Object Oriented Modeling of DSA for Authentication of Student in E-Learning

Ambalika Ghosh[1], Sunil Karforma[2]

[1]Research Scholar, Department of Computer Science, Burdwan University, India

[2]Associate Professor, Department of Computer Science, Burdwan University, India

Abstract: ***E-Learning is the interactive transfer of knowledge via an intranet or the internet. Due to use of internet as electronic communication media there are several types of risks & threats that may hamper security of E-learning environment. At the time of online submission of filling up form during any course registration by student, the authenticity and integrity of the information can be ensured using digital signature. To enhance the security level of the information the Digital Signature Algorithm (DSA) can be used to generate digital signature which will be an industry standard algorithm using public key cryptography for security of various electronic systems like E-Governance, E-Banking, E- Commerce etc. In this paper authors have applied DSA algorithm to achieve optimal resource allocation, faster information and enhanced security for authentication of information in E-Learning during submission of ICT (Information and Communication Technology) based filled up course registration form in Object Oriented paradigm.***

Keywords: Digital Signature, DSA, Authentication, ICT, Object Oriented

1. Introduction

The use of Information & Communication Technology (ICT) [4] as operation of a public communicating tool for delivery of services electronically in the public and private sectors have changed the scenario of every system. This has resulted emergence of E- learning system [9]. E-learning means delivery of services electronically among the Faculty, Student and Admin [20, 21]. During exchange of information among these three entities, hackers [8] can steal or modify the information. Application of Digital Signature Algorithm (DSA) [7] is implemented to impose authenticity of information. Digital Signature Algorithm (DSA) provides an authenticity [15] over the message communicated among Faculty, Student and Admin. Use of Digital Signature Algorithm (DSA) enhanced the security feature [11, 12] of the system. In this paper the authors have wrapped DSA in an Object oriented [5] manner for security of information which is needed during filled-up of registration form to enroll for any course electronically between Student and Admin.

In our proposed system each student is allotted with one roll number which is used for course registration. During course registration, students have to send their roll number along with personal information. The roll number may be changed by hacker causing insecure system [14]. The Admin verifies the roll number efficiently using the strong security features of DSA [10] algorithm and hence implementing authentication of the information in the proposed system is easily possible.

In section II, authors give a short outline about DSA. In section III authors have outlined how Object Oriented Modeling can be used to implement DSA for authentication of a Student during course registration. In this paper; authors designed & embodied the UML [1, 2, 3] based Object Oriented Model of E-Learning System using DSA. For an efficient design, we have used CLASS Diagram SEQUENCE Diagram and ACTIVITY Diagram to represent the required class representation for programming purpose in the E-Learning system.

2. DSA- An Overview

The Digital Signature Algorithm (DSA) is a United States Federal Government standard or FIPS for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) [16]. The Digital Signature is basically a mathematical implementation of asymmetric cryptographic technique over the digitized document to ensure its authenticity and integrity to its users. Its concept is very much similar with the conventional signatures which are used to prove the origin of the document so that a recipient has a reason to believe that the message was created by the actual sender and was not distorted during the transit. The Digital Signatures are used to achieve authentication, non-repudiation and integrity over the digital data. Generally, the digital signature algorithms are composed of three sub phases [17];

a. Key generation algorithm.
b. Signing algorithm.
c. Signature verification algorithm.

The DSA algorithm makes use of the following variables [18]:
p= A prime number of length L bits. L= A multiple of 64 between 512 and 1024.
q= A 160- bit prime factor of (p-1).
g= $h^{(p-1/q)}$ mod p, where h is a number less than (p-1) such that $h^{(p-1/q)}$ mod p is greater than1.
x= A number less than q.
y= g^x mod p.
H= Message Digest algorithm.

The first three variables p, q and are public in nature and can be sent across an insecure network free. The private key is x, where as the corresponding public key is y.

Let us assume that the sender wants to sign a message m and send the signed message to the receiver. Then the following steps take place;

1. The sender generates a random number k, which is less than q.
2. The sender now calculates:
   a. r= $(g^{k}$ mod p)mod q
   b. s=$(k^{-1}$(H(m)+xr))mod q
   The values r and s are signatures of the sender. The sender these values to the receiver. To verify the signature, the receiver calculates:
3. w=s^{-1} mod q
   u1=(H(m)*w)mod q
   u2=(rw) mod q
   v=$((g^{u1}*y^{u2})$mod p)mod q

If v=r, the signature is said to be verified. Otherwise, it is rejected.

