Digital Certificate Mobile Agent Technologies in Distance Learning

Dong-Liang Lee \(^1\) and Lawrence Y. Deng \(^2\)

\(^1\)Dept. of MIS, St. John’s University
\(^2\)Dept. of CSIE, St. John’s University
Tamsui, Taipei, R.O.C.
lianglee@mail.sju.edu.tw

Abstract

Security issues are become more and more important in network application. This paper proposed an application of distance learning which integrated with Citizen Digital Certificate (CDC) Public Key Infrastructure (PKI), including the grade uploading, student information inquiring, and electronic documentation flow control. We integrated a tracking and persistent agent-based mobility management system in the case of distance learning. The main purpose of this system is addressed to achieve the universal access objective. We addressed to solve the problems in case of the data transferring in the network, such as eavesdropping, snooping, modification, masquerading and repudiation. And this would improve the efficiency of entire computerize procedure of electronic campus policy totally which in the following projects: Grade Processing System and Governmental Autographing System, etc. Especially, the Grade Uploading System was the first time to integrate with CDC. This experience was very important to integrate/generate the most secured application system in the Distance Learning.

Keywords: Citizen Digital Certificate (CDC), Public Key Infrastructure (PKI), Distance Learning, Digital Certificate, Mobile Agent.

1. Introduction

As the popular of the information technology and internet accessing, the distance learning was a very important issue in the world. As usual, the information broadcasting in the campus was based on traditional medium, like poster, leaf and campus news. At this point, there is a significant revolution on the limitation of the information transmission because of the real-time benefits on the network (include multimedia, communication, and high performance computer). This benefit also made user more disbelieve due to the open environment on the Internet; you could not get any protection on those digital documents which were transmitted on the network [1][2]. Therefore, the information security should be founded on a completed system that provided identification authentication, non-repudiation and exchangeable information. [3][4]

Besides, many marketing and technical terms under which agent supports in desktop, Internet, Intranet and so on. With the growing of network, likewise, the application-driven agents also provide many specialized facilities such as information retrieval agent, mobile agent, process automation agent, collaborative customization and database agent. The ever-increasing growth of mobile agent applications are encouraging research aimed at the wide spread communication infrastructure. In [5], the mobile agent paradigms and technologies were discussed. The relationships among paradigms and technologies for mobile agent are showed in Table 1.

Table 1. Relationships among paradigms and technologies

<table>
<thead>
<tr>
<th>Paradigms</th>
<th>Technologies</th>
<th>Client-Server</th>
<th>Remote Evaluation</th>
<th>Mobile Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weakly mobile</td>
<td>Message-based</td>
<td>Code is a single instruction</td>
<td>Well suited</td>
<td>States as data restoring</td>
</tr>
<tr>
<td>Strongly mobile</td>
<td>Code is a single instruction</td>
<td>Manage migration</td>
<td>Move state back and forth</td>
<td>Well suited</td>
</tr>
</tbody>
</table>

In this paper, we devoted our attention to the mobile agent issues especially in universal access objective. Since, mobile agents often work on heterogeneous network and operating system environment. Therefore, integrated logical interfaces to access physical structure via mobile agent application is become more and more important [6]. For flexibility, mobile agents can be accepted as a design paradigm like object-oriented programming or client/server computing [7]. So, we proposed a tracking and persistent agent-based mobility management system with security concerned in the case of distance learning to illustrate the entire processes.

The remaining parts of this paper were organized as follows: The related work was discussed in section 2. A mobile agent system architecture model describes server
agent and client agent components are illustrated in section 3. The limitations and possible solutions are then discussed in section 4. And finally, we discuss our conclusion and extensions in section 5.

2. Related Work

2.1 Public Key Cryptography

The technology of Public Key Cryptography was proposed by Diffie and Hellman in 1976[8], and the first RSA Cryptosystem also developed by Rivest, Shamir and Adleman in 1977[9]. Each cryptosystem had its own characteristic in public key infrastructure individually. According to cryptography, the Key is a unit digits which created by a special way. The Public Key Infrastructure (PKI) system consist a pair of Keys --- the Public Key and the Private Key. Each pair of Keys was identical and unique, there were a corresponding mathematical relationship between the Public Key and the Private Key, and the generated procedure was irreversible. And the Private Key could not figure out from the Public Key practically. The Public Key was open to public in PKI system, but the Private Key was saved in privacy. It was possible to decode with an encrypted Public Key which was pair to the specified Private Key previously. At the same time, it also needed an encrypted Private Key to decode the coded data which pair to the specified Public Key formerly. Therefore, we need to establish an acceptable Public Key on both side in the network, and this process should be verified by a certain procedure under a righteous Certificate Authority (CA) which had confidence in both two ends fairly. In the electronic identity authentication system, there was a common problem that the Certificate relationship was built between an end-user and particular computer system eventually. This was impossible to make this relationship expand to more end-users and more networking systems, and the public identity authentication system will not be come true at all. Therefore, PKI structure provided a certificate system for public identity authentication correctly, that is the correction of every user’s authentication is accuracy and validity for sure.

