OBJECT ORIENTED MODELING OF RSA DIGITAL SIGNATURE FOR SECURITY IN E-LEARNING

Dr. Sunil Karforma[1], Soumendu Banerjee[2]

[1]*Associate Professor, Dept. of Computer Science, The University of Burdwan*

[2]*Research Scholar, Dept. of Computer Science, The University of Burdwan*

ABSTRACT

One of the most recent trends of learning is E-learning. The main thing to concern about an E-learning system is that, this is fully controlled through online. It is being a public network; security always plays an important role. In this system teachers send their materials, for various purposes, to the administrator, through online. While sending these materials, hackers can change or destroy those. Digital signature can be used to detect whether the material is changed or not. In this paper, we have wrapped RSA Digital Signature algorithm in an object oriented model for implementation of authenticity of these study materials utilizing the benefits of object oriented analysis and design.

Keywords: Class Diagram, DFD, E-Learning, RSA Digital Signature, Use Case Diagram.

I INTRODUCTION

Like the other learning systems, teachers and administrators are the main components of e-learning system. All the communications, between teachers and administrators is mainly done through the Internet. Now-a-days, e-learning is also becoming a part of this competitive world. In e-learning system, teachers prepare study materials, question papers, mark sheets and they have to upload it securely to the administrator. While sending these confidential materials, digital signature can be used to detect whether the materials are modified by the hacker or not.

We have made an attempt to object oriented[1] implementation of RSA Digital Signature algorithm[2] for secure transmission[4,5,6,8] of study materials from teacher to administrator. In this context, teacher will send their materials with a signature, which will be also verified at the administrator end. If anyone tries to hack the message, the sign will be changed and the administrator can track it. We have utilized the benefits of object oriented analysis and design during our implementation.

In the section II, we have analyzed the system with the help of Data Flow Diagram[7] (DFD) and Use case diagram. Section III covers the proposed class diagram and code segment written in C++ language. Section IV contains all the figures. Finally, we have concluded in section V by citing some future scopes of improvement.

II. DATA FLOW DIAGRAM (DFD)

The data flow diagram[7] 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. The data flow diagram of material sending from the Teacher to Administrator is shown in the fig: 1, in section IV. Here teacher is sending the material and compute the hash value from the material using hash() function. The public key and the teacher's private keys are stored in the data store. Using the private key teacher is generating the signature and sends it along with the study material and public key to the administrator. Admin then again computes the hash value from the public key of Teacher and compare the hash values with the given hash value. If there is no change, then it is accepted otherwise take the required action.

USE CASE MODEL

In the use case model, we take two types of objects like, Teacher and Administrator. Here Teacher is generating the signed material and sending this material along with the signature to the administrator. The administrator compares the hash values and verifies if the material is hacked or not. Here we use two use case models.

In the first use case model, shown in fig. 2, in section IV, we discuss about the signature generation. Here teacher generates the signature, computes the private key, secret key and ultimately sends the material along with the signature to the administrator. The last step also include two other functions getdata() and hash().

In the second use case model, shown in fig: 3, in section IV, we discus about the signature verification, that means the administrator checks that the signature, sent by the teacher, and the signature, received by him/her, is same or not. Here the administrator gets the public key of teacher, receive the message and signature from the teacher and compare the two hash values. This last step includes two other processes, one is the first hash value sent by the teacher and the other hash value, generated by the administrator himself/herself.

III. CLASS DIAGRAM OF RSA DIGITAL SIGNATURE

The class diagram[3] for RSA digital signature consisting of classes RSA1, RSA2, Tchr (sender) and Admn (receiver) is shown in fig 4, in section IV:.

