ISSN 2231-3478 (Print)
JUSPS-B Vol. 28(7), 158-162 (2016). Periodicity-Monthly
Section B
ISSN 2319-8052 (Online)
JOURNAL OF ULTRA SCIENTIST OF PHYSICAL SCIENCES
An International Open Free Access Peer Reviewed Research Journal of Physical Sciences
website:- www.ultrascientist.org
Estd. 1989

Object Oriented Analysis and Design of Digital Certificate based Mark-sheet Authentication in E-learning

SOUMENDU BANERJEE[1] and SUNIL KARFORMA[2]

[1,2]Department of Computer Science, The University of Burdwan (India)
Email of Corresponding Author: bansoumendu@gmail.com
http://dx.doi.org/10.22147/jusps-B/280702

Acceptance Date 29th Oct., 2016, Online Publication Date 2nd Dec. 2016

Abstract

Since e-learning totally depends on Internet, the transmission of mark sheet to the students from the administrator should be done very securely; otherwise, if the hackers reach the documents, then it may be very harmful for the students as well as for the corresponding e-learning institution also. By using, digital certificate the administrator can send the mark sheet securely to the students and also it helps in non –repudiation, one of the security issues in e-learning. The implementation of the object orientation model helps others in better understanding of the system. The other goals of object oriented implementations like code re-usability, data redundancy etc. can be madeby object oriented models. Here we will analysis the values of the metrics for two basic models of object oriented metrics: Chidamber and Kemerer metric (CK metric) and Metric for Object Oriented design metric (MOOD metric) based on the class hierarchy diagram of digital certificate transmitting from the administrator to students.

Key words: E-learning, Object Oriented metrics, Class hierarchy diagram, Digital Certificate

Introduction

Regardless of the type of learning, mark sheet is an essential identification document for students. Submission of the mark sheet is essential for each student, where mark sheet plays an important role. In case of e-learning, mark sheets are distributed to the students via Internet where authentication is a main concern while sending the mark sheet to the student. To provide authentication and non-repudiation, administrator of the concerned institution may use digital certificate and digital signature[1]. Digital certificate is a public key infrastructure (PKI), which provides the security while transmitting documents through online, in sense of identification/authentication, confidentiality, integrity, non-repudiation[2] and access control[3]. The digital certificate is digitally signed by a trusted certificate authority and also contains the name of the certificate holder, serial number, expiration date and copy of certificate holder's public key which used to encrypt messages and digital signature[4].

Object oriented implementation of any system is used for reuse of code, removal of data redundancy, better understandability and hiding of private data. There are several advantages like inheritance, encapsulation, and data hiding which can be achieved through the implementation of a system using object oriented design[5]. Though there are several object oriented metrics, in this paper we will focus only the two main object oriented metrics: Chidamber and

Kemerer metric (CK metric) and Metric for Object Oriented design (MOOD metric). These metric analyses are mainly done in respect of the cohesion and coupling. High cohesion and low coupling refer to the better understandability, robustness, reusability and reliability as well as better quality of software on the other hand, low cohesion and high coupling mean the system is difficult to understand and maintain.

In this paper, we have analyzed the metrics, based onthe class hierarchy diagram of digital certificate along with the mark sheet transmitting from the administrator to the students in an e-learning system. Section II covers the class hierarchy diagram of the digital certificate based transaction system and section III covers the object oriented metric based analysis of the system and finally we conclude in section IV which include some future scopes.

II. Class Hierarchy diagram :

The class hierarchy diagram is a diagram that is used to show the structure of a system by showing their classes, their attributes, operations and relationship between objects[6]. In the following class diagram, we have used five classes: Base, RSA, CA, Admin and Student. Class CA is publicly inherited from the classes Base and RSA and Admin and Student classes are publicly derived from the class CA[7,8].

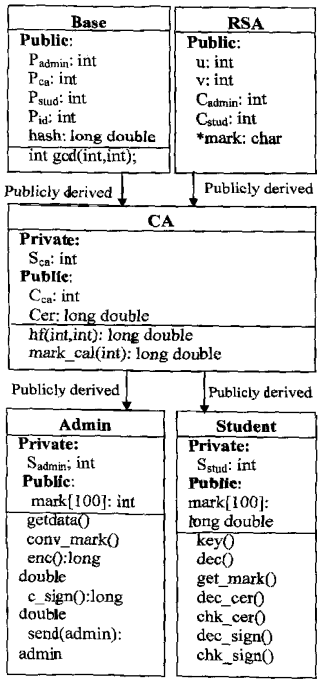

Fig: 1. Class Diagram for mark sheet authentication using digital certificate during transmission

Base class is publicly inherited by the class CA (Certificate Authority). It contains five data members, four of which contain public keys and one contains the hash value and one member function to calculate and store the GCD of two co-prime numbers.