3. UML Based Proposed Object Oriented Modeling

To depict our proposed system using UML we only consider the Class Diagram, Sequence Diagram and Activity Diagram.

A. Class Diagram

The given Figure-1demonstrates the organization of class hierarchy [19, 24] showing how an Admin called Alice can authenticate a Student called Bob during his Course Registration using DSA in object oriented approach.

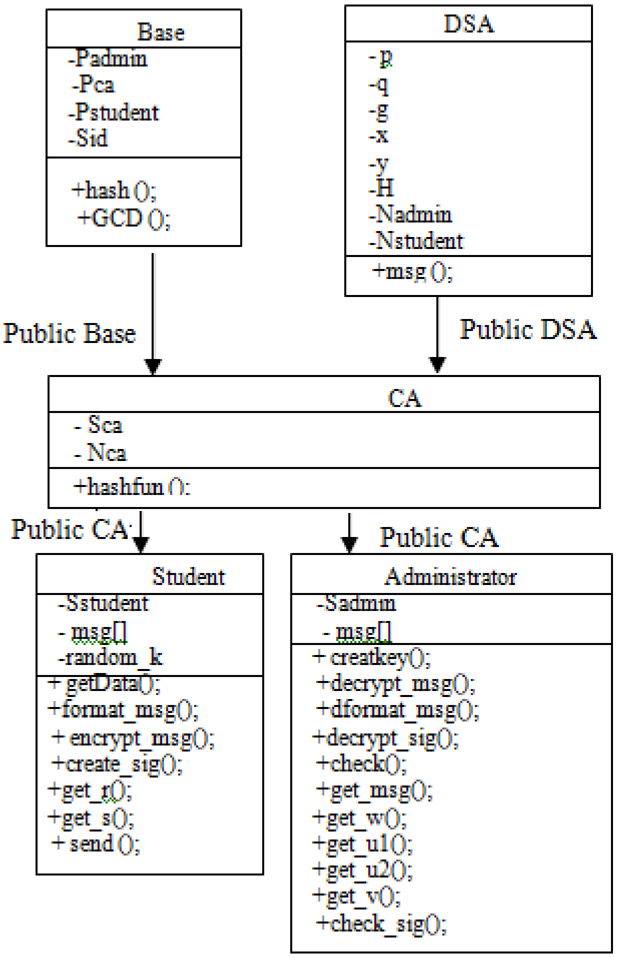

Figure 1: Class Hierarchy diagram of E-Learning system

1) Analysis of Class Hierarchy

- Class Base:
  The Base class is used to test signature generation and verification using DSA algorithm. This class is publicly inherited by the class CA (Certificate Authority).
- Public Member
  int Padmin- Administrator's public key
  int Pstudent-student's public key
  int Pca-certificate authority's public key
  int Sid-student's identity number
  long double hash-hash of message
  int GCD(int,int)-This is the only function in this class & this is used for finding an appropriate public key from two co-prime numbers supplied to it.
- Class DSA:
  This class is also publicly inherited by CA.
- Public Members
  int p,q-these are two co-prime numbers to create public and secret key.
  int g,y- used to calculate other required variable
  int Nstudent, Nadmin-these are used to encrypt or decrypt the message.
  char msg-this is the message(character string) which is sent to Administrator by Student
- Private Members
  int x-number less than q
  string H-message digest
- Class CA:
  This class corresponds to the Certificate Authority and it inherits the classes Base and DSA publicly and it is inherited by the classes Student and Admin.
- Private Members
  int Sca- this is the secret key of CA used to encrypt
- Public Members
  long double hashfun (int, int)-used to calculate of message, sign hashed value for certificate
  int Nca-public key used to encrypt or decrypt
- Class Student:
  The Student class implements all necessary operations for signature generation.This corresponds to the student and it inherits the class CA publicly i.e. it is in turn inheriting the classes Base, DSA and CA.
- Private Members
  int Sstudent-this is the secret key of class Student
- Public Members
  int msg[]-this array actually holds the message after being converted into integers
  int random_k-generates a random number less than q
  void getData()-get message and also creates the public and secret key
  void format_msg()-this is used to format the message into an integer array which contains integers
  long double encrypt_msg()-this is used to encrypt the message
  long double create_sig(int, int)-It is used to create the digital signature
  Admin send(Admin)-this function sends two Part(msg,sig)information to administrator
  int get_r()- calculate the value of r