The descriptions of individual classes are given below:

```
Class RSA1{

Public:

        //these are the public member functions of the class RSA1

char *msg;     //msg is the message to be sent by an object of class Tchr
```

long int Ntchr; //it is the product of two prime numbers

long int sign; //sign represents digital signature

};

Class RSA2{

Public:

//these are the public member functions of the class RSA2

int hash(char[]);//this function is used to create a hash value

int GCD(int, int);//this is used to determine the GCD value of two numbers

};

Detail implementation of Class Admn, a multiple inheritance of RSA1 and RSA2 derived both publicly as follows:

Class Admn: public RSA2, public RSA1

{

long int Ptechr;//this is the public key of Tchr

int check();//this is used to verify the digital signature of an object of class Tchr

};

Detail implementation of the class Tchr derived publicly from RSA2 and privately from RSA1 is given below:

Class Tchr: public RSA2, private RSA1

{

Private:

//following data members are private of the class Tchr

long int U,V;//U and V are two random numbers

long int h;//h is storing hash value

long int Stchr;//this is the secret key of Tchr

```
Public:

    // following data members are public of the class Tchr

long int Ptchr;//this is the public key of tchr

void getData();//this function is used to get message and signature from Tchr

/* An object of class Tchr use following function to send his message and digital signature to an object of class Admn*/

admn send();

};
```

The objective of the Driver program segment is given below:

The program execution starts from the function main(). Here t is an object of class Tchr and a is an object of class Admn. t.send() sends a digitally signed message to a and a.check() verifies the signature and detects whether the received message is unaltered or modified by a third party i.e., intruder. Hence message integrity is checked by this check() function.

```
Void main()

{

Tchr t;//t is an object of class Tchr (sender)

Admn a;//a is an object of class Admn (receiver)

Int x; /*x is storing the result after comparison between computed signature on received message and the received signature*/

a=t.send();//t is sending signed message to a

x=a.check();//a is verifying the digital signature of t

if (x==1)

 cout<<"\nMessage is Ok";//message is not modified after transmission

else

 cout<<"\nMessage is Wrong";//message is modified after transmission
```

}//end of main()