Class RSA is also publicly inherited by the class CA. It contains four data members which are used to store the two prime numbers, mark sheet and two other data members are used to encrypt and decrypt the mark sheet. Class CA stands for the certificate authority and it is inherited from the classes Base and RSA and two other classes Admin and Student also publicly derived from this class. It contains one private data member to store the secret key of certificate authority, two public data members to store the public key of the certificate authority and the digital certificate and also two public member functions to calculate the hash function and certificate.

Admin class is publicly derived from the class certificate authority. It contains one private data member to store the secret key of the administrator and one public data member to store the mark sheet, which has to be sent to the student. This class also contains five member functions for several purposes, like encrypt the mark sheet, generate the public key, generate the digital signature, receive data from certificate authority etc.

Student class is also publicly derived from the CA class. It has one private data member to store the secret key of the student and one public data member to store the mark sheet. It also has seven public member functions to generate the keys, decrypt the encrypted mark sheet, certificate and digital signature, and check the certificate and signature for authentication.

III. Metric based analysis :

There are several object oriented metrics[9] analyses procedures advised by Lorenz and Kidd, Henderson, Harrison, Lee etc, but the two most important of them are Chidamber and Kemerer metrics (CK metrics) and Metrics for Object Oriented Metrics (MOOD metric). The main characteristics[10] based on which the measures of the metrics are generally done are class, coupling, cohesion, inheritance and polymorphism. On basis of these features, we will calculate the values of some object oriented metrics[11] related to the class diagram, we discussed above. Here we will discuss about some object oriented metrics below:

- **NOA (Number of attributes)**: It calculates the total number of attributes of the classes.
- **NOM (Number of methods)**: It calculates the total number of methods in the classes.
- **CBO (Coupling between objects)**: Number of other classes to which the class is coupled.

- **DIT (Depth of inheritance tree)**: It calculates the number of maximum path from the node to the root in the inherited tree.
- **NOC (Number of children)**: It contains the number of subclasses inherit the methods of parent class.
- **RFC (Response for a class)**: it is same as the number of methods that can be invoked in response to a message in a class.

Here we have applied above metrics on our proposed model to get the following results:

Object Oriented Metrics	Classes of proposed system				
	Base	RSA	CA	Admin	Student
NOA	5	4	3	2	2
NOM	1	0	2	5	7
CBO	3	3	2	0	0
DIT	0	0	1	2	2
NOC	1	1	2	0	0
RFC	15	14	15	8	10

Table 3.1: Metrics of mark sheet authentication using digital certificate

A comparative study of above metrics is shown graphically below:

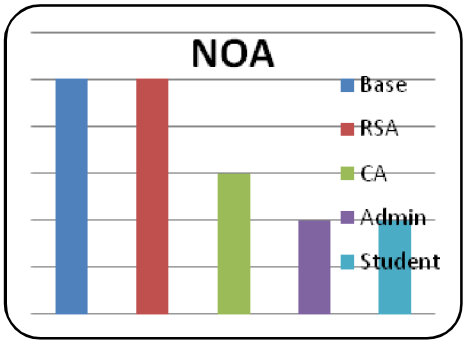

Fig: 3.1 NOA

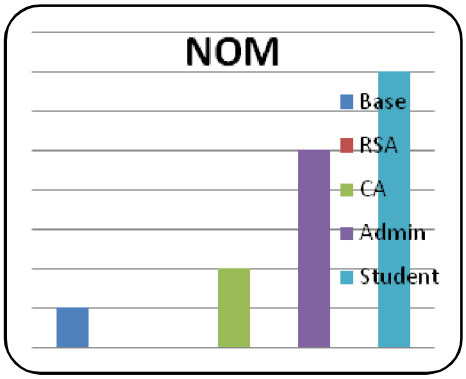

Fig 3.2: NOM

Fig 3.1 and Fig 3.2 shows the values of Number of attributes and the Number of methods graphically, which is helpful to make an estimate of the required time and effort to develop and maintain each and individual classes. According to the measurement, these values should be kept down, which means that our proposed system is quite ok.

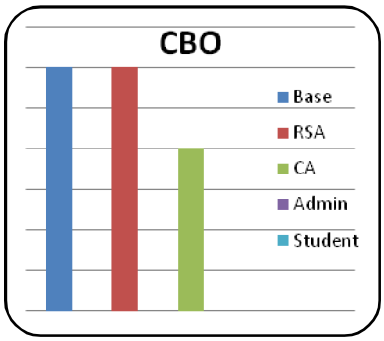

Fig 3.3: CBO

Fig 3.3 shows the value of CBO metrics, *i.e.*, the value of coupling between objects. A good software design always maintains a low coupling, and our proposed system is also maintaining that fact.

