Mobile Agent based realization of securely Question Distribution System

Myat Kalyar Khaing1, Moe Moe Aye2

1Dept of IT, Mandalay Technological University, Mandalay, Myanmar, E-mail: myatkalayarkhaingmu@gmail.com.
2Dept of IT, Mandalay Technological University, Mandalay, Myanmar, E-mail: moeaye255@gmail.com.

Abstract: Mobile Agents are autonomous software entities that can migrate from one computer to another, halt their executions on one host, transfer to another host, and continue execution from where it left off on the remote host. They offer several advantages over traditional methodologies such as reduction the network load, overcoming network latency, executing asynchronously and autonomously and adaptation dynamically. In this paper, we present a new solution for implementation of flexible protection mechanisms in the context of the mobile agent systems. The security enhanced agent, Question agent carries examination questions to the examination centers that can achieve many benefits such as time saving, and relief of human. Moreover, the system can also be enhanced by encrypting and decrypting the question with the DES algorithm to achieve the secrecy, confidentiality and to distribute the questions to the exam centers with secure manner. This system presents a mobile agent-based system for secure question distribution.

Keywords: Decrypt, DES, Encrypt, Exam Question, Mobile Agent.

I. INTRODUCTION

Agent is a software agent that performs activities on user’s behalf, when given instruction. They are used to execute asynchronously and autonomously without intervention from the user and to perform its task and save any results until its connection to the user is re-established. In addition to this, saving network bandwidth and reduction of network latency can also be achieved. Therefore, they are being used in an increasing variety of applications, ranging from relatively small systems such as assistants to large, open, mission-critical systems and for developing software applications in many fields. However, mobile agents have many security problems. These security problems have become a bottleneck in the development and maintenance of mobile agent systems, especially in security sensitive applications. An agent cannot carry sensitive data in a form that can be used on untrusted parties. Therefore, that data must be carried in encrypted form so that security can be achieved.

In education field, distribution of questions to exam centres is very vital and sensitive and can be implemented by only extracting the advantages of Mobile Agent. Security also plays an important role in it as the leakage of questions is illegal. For the security, DES algorithm provides for secrecy and confidentiality. In this kind of application, to get several advantages, distribution exam questions can be done with the combination of Mobile agent and DES algorithm. The system would help save money and time to distribute questions to exam centres and reduce labour force. Therefore, this intends to use mobile agents and DES to provide benefits for secure question distribution system.

II. SOFTWARE AGENTS

A software agent is a computer program that has autonomous behavior and represents some entity. It has authority (delegation) and reacts and learns about environment. A software agent communicates using high-level Agent Communication Languages (ACLs) [7]. Software Agents are able to live in many different settings like computers, operating systems, databases and they are up to very different tasks [8].

A. Stationary Agent

A stationary agent executes only on the system where it begins execution. If it needs information that is not on that system or needs to interact with an agent on a different system, it typically uses a communication mechanism such as remote procedure calling (RPC) [9].

B. Mobile Agent

A mobile agent system is a distributed computing paradigm. It is not bound to the system where it begins execution. It has the unique ability to transport itself from one system in a network to another. The ability to travel allows a mobile agent to move to a system that contains an object with which the agent wants to interact and then to take advantage of being in the same host or network as the object [9].

III. MOBILE AGENTS

A mobile agent migrates from one machine to another under its own control. It decides which locations to visit and what commands to execute. Interaction with the original source isn’t required and mobile agents can suspend execution at any time and migrate to a new host [1].
agent composes of two things: data (data collected and process states) and code (instructions that direct the behavior). It is carrying both its data and the code from one host to another. After arriving, it continues with execution where it stopped. It is mobile agent that should be able to execute on any machine within a network, regardless of the processor type or operating system. And agent code should not have to be installed on every machine that the agent could potentially visit; it should transfer with the agent’s data automatically [2]. This illustrates as shown in figure 1.

![Figure 1. Mobile Agent Paradigm.](image)

**A. The Lifecycle Model**

The life of a mobile agent is modeled with the stages it goes through called lifecycle model in figure 2. The states are Creation of the agent is done only once when new agent is created. Every agent gets its unique id, initial state and then it is prepared for further instructions. Starting is done each time when the agent arrives to a new host. It is the agent that has its own thread of execution and can execute asynchronously. All the agents are executed in parallel on the host. After deactivation, the agent stops all its calculations and stores its state and intermediate results to a disk. It is the states of the agent objects that are exported to a byte stream and later, they are reconstructed from the byte stream [3]. The deactivation can also be used for making checkpoints before performing some unsecured operations or moving to unknown host. To prevent confusion or errors, before using the checkpoint for creation, it must be absolutely certain the original agent is deactivated [4]. Disposal that means the agent terminates all its activity and frees all resources it’s using. After that, its state is lost forever. It is cloning that is process of making multiple clones of an agent using object serialization. It is used when more than once agent is needed for completing the task.