2.2 Digital Signature

Please do not revise any of the current designations. Beside the style of an autographed document was different, the traditional stamp or personal signature would have the same content even the documents were not alike. This was the major difference between the traditional stamp that we used in Oriental and personal signature. Eventually, the Digital Signature was the calculated result of which generated through the Private Key that owned by the electronic document and dispatcher. And the Digital Signature was interrelated to the content of the electronic document. Therefore, there would have various Digital Signatures that came with numerous documents even they were generated by the same owner. Currently, the Digital Signature was based on the Open Public Key Cryptosystem of the Cryptography; it also named “Asymmetric Cryptosystem” as well. It was paired with Digital Signature and Digital Envelope basically. The dispatcher used his own Private Key to ‘sign’ with the messages by the Digital Signature that generated by the productive mechanism of signature. And the accepter of the Digital Signature would verify its validity by the dispatcher’s Public Key that generated by the productive mechanism of signature similarly. This would make the contents of electronic document to give all consideration in confidential, integrity, authentication and non-repudiation [11]. The productive mechanism of signature was a method or a procedure which produced a Digital Signature by the dispatcher; it also treated as a mathematical algorithm. When the dispatcher signed the Digital Signature, there was a value need to input in the algorithm with his own Private Key and electronic document which would be signed. And the Digital Signature of this electronic document would be obtained after the execution of the algorithm. The productive mechanism of signature was also useful to accepter to verify the validity of the method or procedure in Digital Signature. When the accepter received the signed electronic document which delivered from the dispatcher, it was necessary to verify the validity for this Digital Signature through previous mechanism, including electronic document, Digital Signature and the Public Key of the dispatcher.

2.3 Mobile Agents

Mobile Agents is an agent encapsulates the program that a receiving server is to execute, the data comprising the program’s arguments and state. Figure 1 shows a mobile agent scenario. Software agents that transport themselves form a client computer to various servers for remote execution.

The concept of agent-based software engineering is discussed in a survey paper [12]. The author presents two important issues: agent architecture and agent communication language. Agent architecture, on the other
hand, includes network infrastructure and software architecture that ensures agent computing. An open agent architecture for kiosk-based multimedia information service is proposed in [5]. Agent communication languages allow agents to share information and send message to each other.

2.4 Mobile Agent Programming Language

Mobile agent needs a programming language that lets users define the role of their agents as they travel across a network. The following languages can be used for specific niches as well.

KQML: A language developed through ARPA knowledge sharing effort aimed at developing sharable large-scale knowledge bases to enable agent-to-agent communication and knowledge. KQML is suitable for development agent prototype for integration into existing application [13].

Java: Java is an interpreted, multithreaded, and secured platform-independent language suitable for agent application. The multithreading and built-in security features give Java an edge in the implementation of interactive e-commerce applications [14].

ActiveX/OLE: The programming technologies from Microsoft Corporation. Microsoft’s answer to Java embracing both Java and Component Object Model (COM) based on Object Linking Embedded (OLE). [15]

Tcl and Safe-Tcl: This is a machine-independent scripting language that uses email to transport agent procedures as contents of mail messages [16].

Telscript: A language proposed by General Magic. Telscript is an object-oriented language and agent-based operating environment designed for mobile agent [17].

3. Mobile Agent System Architecture

Before In this paper, we proposed a model to characterize the mobile agent system architecture. As Figure 2 illustrated, the mobile agent virtual society was composed within three cells: Pico cell, Micro cell and Macro cell. The Pico cell represented the client mobile agent. The Micro cell constituted by at least one client mobile agents (Pico cells) and one server agent. Several Micro cells construct a Macro cell. The following article describes the architecture of the Micro cell (Server side) and the Pico cell (Client side).

3.1 Micro Cell

A micro cell is composed of agent profiles/database, server agent and web server.

Agent Profile and Database:
- User personal environment setting information: This information forms strings, including the items the user chose with their needs for the environment.
- User Log Files: The log file plays an important part while agent carried back to agent server. The agent server will parse the log files with different catalogs, such as the course participations, the shopping experience, and so on.
- User personal information: The user may change his/her own personal information via the agent, the modification of the member databases.
- User submitting results: There is some information, which users can submit via the agent architecture, such as the questionnaire system, the pop-up quiz system. Agents won’t bring all of the submitted information, and some of that information will be sending back to the database with the functions provided in each subsystem.

![Macro Cell](image)

**Figure 2. A Mobile Agent Society Environment**

**Figure 3. Verification processes**

Server Agent:
The server agent contains four components: verification components, communication components, management components, and roles setting objects (agent...
characteristics) provider. As with non-mobile agent, the primary requirement is a method of delegating authority to the mobile agent.