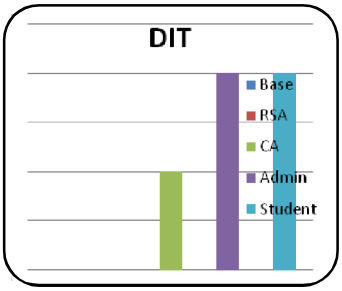

Fig 3.4: DIT

Fig 3.4 shows the value of DIT metrics, *i.e.*, the value of the depth of inheritance tree which represents the complexity behavior of the class. The increasing value of DIT means that the complexity is higher. Here the maximum value of DIT is 2, which mean our proposed system is ok.

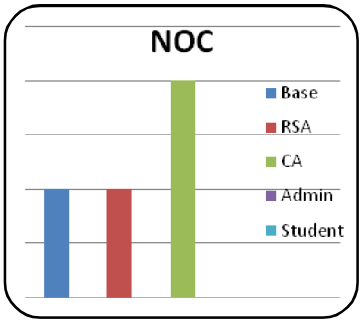

Fig 3.5: NOC

Fig 3.5 represents the value of number of children in amodel. Here the maximum value of a proposedsystem is 2, which means the system isnot so difficult to understand.

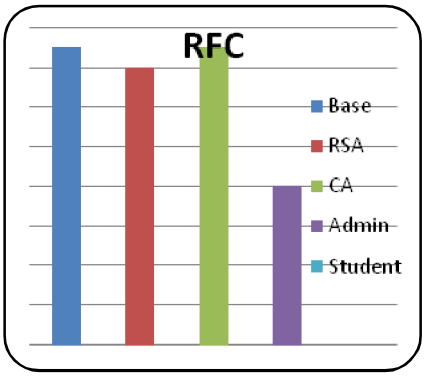

Fig 3.6: RFC

Fig 3.6 shows the graphical representation of the value of RFC metric. If the value of the RFC metric increases then the system becomes difficult to understand and if it keeps vary low, and then polymorphism increases. Here we reach at the optimal value of RFC.

Now we will apply metrics, which are the part of MOOD metrics on our proposed system[12].

MHF (Method Hiding Factor): It is a measure of the encapsulation which states the sum of the invisibilities of all methods in all classes.

Equation for **MHF**=$\Sigma_{i=1}^{TC} M_h(C_i)/ \Sigma_{i=1}^{TC} M_d(C_i)$ //TC means total number of class

Where $M_d(C_i)$= $M_v(C_i)$+ $M_h{\cdot}(C_i)$ where $M_d(C_i)$= methods defined in class C, $M_v(C_i)$= methods visible in class C and $M_h{\cdot}(C_i)$= methods hidden in class C

	Classes of proposed system					Summation (Σ)
	Base	RSA	CA	Admin	Student	
$M_h(C_i)$	0	0	0	0	0	0
$M_v(C_i)$	1	0	2	5	7	15
$M_d(C_i)$	1	0	2	5	7	15
MHF	0/15=0					

Table 3.2: MHF

Table 3.2 shows the value of the metric MHF, which is low, that means our proposed model is very simple to implement and understand.

AHF (Attribute Hiding Factor): It is also a measure of encapsulation in object oriented design which is calculated by the sum of invisibilities of all attributes in all classes.

Equation for **AHF**=$\Sigma_{i=1}^{TC} A_h(C_i)/\Sigma_{i=1}^{TC} A_d(C_i)$

$A_d(C_i)$= $A_v(C_i)$+ $A_h(C_i)$, where $A_d(C_i)$= total attributes defined in class C, $A_v(C_i)$= Attributes visible in class C and $A_h(C_i)$= attributes hidden in class C

	Classes of proposed system					Summation (Σ)
	Base	RSA	CA	Admin	Student	
$A_h(C_i)$	0	0	0	1	1	2
$A_v(C_i)$	5	5	3	2	2	17
$A_d(C_i)$	5	4	3	2	2	16
AHF	2/16=0.125					

Table 3.3: AHF

Table 3.3, contains the value of the AHF metric. This value is in between 0 and 1, which is ok for any model or system.

MIF (Method Inheritance Factor): Method inheritance Factor is measured by the ratio of the sum of the inherited methods in all classes of the system to the total number of methods available for all classes.