int get_s()-calculate the value of s

- Class Admin:
  The Admin class implements all necessary operations for signature verification.This corresponds to the Admin of the E-Learning system and it inherits the class CA publicly i.e. it is in turn inheriting the classes Base, DSA and CA.
- Private Members
  int Sadmin- this is the secret key of administrator & it is used to decrypt the message
- Public Members
  long double msg[]-It stores received message after decryption
  void dformat_msg() – which is used to get actual message
  void decrypt_sig()-decrypts the encrypted digital signature
  void createkey()-to create public and secret key of admin
  void decrypt_msg()-to decrypt the encrypted message
  void check()-invokes the functions get_msg() & check_sig() for authentication checking
  void get_msg()-invokes decrypt()function to get the original message
  void check_sig()-invokes decrypt_sig() methods to check the signature
  int get_w()-calculate the value of w
  int get_u1()-calculate the value of u1
  int get_u2()-calculate the value of u2
  int get_v()-if v is equal to r then verified, else rejected

B. Sequence Diagram

A sequence diagram [22] shows interaction among objects as a two-dimensional chart. Here, we only describe the steps that are needed to authenticate any Student during securely submit registration form using DSA algorithm in E-Learning system with the help of Sequence diagram.

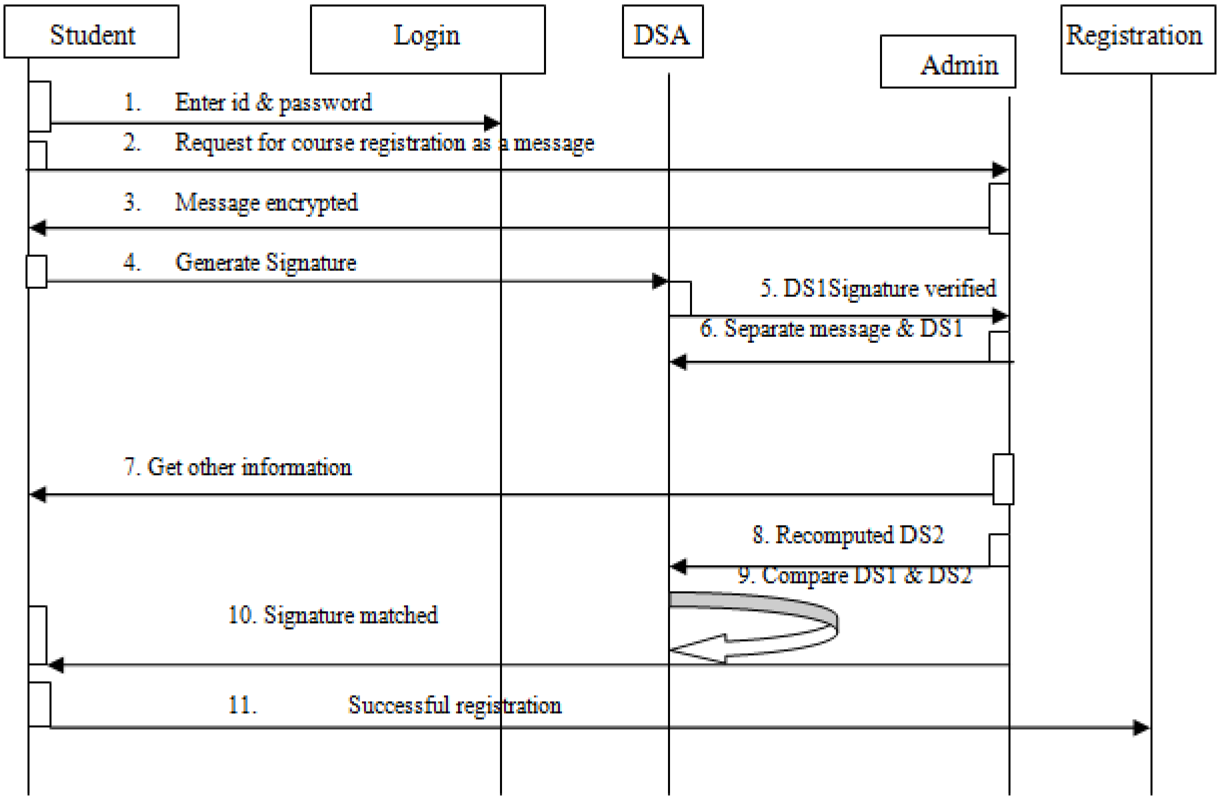

Figure 2: Sequence diagram of Course Registration in E-Learning system

C. Activity Diagram