- Verification components: provide the security-minded with agent delegation and authentication, privacy and access control. (the processes of verification in case of updating the student’s degree are shown as figure 3)
- Communication components: provide the universal communication tools, such as the chat (text), audio, video and windows message (annotation) application tools.
- Management components: provide the system management facilities, such as the administration, resource allocation and agent profiles modification functions.
- Roles setting objects provider: provide the application-driven/characteristic objects to the client agent to download those objects. (e.g. E-notebook, Authoring tool (for course design), questionnaire sub-system, lecture-on-demand and so on.)

3.2 Pico Cell

The client agent is the base unit (Pico cell) of the mobile agent society. The main elements of a client agent include the client profiles, object function loader and role setting components selector.

- Client profiles: User personal environment setting information, User Log Files, User personal information and User submitting results. (Those are same as the server side’s profiles/database)
- Role setting components selector: this component provide several of role templates for user, user can choose the agent’s role which represents the agent will possess some application tools and put to use in the society.
- Object function loader: after user had selected their role sets, the object function loader will download the related objects from server agent (Roles setting objects provider).

3.3 Operation

This section shows several examples of Mobile Agent operations. The examples illustrated three main phrases: (1) registration (2) communication (3) role setting.

When a user wants applying into a new society, the client agent is invoked to coordinate the updates between the server and subscriber. Figure 4 shows the operations for a mobile registration to be a new society’s member.

After the MMVS register system received the uses apply, it send a registration notification message to the administrator verification component (event 1, Figure 4). In this example (event 2), the administrator verification component sends a reject notification to the MMVS register system. Upon receiving response form administrator verification, the MMVS register system send a response back to the user (shown in the Figure 4 as event 3).

In event 4, the administrator verification records the registration acceptation message into the profile database. Event 5 is the acceptation response back to the user.

![Figure 4. Registration operating phase](image)

In the event that the client agent applies the roles setting objects, the server provides a set of commensurable application-driven components for the authorized agent. These operations were shown in Figure 6. The first two events handled the testing and verifying the agent status, and rejected the unauthorized login agents. The function of these events provided the delegation and authentication. Event 3

![Figure 5. Communication phase](image)
and 4 provided the role configurations. After the role configuration steps, event 5, 6 and 7 will record the user’s profile and dispatch the desired agent role’s objects to the user.

![Figure 6. Agent’s role setting phase](image)

### 4. Discussion: Limitations and Solutions

There were many focus issues occurred after the system constructed. We had received many diverse opinions such as plenty responses, valuable suggestions and important request from teachers and staffs’ feedback, although this made us much more challenge and difficulty when the system developing. But, for the system to implement certainly that the involution of administration’s authority was necessarily and essentially. We summarized some important issues as followings:

1. For the principals of the equitableness, publics and reasonableness in teaching’s evaluation. The teacher should provide completed information of its score record that in his course responsibly. This standard might reduce some disputation which caused of incomplete score record.

2. The System provided a Web page with fixed style or format (it combined with Ordinary score, Mid-term score, Final-term score and Semester score), and the data imported from the selected course database would be Course’s Name, Class’s Title, Teacher’s Name, Student’s List and so on. There was a convenient way to let teacher filled out the Mid-term score and Final-term score in his familiar software tools to evaluate the grade sequentially, and import those manipulative scores into the system through Web page. This approach would reduce the perplexity of direct output that was in various software tools, distinct number of record field, and dissimilarity of the field name.

3. There was an adjustable function for user that he could modulate the percentage of each item in Semester score calculation. It was possible to adjust one specified record/field with a reference explanation individually. Also it was able to get a static analysis on-line, analyze class grade data; of course, printing and saving functions were available too. It was complete record if the score data and other information were uploaded together which were the score data of all course, relative percentage value, exceptional processing, explanation of static analysis, etc.

4. It was encourage to all teachers to utilize the Grade Uploading System (GUS) in the promotion phase basically. There was a gift of IC Card Reader to come with the application of Natural Person Certificate, it also had several training course in Campus, and the Operation Manual in book and on-line learning were available at same time. There was a fully service that could satisfy to all teachers to increase their aspiration in GUS project.

### 5. Conclusions

In our experiment, it was possible to provide a fundamental for extensive application with identity authentication, non-repudiation and the information exchange was confidential and integrity. An agent-based mobility management system was introduced and the ways of constructing the application-driven mobile agent was addressed. We suggested a framework to model the mobile agent virtual society, which contained both mobile agent communication network and mobile agent evolution states. This approaches aspired to provide to the software developers who could get advantages in the agent computing and the management routine work. Also, the role-setting components are object-oriented approach. This approach not only gives the flexibly but also scalable in user’s utility tools. In out experiments, the application-driven mobile agent actually improved the persistent look-and-feel for roaming student in distance learning environment. The Grade Uploading System in SJU Campus has been a trial test since January 2004, and it also has started using on April 2004. There were hundred of course in the system at beginning, and the consequence got appreciative criticisms from teachers and staffs. We hope that, this study should be prolonged and applied to future communication network environment.

### References


