IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. VII (Jul – Aug. 2014), PP 62-66
www.iosrjournals.org

Distribution of RSA Public Key with Security Device based Identity for Multi-Agent secured Distributed Computing System

Sugumaran S[1], Kumaravelu R[2]
[1]*(Product Development, M/s Akashwa Technologies, India)*
[2]*(Research & Development, Vivekha Charitable Trust, India)*

Abstract: *In Mobile Agent Technology, interoperability between agents is indispensably to secure the data from malicious agents under Multi-Agent System. To protect data and agents from malicious attacks, the multi-agent system essentially needs to offer secure communication and access control mechanisms. Hence the digital signature and cryptosystem of asymmetric key based encryption and decryption provides secure communication and increases the confidentiality of accessing services designated only to a determined group of users. However, for the distribution of public key between agents we need to identify the trusted agent. The identification of trusted agent in a multi-agent platform is a challenging work. The technique of adapting USB Dongle is like a security device, which makes the identity of trusted agent, gives a robust mechanism for the identification of trusted agents in a Multi-Agent secured Distributed Computing System. In addition to that bio-metric based finger print sensor enables the owner's physical contribution to access the data.*

Keywords: *Asymmetric Key Cryptosystem, Authentication, Authorization, Dynamic Key Distribution, Hardware Identity Module (HIM), Multi-Agent System (MAS).*

I. Introduction

Mobile Agent based programming paradigm is an emerging archetype for structuring distributed applications over the Internet. A mobile agent is a composition of software and data which is able to migrate from one host to another autonomously and continue its execution on the destination host. Mobile agents are mainly intended to address problems of applications distributed over large scale and slow networks. Mobile Agents reduces communication costs by moving computation to or close to the host on which the target data resides and therefore it replaces remote procedure calls [1].

However, this type of Agent system introduces new ways of attacks and crimes since there is no physical contact between owner and their information. It tends to leakage of confidential information or unauthorized access. Poor access control mechanism also tends to ease of attacks towards the agents by malicious one. It results malfunctioning of agents in computational environment and generates several security issues.

Some of the threats associated with agent security are [2]

- Interception – due to breach of Confidentiality
- Interruption – due to loss of Availability
- Deception – due to loss of Integrity
- Usurpation – due to bad access control mechanism

The Security concerns against this kind of threats are [2]

- Cryptography
- Authentication
- Authorization.

The proposed concept intended to focus on the security of communication between agents in distributed computing system. This paper contributes various concepts for multi-agent distributed computing system such as (i) the Asymmetric Key Cryptosystem [3] for establishing secure communication between agents, (ii) Hardware Identity Module with USB Dongle [4] for authentication and identification of trusted agents, (iii) bio-metric based finger print sensor for user authorization [5] and (iv) dynamic distribution of public key for record less Key Management System.

For the development of multi-agent system, the JADE framework offers Run-time supports [1].

II. Proposed System Architecture

The Fig.1 shows architecture of the proposed system, which consists of server and client environment. The server environment consists of Key Manager (KM), Platform Managers like AMS, DF, RMA [1] and Service Providers (SPAs – Service Providing Agent). Client environment consist of Service Requestors (SRAs – Service Requesting Agent).

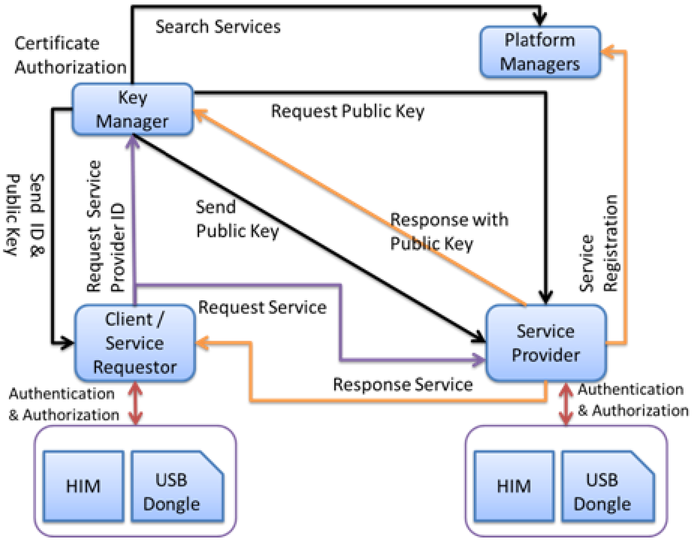

Figure 1 – System Architecture

Each SPA and SRA has a USB Dongle which is configured uniquely for the purpose of identifying a distinct and trusted agent in MAS.