**B. Mobility**

The mobile agent has the most important issue is their mobility. There are two basic models of migration: weak and strong migration. The agents used two mechanisms of migration between the hosts: RMI (widely used) or through sockets. RMI is a feature of Java Developing Kit 1.1 (JDK 1.1) where a process can invoke Java public method of remote process. An agent, using RMI migration, firstly, sends a message to his local host demanding transfer to the new host, then the local host connects with the requested new host and initializes the transfer invoking public method on the remote host in figure 3. From this point, the remote host is responsible for directing the transfer. First, the remote host invokes Begin Transfer method on the local host. The local host serializes the agent and prepares it for transfer. The next step is transfer of resource and data of the agent, using RMI for initializing. Finally, the remote host informs the local host that the transfer is completed and it restarts the agent on the new location [5].

![Figure 3. Agent migration using RMI.](image)

In the migration mechanism that uses sockets, the idea is to convert the agent data and code to byte array that would be protocol independent. To do this, it is the agent that invokes public method on the local server after which it is serialized and prepared for transfer by passing it through multiple layers. Being prepared, the agent can be transferred to the new location by using standard transport protocols (e.g., TCP/IP) in figure 4.

![Figure 4. Migration through sockets.](image)

**C. Communication**
Mobile Agent based realization of securely Question Distribution System

The computer science has produced many communication mechanisms that are used in mobile agent’s systems. The most used ones are:

**Procedure call (synchronous) mechanism:** An entity A calls entity B to do a service during which the entity A is blocked. It enables procedure nesting. It is fast and easy to follow through programs’ follow of execution. The disadvantages are that it is synchronous and difficult to parallelise. RMI is such mechanism.

**Callback (asynchronous) mechanism:** An entity A calls an entity B to do a service but continues on with its task. The entity B, when it finished, calls back and gives the result to the entity A. It permits truly asynchronous processing but it is complicated and difficult to follow [6].

**Mailbox mechanism:** Somewhere between previous two mechanisms. An entity A calls entity B for a service and tells it to put the results into mailbox.

The entity A continues on its task, periodically checking its mailbox if the results are there. This is more difficult to implement but it’s asynchronous and easy to follow [6]. The most of the mobile agent systems use more than one of these mechanisms as well as broadcast or multicast mechanism for sending a same message to multiple receivers.

**IV. SECURITY OF MOBILE AGENT**

Mobile agents are processes which can autonomously migrate to new hosts. Despite its many practical benefits, mobile agent technology results in significant new security threats from malicious agents and host. The primary added complication is that, as an agent traverses multiple hosts that are trusted to different degrees, its state can change in ways that adversely impact its functionality [10]. Therefore, security is a fundamental concern for a mobile agent system [11]. Agents can communicate with other agents and humans. Just as an agent’s communication with its environment needs to be protected, so does its communication with other agents and humans [12]. The use of mobile agents raises a number of security concerns. Agents need protection from other agents and from the hosts on which they execute. Similarly, hosts need to be protected from agents and from other parties that can communicate with the platform [12]. Communication security properties are issues relating to the identification and authentication of the sending and receiving parties. These properties are confidentiality, data integrity, and authentication of origin, availability and non-repudiation [12].

Confidentiality is the assurance that communicated information is not accessible to unauthorized parties. Data integrity is the assurance that the communicated information cannot be manipulated by unauthorized parties without being detected. Authentication of origin is the assurance that communication originates from its claimant. Availability is the assurance that communication reaches its intended recipient in a timely fashion. Non-repudiation is the assurance that the originating entity can be held responsible for its communications [12]. The integrity of the data collected by a mobile agent might be protected using a cryptographic technique [13]. Encryption allows an agent to carry encrypted code or information. The encrypted data can be decrypted when the private information is accessed by the valid recipient.

