Object Oriented Modeling of Digital Certificate in E-learning

Dr. Sunil Karfoma1, Soumendu Banerjee2

1Associate Professor, Department of Computer Science,
The University of Burdwan

2Research scholar, Department of Computer Science,
The University of Burdwan

Abstract
The current trend of learning is e-learning. In e-learning, security plays a vital role. Security is the main concern which can never be neglected by any e-learning institutions. In e-learning system, all participants exchange many valuable documents electronically. During transmission of study materials from teacher to developer, hacker can damage or destroy those and there may arise some cases, when the teacher can deny of sending the study material. In this paper, we have considered transmission of the study materials from the teacher to developer, where authentication of study material can be done using digital certificate. For this reason, to provide confidentiality, authenticity and strong non-repudiation, we wrapped digital certificate in object oriented models utilizing the benefits of object oriented analysis and design, which is the current trend of software engineering.

Keywords:- Digital Certificate, E-learning, Use case diagram, Data flow diagram, Class hierarchy diagram, Sequence diagram

1. Introduction

E-learning, now-a-days is becoming a most popular form of Information and Communication Technology (ICT) based education system. In an online learning system, learner has no barrier of place, no need to move elsewhere, all the procedures like search of courses, checking course fee, paying course fee, registration, getting admit card, receiving study material, giving examination, getting mark sheet etc. all the processes related to learning are done through Internet. Internet, being an insecure network, security plays an important role here. The online transmission of study materials, mark sheets and all other important things, from teacher to developer and from developer to learner must provide security, because, during transmission of these materials through online, materials can be hacked or damaged by intruders[5]. Transmission of study material from teacher to developer, privacy, authentication and non-repudiation are three main issues[9], which can be obtained by applying digital certificate along with cryptographic techniques. Privacy is the main issue of security and here authentication means that the study materials, sent by the teacher, is authenticate or not. Non-repudiation means that no party can deny of sending the material. Here we restrict our discussion only on transmission of study material from teacher to developer using digital certificate to achieve above three aspects. In this process the teacher sends three part transmission (encrypted study material, digital signature and digital certificate) to the developer. Developer decrypts the study material and compares the recomputed hash values with the hash value of teacher. If the values are identical, the developer accepts the material, otherwise request the teacher to send the study material again. By use of digital certificate, not only the teacher can send the study material to the developer securely, but also this is helpful to build a trust relationship between the customer and the developer. In this competitive market, e-learning[7] institutes should emphasis on secure transmission. A digital certificate is simply an electronic message “signed” by the issuer of the certificate (known as Certificate Authority, CA) with that CA’s private key, so that it uniquely identifies the user holding the issued key pair.[10] In this paper we present, necessity and use of digital certificates and how a combination of digital signature[11] and digital certificate provides strong non-repudiation. Next, we concentrate on implementing digital certificate using object oriented modeling. The motivation behind such object oriented approach[6] is that, it is the recent trend of the software development making possible with the reuse of code[12]. Through inheritance, we have been able to eliminate redundant code, which are used by both communicating parties. Using data hiding feature of object oriented approach we can hide some secret keys, which is needed for implementing cryptosystem. Here, we use sequence diagram, use case diagram, data flow diagram and class hierarchy diagram for our proposed object oriented model. In section 2, we have drawn the DFD to analysis and design the object oriented feature of proposed model. In section 3, we have design the object oriented models like, Use case diagram, data flow diagram and the class diagram of the proposed e-learning system. Finally, we have concluded in section 4 by highlighting some future scopes.

2. Data Flow Diagram of Proposed Model
The data flow diagram is a graphical representation of a system, which contains the input data to the system, processes which has been carried out on these data and also the output data generated by the system[2][8]. Here we use two Data flow diagrams, shown in the figure1, and in figure2, in annexure. The data flow diagram, shown in figure1, in annexure, discusses about the secure transmission of the study material from the teacher to developer using digital certificate. Teacher sends the three part transmission (encrypted study material, digital signature and digital certificate) to the developer. The DFD, in figure2, in the annexure, discusses about the decryption of the study material, comparing of hash functions to verify digital signature and digital certificate at the developer’s end. If the hash functions are equal, then the signature and certificate is considered as unchanged and accepted for further use.