1. Agent Description

1.1. Key Manager

It provides three important services such as

- Public Key Distribution – Public key of SPAs are distributed to SRAs (vice versa) during the establishment of communication between those agents. It brings dynamic concepts of distribution of public key and there is no need to maintain database for records all agents public key. It support for dynamic changing of keys for all the agents in any time and it results record less key management system.
- Certificate Authorization – Certificate of every agent participated in this system is authorized for the security purpose.
- Service Indexing – Process of searching SPA registered under this system, which provides services

1.2. Service Requesting Agent – SRA

It is also known as Client Agent which is interfaced with the user application for performing distributed computation.

1.3. Service Providing Agent - SPA

The Service Providing Agent provides several services and they are registered in the Distributed Computing System environment.

While establishing communication between agents, they require a uniquely configured USB Dongle which contains Signature of user, RSA asymmetric key pair, and Hardware identification data and also a smart Crypto-Agent. A **Crypto-Agent** is small software loaded into the USB Dongle at the time of Dongle Configuration which performs read/write information from/to the Dongle like key file for encryption and decryption. It also enables the USB Dongle as strong identity module.

2. Dynamic Key Distribution and Session Establishment

For establishing session between two agents, sender needs Public key of receiver for encryption and receiver needs Public Key of sender for decryption of message, which is illustrated in section-3.

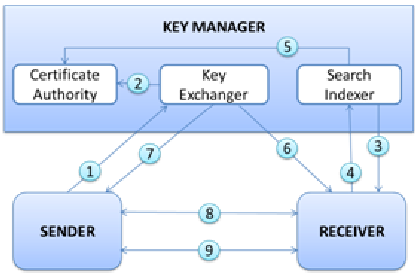

Figure 2 – Sequence of Key Distribution and Session Establishment

Before establishing a session, agents' Public key should be distributed to the corresponding agents. It is described as follows.

After completing the successful access control mechanism with USB Dongle the agent performs the following steps which is shown in Fig.2.

1. Client Agent sends request for SPA's ID with its Public Key and Certificate to the Key Manager
   - Certificate consists of their Public Key and Signature
   - Details of Service consists of type and name of service
2. Key Manager Calls Certificate Authority to authorize the SRA and it is briefed in section-4.
3. After successful authorization, Search Indexer searches the registered SPA with help of platform managers and forwards the service request to corresponding SPA.
4. SPA responds with its Certificate.
5. Key Manager calls Certificate Authority to authorize SPA.
6. After successful authorization, Key Manager has Public Key of both agents and it distributes Public Key of SRA to SPA.
7. Distributes Public Key of SPA to SRA
8. After receiving Public key of SPA, SRA starts to establish session with SPA.
9. Finally, communication is started.

In this key distribution mechanism, server does not need to maintain any database for storing the public key of all agents.

3. Secure Communication

The Fig.3 illustrates the asymmetric based encryption and decryption mechanism. In which, the sender agent (1) generates public certificate with public key using Crypto-Agent, (2) this certificate and message to communicate is encrypted with its Private key followed by the Public key of Receiver which results Cipher Message, (3) this Cipher Message is sent through communication channel in a network, (4) the Receiver receives that Cipher Message and decrypt with its Private key followed by the Public key of Sender, which generates Original Message and Sender's Certificate and (5) this certificate is used to identify the message sending agent.

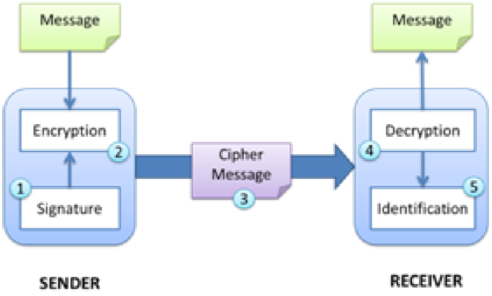

Figure 3 – Illustration of Secure Communication.

In this communication system, only the corresponding agent can read this message. It ensure the confidentiality and authenticity of information.

4. Identification of Trusted Agent

The USB Dongle which contains digital information which is used to authenticate the agent and authorize the user.