IV. FIGURES:

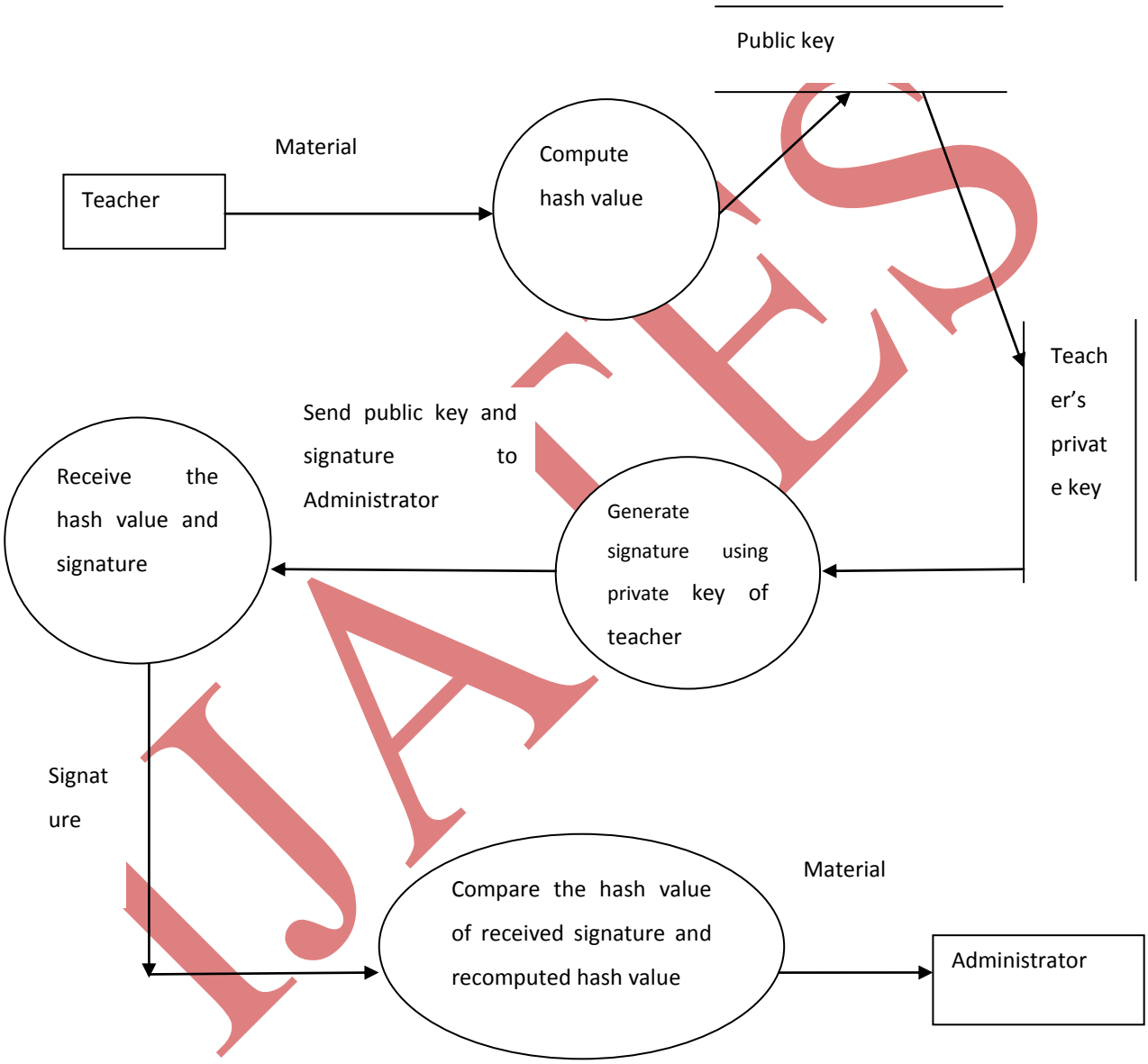

Fig: 1. DFD for RSA digital signature (from teacher to administrator)