3. Proposed Object Oriented Models

This section contains the proposed object oriented model with the help of different object oriented analysis and design diagrams such as use case models, sequence diagrams and class diagrams.

3.1 Use case diagram

In this use case[8] model, we use three types of objects like, Certificate Authority, teacher and developer. The first use case model, shown in figure1, discuss about the creation of certificate of teacher by the Certificate Authority or CA. Certificate Authority first receive the public key of teacher and his identity proof. The CA does not direct receive these. Usually CA delegates Registration Authority for this purpose. For this reason, digital certificate is also known as a trusted third party system. After being sure about the teacher’s identity and the authentication of public key, CA creates the digital certificate for him and sends this to the teacher. In the second use case diagram, shown in figure2, discuss about the activities of teacher. Teacher creates his key pairs, public key and private key. Teacher sends the public key and identity key to the CA to create digital certificate, use developer’s public key to create encrypted message and his secret key to create hash function. Finally, teacher sends the encrypted study material, digital signature and digital certificate to the developer. The third use case diagram, shown in figure3, discuss about the activities of the developer. After receiving the three part transmissions from the teacher, the developer decrypts the study material, recomputed the hash functions and compares the recomputed values with the hash value of the teacher.

Figure1: Use case diagram for Certificate Authority

Figure2: Use case diagram for Teacher

Figure3: Use case diagram for Developer
3.2 Sequence Diagram:

A sequence diagram\[3][8] shows the interaction among objects as a two dimensional chart. The chart is read from top to bottom. Here we use two sequence diagrams, shown in the figure3 and in figure4, in the annexure. The sequence diagram, shown in figure3, in annexure, discusses about the transmission of encrypted study material, along with digital signature and digital certificate to provide security and authenticity, from teacher to developer. Next sequence diagram, shown in figure4 in the annexure, discusses about the decryption of the study material, re-computation of the hash functions from the digital signature and digital certificate and also of the verification of the digital signature and certificate by comparing the hash functions, which have been done at the developer’s end.

3.3 Class diagram for study material transmission:

The figure4 demonstrates the organization of class diagram\[4] showing how the teacher can authenticate to the developer using a combination of digital certificate and digital signature in object oriented approach.

![Class diagram](image)

**Analysis of Class Diagram:**

**Class Base:**

This class is publicly inherited by the class CA, short form of Certificate Authority. In the Base class we use five data members and one member function. From the five data members, four of them contain the public keys of the objects used here and one is used to store the hash value. The member function is used to find the GCD value of the given two co-prime numbers.

**Public members:**

- int \( P_{\text{developer}} \); // developer’s public key
- int \( P_{\text{CA}} \); // certificate authority’s public key
- int \( P_{\text{teacher}} \); // teacher’s public key
- int \( P_{\text{id}} \); // teacher’s identity number
- long double \( \text{hash} \); // hash function

**Class RSA:**

This class is also publicly inherited by the class CA. In this class, we use four data members. This class is used to store the two co-prime numbers and the study material, sent by the teacher to developer and the other two data members are used to encrypt and decrypt this study material.

**Public members:**

- int \( u,v \); // these are two co-prime numbers used to create public and secret key
- int \( N_{\text{developer}}, N_{\text{teacher}} \); // these are used to encrypt or decrypt the message
- char *\( \text{stdmat} \); // this is the study material (character string), sent to the developer by the teacher

**Class Teacher:**

This corresponds to the customer and it inherits the classes Base, RSA and CA publicly and it is inherited by both the classes Teacher and Developer. This class is used to store the data and functions of certificate authority. It stores the secret and public key of CA, certificate of the teacher; create by CA and two member functions for the hash function, to create certificate and the certificate calculation.