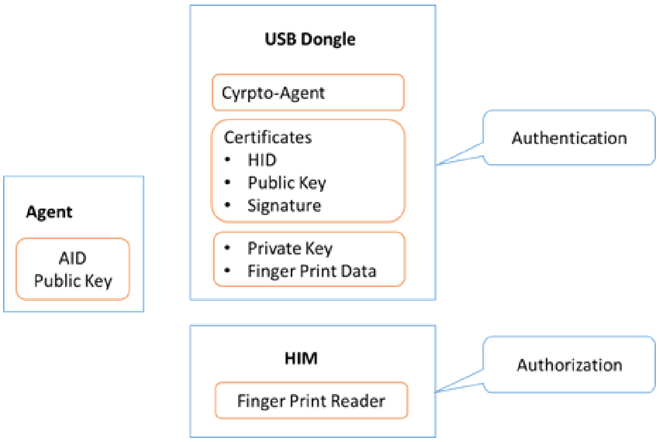

Figure 4 – Identity of Trusted Agent

The USB Dongle is grouped by three sections as shown in Fig.4. First section contains Crypto-Agent, is a tiny program ported into USB Dongle for retrieving information from the dongle. Second section contains Digital Certificate, it consists of unique Hardware ID, RSA Public Key and Signature of the User, and third section contains Private Information such as RSA Private Key and Finger print data.

4.1. Hardware Identity Module - HIM

Hardware Identity Module consists of finger print reader which is used to read the user's finger print for performing user authorization process to access the USB Dongle.

4.2. Authorization

The users finger print data read from HIM is compared with the Finger Print data stored in the USB Dongle by the Crypto-Agent to authorize the user who can use the USB Dongle.

4.3. Authentication

The Application Agent communicates with Crypto-Agent to identify the digital certificate stored in the USB Dongle. The method used to communicate with crypto-agent is known only to the trusted agent and it is known as **Secret Communication Method**. This process is done only after the successful authorization.

The Trusted Agent contains Unique Agent ID for agent Identification and RSA Public Key of Key Manager Agent which is a centralized agent situated in server platform for distributing the Public Key between agents. The Certificate Authority Agent in server platform authenticates and authorizes the agents, based on the information provided in digital certificate.

III. Significance of USB Dongle

A USB Dongle is a small piece of hardware that connects to a laptop, desktop or server computer. It supports plug and play technology.

Generally USB Dongles have two different technologies to protect software and files. First one is Authentication technology, the keys stored into the dongle is used to run application if desired key is found. Second one is code porting technology; a part of the code is ported inside the dongle. In the proposed system agents Key Pair is stored in the USB Dongle in the form of encoded manner and Crypto-Agent is ported into the dongle.

It has some important features like File Protection System, Code Port solution, Smart Technology and Automatic Self-locking Mechanism, Global Unique Serial Number and Built-in Timer.

IV. Conclusion

The proposed style of distribution of RSA public key with effective identification of trusted agents using USB Dongle gives secured communication and robust access control mechanism for the data transfers among the agents in the network against malicious attacks.

The bio-metric based finger print data is used for authorization which enables unique identity of user. The code like crypto-agent ported into the Dongle gives dominant key management techniques and therefore malicious crackers cannot get algorithms or data by physical interception. Combined features of these increases the level of security in communication system and it used to develop business application, bank application, military application and any secured distributed computing systems.

References

[1] Fabio Bellifemine, Glovanni Caire, Dominic Greenwood, Developing Multi-Agent System with JADE (John Wiley & Sons Ltd, 2007).

[2] Rodolfo Carneiro Cavalcante, Ig Ibert Bittencourt, Alan Pedro da Silva, Marlos Silva, Evandro Costa, Roberio Santos, A survey of security in multi-agent systems, Expert Systems with Applications 39 (2012), 4835–4846.

[3] Vanderson Botelho, Fabricio Enembreck, Braulio Avila, Hilton de Azevedo, Edson Scalabrin, Using asysmmetric keys in a certified trust model for multiagent systems, Experts Systems with Applications 38(2011), 1233-1240.

[4] Kumaravelu R, Kasthuri N, Distribution of Shared Key (Secret Key) using USB Dongle based identity approach for authenticated access in Mobile Agent Security, Internation Conference on Communication and Computational Intelligence (2010), 558-562

[5] Salvatore Vitabile, Vincenzo Conti, Carmelo Militello, Filippo Sorbello, An extended JADE-S based framework for developing secure Multi-Agent Systems, Computer Standards & Interfaces 31 (2009), 913–930.