Activity Diagrams are graphical representations [23] of workflows of stepwise activities and actions with support for choice, iteration and concurrency. Hence they can be regarded as a form of flowchart.

Here, students enter into the system by giving his/her id & password. To check the authenticity of the student, they must generate digital signature by applying DSA and Admin must verify it. After that students can finally upload the personal information details in the registration form.

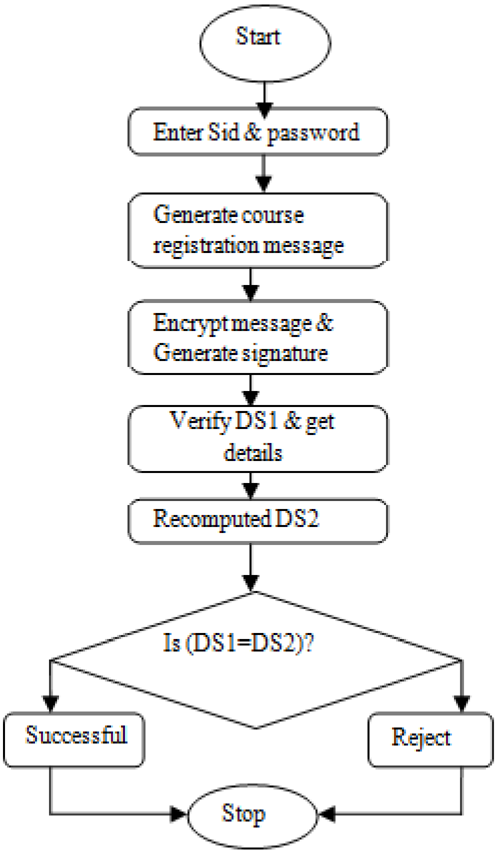

Figure 3: Activity diagram of course registration in E-Learning system

4. Conclusion

To ensure the privacy & confidentiality of information suitable encryption technique is necessary for E-Learning security [13]. The proposed system is implementing security of information in E-learning employing DSA algorithm in which digital signature generation and verification is done very efficiently compared to other traditional cryptography [6] algorithms. With implementation of DSA wrapped in Object Oriented Model using UML we can realize a level of safety, reliability & hence trust in the mind of huge number of students. This proposed system will help to reuse the code design. An effortless secure transfer & exchange of data between the admin & student along with other component of the system become easy. The level of security of the proposed system can be improved further by using Elliptic Curve Cryptography and more secure SHA-2 hash function instead of SHA-1 [24], which can be considered as the future scope of this work.