**Private member:**

- int \( S_{\text{CA}} \); // this is the secret key of CA, used to encrypt certificate

**Public member:**

- int \( N_{\text{CA}} \); // public key, used to encrypt or decrypt certificate long double \( \text{stdmat}[100] \); // holds the certificate
- long double \( \text{stc} \); // used to calculate sign hashed value
- long double \( \text{hash} \); // calculate certificate

**Class Developer:**

This corresponds to the customer and it inherits the class CA publicly i.e. it is in turn inheriting the classes Base, RSA and CA. Though it contains the public members of the Base, RSA and CA classes, it also has one private and
public data member and five public member functions. The private member is assign to the secret key of teacher, which is used to create digital signature. The array stores the study material of the teacher. The member functions are used to do the other processes like creation of keys, encryption of study material and the other tasks which have been done at the teacher’s end.

**Private Member:**

```
int S_teacher; //this is the secret key of teacher
```

**Public members:**

```
int fstmat[100]; //this array holds the study material after being converted into integers
void getdata(); //get study material and also creates the public and secret key
void format_stdm(); //used to format the study material into an integer array containing integer
long double enc(); //this is used to encrypt the study material
long double create_sig(); //it is used to create the digital signature Developer send(Developer); //this function sends three part (stdm, sig, cer) information to Developer
/*Here the send(Developer) function is actually calling the other three methods of this class and also the cer_cal() method of the class CA to calculate certificate.*/
```

**Class Developer:**

This corresponds to the Developer and it inherits the class CA publicly i.e. it is in turn inheriting the classes Base, RSA and CA. Except of containing the other public members of the Base, RSA and CA classes, it also has a private and public data member and some other member functions which are used to perform the tasks of the developer related to the study material.

**Private member:**

```
S_developer; //secret key of developer and it is used to decrypt the study material
```

**Public members:**

```
long double stdm[100]; //it stores received study material after decryption
void createkey(); //create public and secret keys for developer
void dec(); ///decrypts the encrypted message
void dformat_msg(); //used to get actual message after getting the decrypted formatted message
void dec_cer(); //decrypts the encrypted digital certificate
void dec_sig(); //decrypts the encrypted digital signature
void chk(); //invokes functions get_stdm(), chk_cer() and chk_sig() for authentication checking
void get_stdm(); //invokes decrypt() function to get the original study material
void chk_cer(); //invokes dec_cer() function to check the certificate
void chk_sig(); //invokes dec Sig() methods to verify the signature
```

The **driver program** is given below:

```
void main()
{
    CA c; //c is certificate authority
    Tchr t; //t is an object of the class Teacher
    Dev d; //d is an object of class Dev
    d.createkey(); //d creates his key pairs
    d=t.send(d); //t sends the encrypted study material, signature and certificate
    d.chk(); //d verifies signature and certificate and finally decrypts the study material
}
```

**6. Conclusion**

The object oriented implementation of digital certificate can be used for any type of transmissions in e-learning system to provide integrity, confidentiality, authenticity and strong non-repudiation. This object oriented model can also be used other online systems, like e-commerce, e-governance etc. Further enhancement of proposed object oriented model of Digital Certificate may be done with the state diagram, activity diagram etc. This proposed model can also be applied for other online transmissions like, transmission of study material from developer to learner, transmission of the scan copy of online transactions and also in other cases where authentication and non-repudiation is required and can be achieved using digital certificate.

**References**

AUTHOR

Dr. Sunil Karforma has completed B.E. (Computer Science and Engineering) and M. E. (Computer Science and Engineering) from Jadavpur University. He has completed Ph. D. in the field of Cryptography. He is presently holding the post of Associate Professor and the Head of the Department in the Department of Computer Science, The University of Burdwan. Network security, e-commerce, e-learning and e-governance are his field of interest in research area. He has published approximately 70 research papers in reputed National and International journals and proceedings.

Mr. Soumendu Banerjee has completed his B.Sc (H) in Mathematics and MCA from The University of Burdwan. Now, he is acting as guest lecturer at Tarakeswar Degree College, Tarakeswar, Hooghly. He is pursuing research in the Department of Computer Science, The University of Burdwan. He has published one International journal paper.

Figure 1: DFD for transmission of study material from teacher to developer.
Figure 2: DFD at the developer’s end

Fig 3: Sequence diagram for teacher
Fig: Sequence diagram for developer