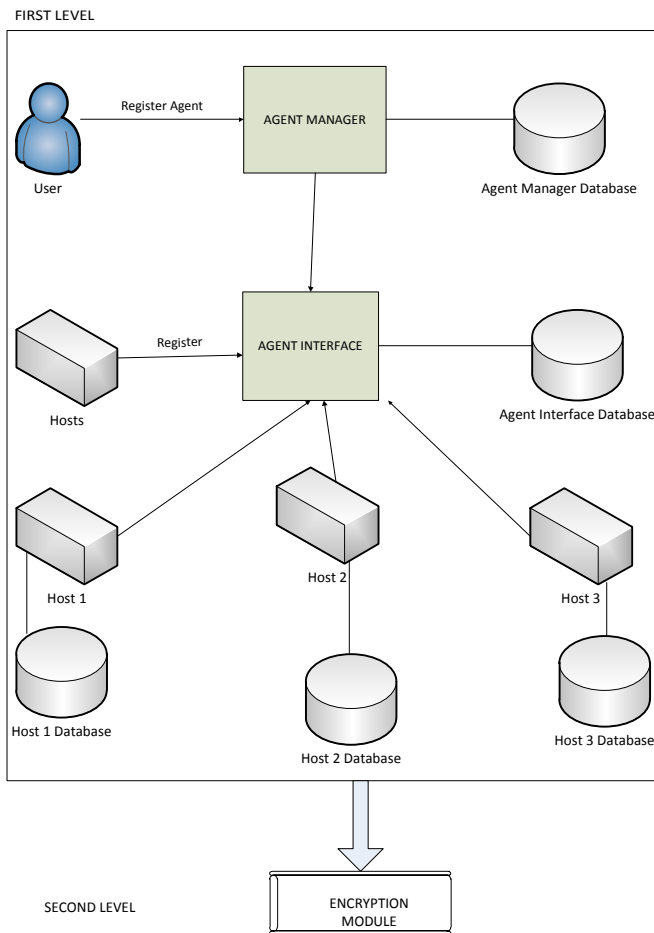


Figure 3.1: Proposed Two-level Security Model

The first level operates on the principle of a closed network. The object, namely Agent Interface and Agent Manager, is introduced into the model, which will provide a form of security for agents and hosts in the system. This, in effect, establishes a closed set of hosts and agents registered and known to the Agent Interface and Agent Manager respectively. The second level operates on the principle of agent tampering prevention. The encryption module uses Advanced Encryption Standard Algorithm (AES-192) to encrypt the agent's data on each host before moving to the next host and decrypts the agent data after passing through the network to the user. This proposed security model will be evaluated using network performance metrics such as response time, network delay, network bandwidth, average round trip time. The security of the proposed model will be evaluated by introducing a threat into the proposed system to determine how fault tolerant and attack-resistant, the proposed model would be.

4.0 CONCLUSION

The use of mobile agent on the internet is still developing, because of its security pitfalls. This paper reviewed literatures on mobile agent security models, proposed a model for secured mobile agent execution on its hosting servers using Advanced Encryption Standard (AES-192).

After proper performance evaluation of the proposed model, it is expected that it will satisfactorily solve the security issues of mobile agent computing if adopted for online e-commerce activities.

5.0 FURTHER WORK

The proposed security model should be used to develop an agent based online shopping system for effective implementation and evaluation of the two-level security model. An application to simulate the existing one-level security model must be developed to give room for wide comparison between the former and the proposed model using network performance and security metrics.

6.0 REFERENCES

- Ahuja, P and Sharma V (2012), "A Review on Mobile Agent Security", International Journal of Recent Technology and Engineering, Vol 1, pp 2-5
- Jansen W (2001), "Mobile Agents and Security", NIST Special Publication Vol 3, pp 5-6.
- Jansen W. and Karygiannis T. (2000), "Mobile Agent Security", NIST Special Publication, National Institute of Standards and Technology 80019, pp 5-7
- Kannammal A. and Iyengar N.Ch.S.N(2007), "A Model for Mobile Agent Security in E-Business Applications", International Journal of Business and Information Vol 3 pp 5-9
- Luck, M., McBurney, P., Preist, C (2012), "Agent Technology: Enabling Next Generation Computing (A Roadmap for Agent Based Computing)", Agent Link, Vol 23pp 31-34
- Rizvi I., Sultana Z., Sun B., and Islam Md. W.(2010), "Security of Mobile Agent in Ad hoc Network using Threshold Cryptography", World Academy of Science, Engineering and Technology Vol 23 pp 70-100.
- Seth M. and Mishra T. (2011) "Comparative Analysis of Encryption Algorithms for Data Communication", International Journal of Computer Science and Technology Vol 2, pp 1-3
- Subalakshmi R., Iyengar N.Ch.S.N, Khatna S. and Haleema S. (2013), "Agent Based Secured Online Hotel Booking System", International Journal of Computer Science Issues, volume 10, pp 2-6
- Yasin S, Khalid H and Rashid J.Q (2012) "Cryptography Based e-Commerce Security : A Review", International Journal of Computer Science Issues, Vol.9, No 1, pp132-137
- .