References

[1] Fundamentals of software Engineering, 2nd Edition by Rajib Mall. PHI Publications, New Delhi
[2] Software Engineering, Revised 2nd Edition by K.K. Aggarwal & Yogesh Singh. New Age International Publishers, New Delhi
[3] Introduction to System Analysis & Design, 2nd Edition by I.T. Hawryszkiewyez. PHI Publication, New Delhi
[4] Data Communication & Networking, 4th edition by Forouzan, TMH, New Delhi
[5] Object Oriented Programming in C++, 4th edition by Robert Lafore, Techmedia, New Delhi
[6] Jon C. Graff, " Cryptography and E-commerce," John Wiley & Sons, New York, 2001.
[7] "An Object Oriented Approach of Elgamal Digital Signature Algorithm", Sunil Karforma, Sripati Mukhopadhay, Siddhartha Sen 259-260, EAIT, 2006, Kolkata, February 10-11, 2006
[8] International Journal on Physical Science,"Digital Certificate for Secure Transaction in E-Banking",S. Karforma,S. Mukhopadhyay,volume17,pp 179-182,April,2005
[9] Edgar R. Weippl "Advances in E-Learning", Springer Publication
[10] Bruice Schneier "Applied Cryptography- Second Edition", WILEY-2008
[11] S. Karforma, S. Mukhopadhyay and B. Bhattacharya "Data Security in Information Age", SAJOSP,Vol 2, No. 2,pp. 108-112"(2003)
[12] Dr. Deepshikha Jamwal, Anita Bhat, "E-Learning security Concepts", www.google.com/ejel.com
[13] eibl, C.Jet.al,"Development of E-Learning Design Criteria with Secure Realization Concepts", In: Mittermeir, R.T.; Syslo,M.M.(eds.): ISSEP 2008,LNCS 5090, Springer,Berlin,June 2008,pp.327-336
[14] Hamdi Ihsana, Zainuddin Bey Fananieb,dan Nur Aeni Hidayahc,"Development of E-Learning System on Online Courses Application in 2TORS.com", www.scribd.com/doc/36332602/English-Journal
[15] Application of Information and Communication Technologies (AICT), 2011 5th International Conference, "Password-based client authentication for SSL/TLS using ElGamal and Chebyshev polynomials", Sarikaya, K., **Page(s):** 1 - 5, 12-14 Oct. 2011
[16] http://en.wikipedia.org/wiki/DSA
[17] Abhishek Roy, Sunil Karforma," A survey on digital signatures and its applications" J. of Comp. and I.T. Vol. 3(1&2), 45-69 (2012).
[18] Atul Kahate, Cryptography and Network Security, Second Edition, Mc Graw Hill, 2003
[19] Ambalika Ghosh, Sunil Karforma ," Object Oriented Modeling of Digital Certificate for Secure Transaction in E-Banking", Proceedings of NaCCS -2012, pp. 103-111. ISBN: 93-80813-18-X
[20] Ambalika Ghosh, Sunil Karforma , Ajit Kumar Singh," Object Oriented Modeling of E-Learning System" Proceedings of ICCS -2010, pp. 103-111. ISBN: 93-80813-01-5
[21] Ajit Kumar Singh, Sripati Mukhopadhyay,Ambalika Ghosh, Sunil Karforma ," Object Oriented Design of E-Library for E-Education" Proceedings of ICCS -2010, pp. 163-167. ISBN: 93-80813-01-5
[22] Ambalika Ghosh, Sunil Karforma , " Object Oriented Modeling of Digital Certificate based E-Learning System" Proceedings of RHECSIT -2012, pp. 103-111. ISBN: 978-81-923820-0-5
[23] Oriental Journal of Computer Science and Technology," An UML based Design of E-Learning System using Digital Certificate**",** Ambalika Ghosh and Sunil Karforma, Volume 05 No. 02 Page No. 257-262 Dec 2012
[24] Ambalika Ghosh, Sunil Karforma ," Object Oriented Modeling of SSL for Secure Information in E-Learning",

Proceedings of ICCS -2013, pp. 62-66. ISBN-13: 978-9-35-134273-1, ISBN-10:9-35-134273-5

Author Profile

Ambalika Ghosh is the Assistant Professor of Department of Computer Application, Swami Vivekananda Institute of Modern Science (SVIMS) under WBUT, Kolkata. She obtained her BCA degree from The University of Burdwan and MCA degree from Haldia Institute of Technology under WBUT. Before joining SVIMS she worked as a Lecturer in "BIMS", Burdwan and as a Software Engineer in Keane India Ltd., Gurgaon. Presently Ms. Ghosh is a Research Scholar under the guidance of Dr. Sunil Karforma, Associate Professor, Burdwan University and she is trying to apply her knowledge in the field of Network Security.

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 and E-commerce, E-Learning, E-Governance etc. is his field of interest in research area. He has published approximately 80 research papers in reputed National and International journals and proceedings.