**A. DES Algorithm**

DES is adopted in 1977 by the National Bureau of Standards (NBS), now NIST and is the most widely used encryption algorithm in the world. For DES, data are encrypted in 64-bit blocks using a 56-bit key. The algorithm transforms 64-bit input in a series of steps into 64-bit output. The same steps, with the same key, are used to reverse the encryption. It provides for secrecy and confidentiality. At the left-hand side of the figure 5, the processing of the plaintext proceeds in three phases. First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input. This is followed by a phase consisting of 16 rounds of the same function, which involves both permutation and substitution functions. The output of the last round consists of 64 bits that are a function of the input plaintext and the key. The left and right halves of the output are swapped to produce the preoutput. Finally, the preoutput is passed through a permutation that is the inverse of the initial permutation function, to produce the 64-bit ciphertext. The right hand portion shows the way in which the 56-bit key is used. Initially, the key is passed through a permutation function. Then, for each of the 16 rounds, a subkey (K) is produced by the combination of a left circular shift and a permutation. The permutation function is the same for each round but a different subkey is produced because of the repeated shifts of the key bits [14].

![Figure 5. General Depiction of DES Encryption Algorithm.](image)

**B. Architecture of the Proposed System**
This session presents the architecture of the proposed system which aims to integrate the use of mobile agents and DES in the distributor of the question to the exam centers from the Question Distributor securely. The overview of the proposed system is illustrated in figure 6.

![Overview of the Proposed System](image1)

**Figure6. Overview of the Proposed System.**

There are three agents in the proposed system, namely Deliver Agent, Question Mobile Agent and Receive Agent. Deliver Agent is a stationary agent at the Question Distributor and it needs to be run all the time to start the proposed system. The function is to encrypt the question with key and create the Question Mobile Agent. After the question has been encrypted, the system then creates Question Mobile Agent to distribute the encrypted question. Question Mobile Agent is a mobile agent that carries the encrypted question to the exam centers. At exam centers, Receive Agent, a stationary is created. When the Question Mobile Agent arrives, it receives the encrypted question and then decrypts that question with key. The tasks of Deliver Agent are shown in figure 7.

![Deliver Agent](image2)

**Figure7. Deliver Agent.**

The tasks of Question Mobile Agent are illustrated in figure 8.

![Question Mobile Agent](image3)

**Figure8. Question Mobile Agent.**

The tasks of Receive Agent are shown in figure 9.

![Receive Agent](image4)

**Figure9. Receive Agent.**

V. IMPLEMENTATION RESULTS

In this session, some of the user interfaces are described to illustrate how the questions are distributed securely to the exam centers. The figure 10 shows the creation of Distribute Agent. Distribute Agent, a stationary agent, creates to encrypt the question at the Question Distributor site.

![Creation of Distribute Agent](image5)

**Figure10. Creation of Distribute Agent.**

When the question is needed to encrypt, the question distributor must log in as shown in figure 11.
After the log in attempt had been successful, then the question to be encrypted can be loaded as shown in figure 12. And then, it is encrypted using DES with the key. To distribute the encrypted question to exam centers, the encrypted question can be seen in figure 13. To distribute the encrypted question to exam centers, Distribute Agent creates Question Agent and provides the itineraries of the exam centers to the Question Agent as shown in figure 14. After getting the itineraries of the exam centers, Question Agent is dispatched to the corresponding exam centers to distribute the questions.

When the question agent arrives at exam centre, then the decryption process begins as shown in figure 16. When the question is decrypted with the key at the exam centre, it has been saved the directory as shown in figure 17.
VI. CONCLUSIONS

“Mobile Agent based realization of securely Question Distribution System” is presented in the paper. The proposed system achieves faster and more accurately many examination questions by using mobile agent. It can save network bandwidth and overcome network latency by using mobile agent and provide secure distribution for examination questions by using DES algorithm. Therefore, secrecy and confidentiality can be obtained and the system can reduce the labor force for sending examination questions. Moreover, it can save time and money for distributing examination questions to examination centers.

VII. ACKNOWLEDGMENT

I would like to greatly thank my supervisor, Dr. Moe Moe Aye, Associate Professor of Mandalay Technological University for her valuable advice, helpful comments, her precious time and pointing me in the right direction during the course of my research. Her encouragement and general guidance helped me to develop my research with good results, improve presentation skills and finish this dissertation. I would like to express my heartfelt thanks to all my teachers, Mandalay Technological University, for their kindness support during M.E course work and their valuable comments for improving my research in all my seminars.

VIII. REFERENCES