Equation for **MIF**=$\Sigma_{i=1}^{TC} M_i(C_i)/\Sigma_{i=1}^{TC} M_a(C_i)$

Where $M_a(C_i)$= $M_d(C_i)$+ $M_i(C_i)$,

$M_a(C_i)$=number of methods available,

$M_d(C_i)$= number of methods defined and

$M_i(C_i)$= number of methods inherited

	Classes of proposed system					Summation (Σ)
	Base	RSA	CA	Admin	Student	
$M_d(C_i)$	1	0	2	5	7	15
$M_i(C_i)$	0	0	1	3	3	7
$M_a(C_i)$	1	0	3	8	10	22
MIF	7/22=0.318					

Table 3.4: MIF

Table 3.4 shows the value of MIF metric. We have to be careful that the value of MIF should not be too low or too high. Here MIF=0.318, which is quite ok.

AIF (Attribute Inheritance Factor): It is also related with inheritance. It is measured by the ratio of the sum of inherited attributes of all classes of the system to the total number of attributes, available for all classes.

Equation for **AIF**=$\Sigma_{i=1}^{TC}A_i(C_i)/\Sigma_{i=1}^{TC}A_a(C_i)$
Where $A_a(C_i)= A_d(C_i)+ A_i(C_i)$,
$A_a(C_i)$=number of methods available,
$A_d(C_i)$= number of methods defined and
$A_i(C_i)$= number of methods inherited

	Classes of proposed system					Summation (Σ)
	Base	RSA	CA	Admin	Student	
$A_d(C_i)$	5	4	3	2	2	16
$A_i(C_i)$	0	0	9	11	11	31
$A_a(C_i)$	5	4	12	13	13	47
AIF	31/47=0.659					

Table 3.5: AIF

From table 3.5 we can calculate the value of AIF of our proposed model as 0.659. For any proposed model, if the value of AIF is 0, it means that there is no attribute exists in the class and also there is lacking of inheritance.

IV. Conclusion

Object oriented metric analysis of any model makes a system more reliable and secure. Here we calculate the values of many standard metrics, most of which are the part of the CK metric and MOOD metric based on the class hierarchy diagram where secure transmission of mark sheet from the administrator to student may be done using digital certificate. The proposed system use combination of digital certificate and digital signature for authentication of mark sheet between developer to student which is a must in an e-learning system.

References

1. Andrew, S. Tanenbaum, *Computer Networks*, Pearson Prentice Hall (2005).
2. Karforma S. and Mukhopadhyay S., 'Digital certificate for secure transactions in E-banking', *Journal of Ultra Scientist of Physical Sciences*, vol: *17* No: *2(M)* (2005).
3. https://www.comodo.com/resources/small-business/digital-certificates-intro.php
4. http://searchsecurity.techtarget.com/definition/digital-certificate
5. Rajib Mall, *Fundamentals of Software Engineering*, Prentice Hall of India, New Delhi (2006).
6. https://en.wikipedia.org/wiki/Class_diagram
7. Karforma S. and Mukhopadhyay S., 'A Study on the application of Cryptography in E-Commerce', *The university of Burdwan, W.B, India*,(Thesis) July (2005).
8. Karforma S., Banerjee S., 'Object Oriented Modeling of Digital Certificate in E-learning', *IJETTCS*, Vol-3 No.5, Sept-Oct, pp: 205-211 (2014). Available at: www.ijettcs.org/Volume3Issue5/IJETTCS-2014-10-22-91.pdf
9. Ali Kamandi, 'Object Oriientted Mettriics', *Sharif University of Technology*, Spring (2007). available at: http://ce.sharif.edu/courses/8586/1/ce924/resources/root/4.%20Kamandi_OOMetrics.pdf
10. Aggarwal K.K., Singh Y., Kaur A., Malhotra R., "Empirical study of object oriented metrics", *Journal of ObjectTechnology, ETH Zurich, Chair of Software Engineering*, Vol. 5, No. 8, November-December, pp: 149-173 available at: www.jot.fm/issues/issue_2006_11/article5.pdf (2006).
11. S. Muktamyee, "An overview of Object Oriented Design Metrics", (Master Thesis) *Department of Computer Science, Umeå University, Sweden* June 23, 2005 Available at: *www.cs.umu.se/education/examina/Rapporter/MuktamyeSarker.pdf*
12. Banerjee S. and Karforma S., 'Object Oriented Metrics Based Analysis of DES algorithm for secure transmission of Mark sheet in E-learning', *IJCSE*, vol-4, special. Issue-1, pp: 93-98 (2016). Available at: http://www.ijcseonline.org/full_spl_paper_view.php?paper_id=38