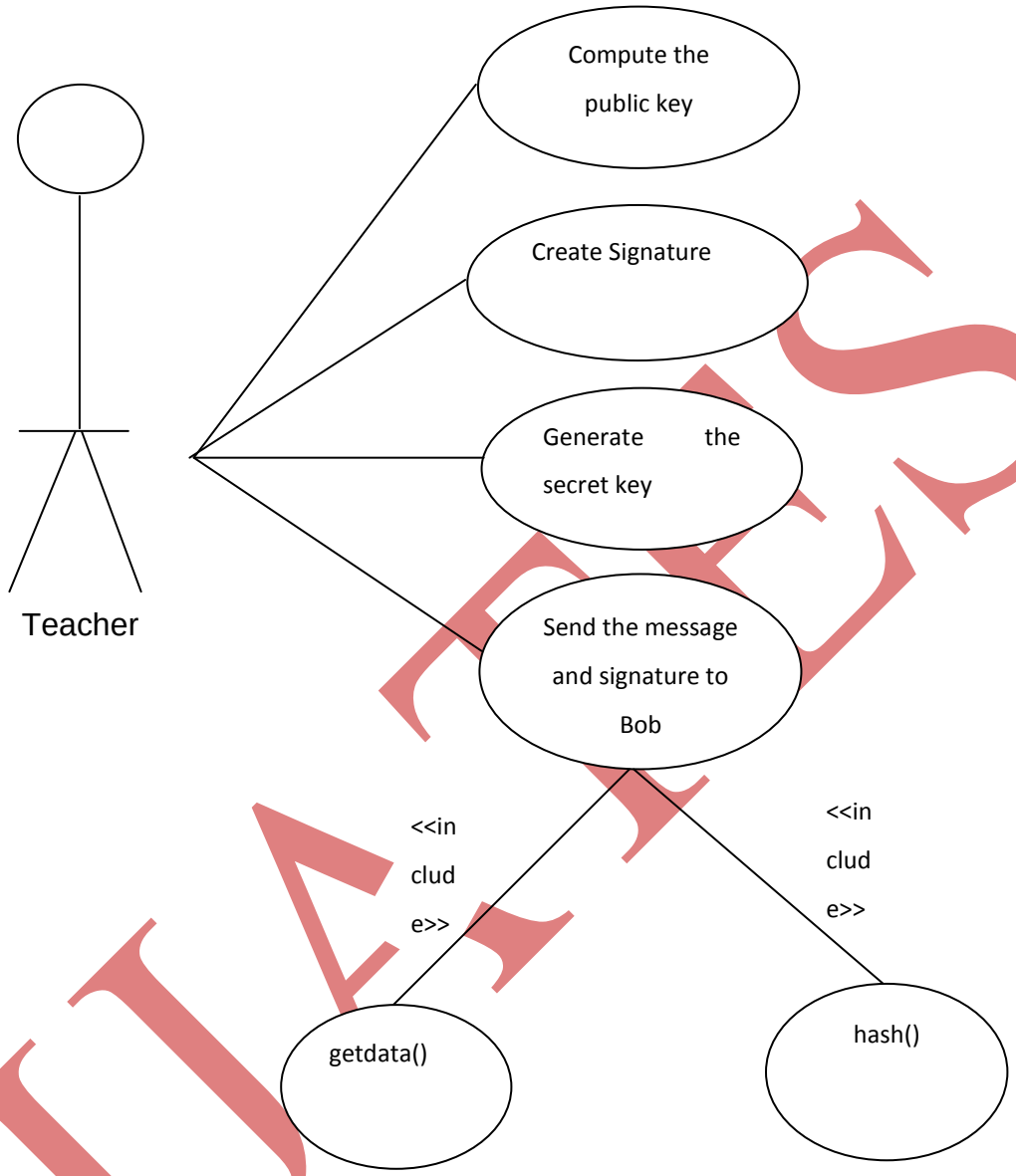

Fig 2: Use Case Diagram For Teacher

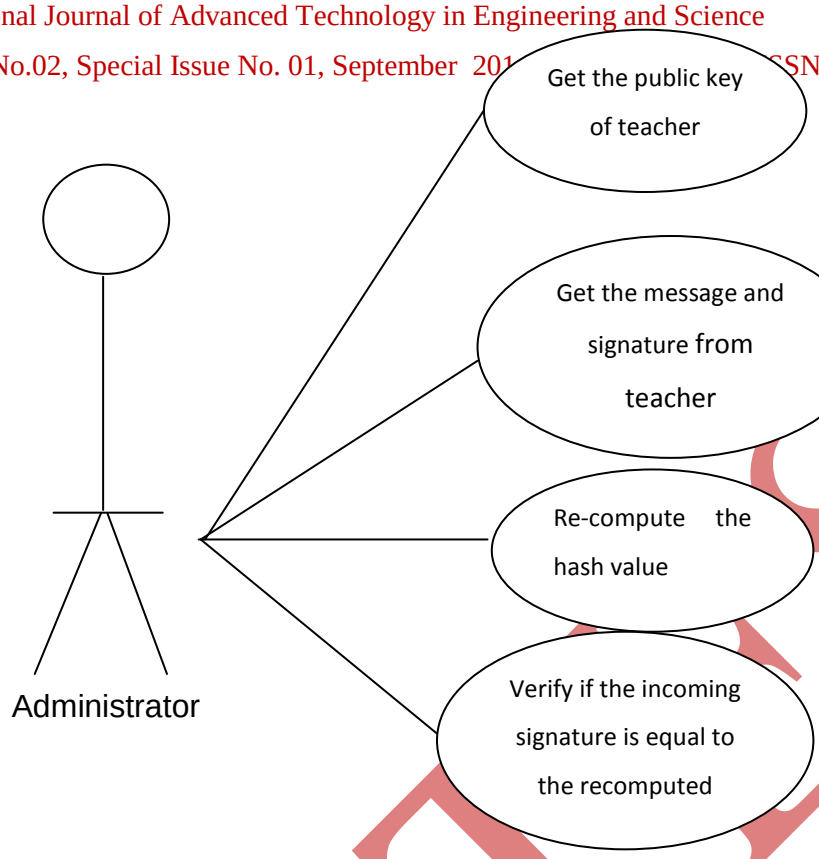

Fig 3: Use case diagram for Administrator

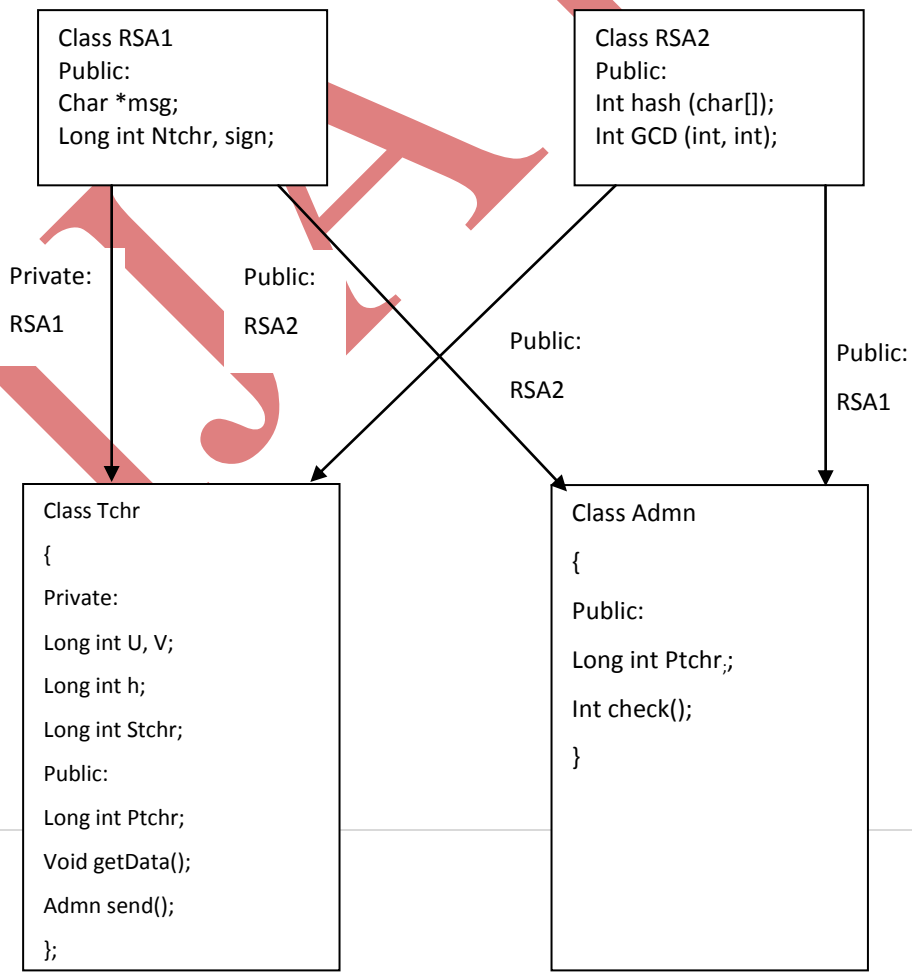

Fig 4: Class Diagram for RSA Digital Signature

V. CONCLUSION

Proposed Object Oriented Model of RSA algorithm may be applied in case of authentication of transacting parties involved in E-learning as well as E-commerce and E-governance. The proposed Object Oriented analysis and design can be done further with the help of sequence diagram, activity diagram etc. Moreover, the security of proposed model may be improved further by selecting large prime numbers, which are used for key selection. The level of security of proposed model may be improved further by using MD5 or SHA algorithm as hash function.

REFERENCES

[1] Balagurusamy, E (2006), Object Oriented Programming with C++, Tata McGraw Hill, New Delhi

[2] Behrouz, A Forouzan (2006), Data Communication and Networking, Tata McGraw Hill

[3] Karforma Sunil and Mukhopadhyay Sripati (July, 2005), A Study on the application of Cryptography in E-Commerce, The university of Burdwan, W.B, India.

[4] Karforma Sunil and Nikhilesh Barik (January, 2012), Risks and Remedies in E-learning System, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, pp 51-59.

[5] Karforma Sunil and Nikhilesh Barik (August, 2012), Object Oriented Modeling of Secured E-Assessment System, International Journal of Scientific & Engineering Research Volume 3, Issue 8.

[6] Kumar Gupta Sapan and K. Kuriachan Juneesh, Issues and Solutions in E-learning System, International Journal in Multidisciplinary and Academic Research (SSIJMAR), Vol. 2, No. 2

[7] Rajib Mall (June, 2006), Fundamentals of Software Engineering, Prentice Hall of India, New Delhi

[8] Weippl, R.E (2005), Security in E-Learning, Springer