International Journal of Information Science and Computing 3(1): June, 2016: p. 1-7
DOI : 10.5958/2454-9533.2016.00001.6

Object Oriented Metrics Based Analysis of DSA algorithm for authentication of Study material in E-learning

Soumendu Banerjee and Sunil Karforma

Department of Computer Science, The University of Burdwan, West Bengal, India

Corresponding author: sunilkarforma@yahoo.com

Abstract

With the increasing popularity of e-learning, the organizations, those are providing the facility of e-learning, facing too many challenges regarding the security. In case of e-learning, the main area, where the security is so much needed, is the transmission of any online documents like marks sheets, study materials, registration numbers, admit cards and so many other learning related documents. To provide authenticity in case of these kinds of transmission of documents, organizations can use Digital Signature Algorithm (DSA). The object oriented analysis and design of any system makes it better in sense of understandability, maintainability, code re-usability, it reduces time and cost of the system development and improves the quality of the system. There are mainly two kinds of metric analysis, those are complement to each other: Chidamber and Kemerer (CK) metric and Metric for Object Oriented Design (MOOD) metric. We will analyze the value for these two metrics using the class hierarchy diagram of the DSA algorithm regarding the transmission of study materials from the administrator to student in an e-learning system.

Keywords: e-learning, class hierarchy diagram, DSA algorithm, OO metrics

E-learning is totally dependent on Internet or Intranet. The total transmission procedure is done via Internet. Since, internet is easily reachable to anyone now-a-days, so the e-learning organizations give so much emphasis on the security during transmission of e-learning related documents, otherwise, hackers can change or destroy those documents. To provide authenticity during transmission of documents between the three main participants in e-learning (teacher, administrator and student), in our proposed model, we apply Digital Signature Algorithm[1]. The two main benefits we achieve by using the DSA, are authenticity and integrity[2], which means that only the authorized persons can access the information or make change or modify the documents. Using DSA algorithm, the administrator will send the study material to the students by applying digital signatures to it and student can verify the signature for authenticity. After

verification, if the signature seems to be ok, then student will accept the material, otherwise, requests the administrator to resend it. That means, the main advantage of object oriented analysis and design is based on encapsulation, data hiding, data abstraction, polymorphism high cohesion and low coupling etc.[3,4].

The metrics can be categorized in the basis of the size, coupling, cohesion, completeness etc. In object oriented metric based analysis, the two main object oriented metrics are Chidamber and Kemerer metric (CK metric) and Metric for Object Oriented Design metric (MOOD metric). These two metrics are also complement to each other. Except these two, there are some other object oriented metrics advised by Lorenz and Kidd, Harrison, Counsell and Nithi etc.[5].

In this paper, we will analyze the value of the object oriented metrics with the help of the class hierarchy diagram of DSA algorithm, which is designed in the basis of sending study material from developer to student in any e-learning system. Here we limit our discussion only on the CK –metric and MOOD metric. In section –II, we will discuss on the class hierarchy diagram of DSA algorithm regarding the transmission of study material from the administrator to student including signature generation (administrator's end) and verification (student's end). Section-III contains discussion on object oriented metrics on the basis of the proposed model. Finally, we will conclude in section-IV, by citing some future scope.

Class Hierarchy Diagram

This class hierarchy diagram is based on the Digital Signature Algorithm of sending study material from the administrator to student in an e-learning system.

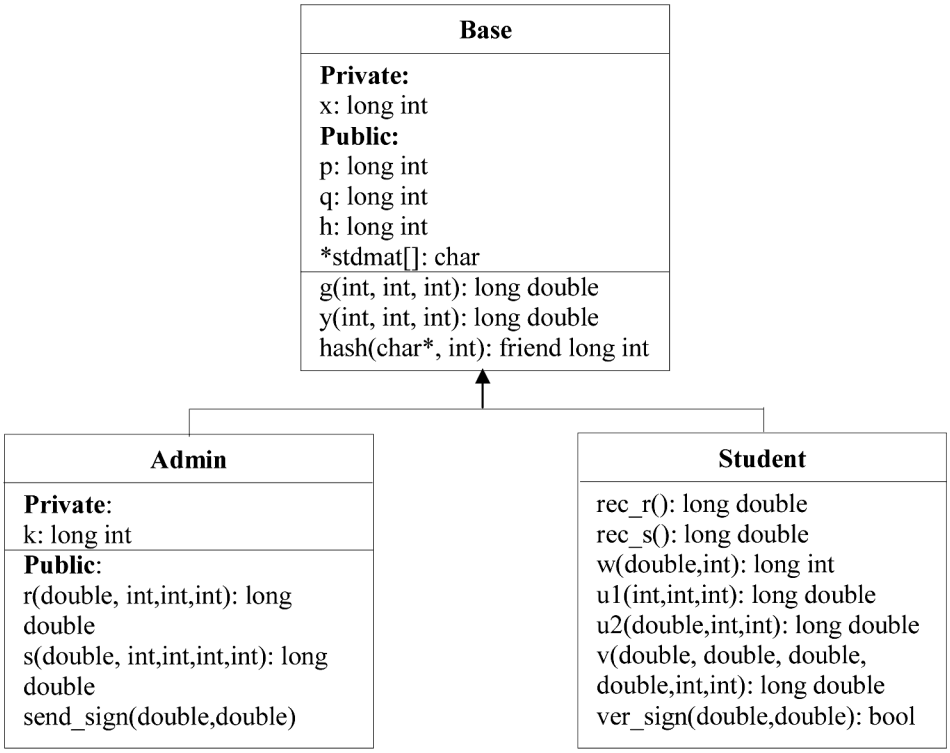

Fig. 1: Class diagram of DSA algorithm signature generation and verification

Class diagram is used in software engineering as a part of Unified Modeling Language (UML), which shows the structure of a system by showing the classes, their attributes, operations and relationship between objects[6]. In this class diagram[7], we use three classes, Base, Admin and Student. The two child classes Admin and Student are publicly derived from the parent class Base.

Base class contains one private data member, the private key x as well as four public data members and three member functions of which y is the public key. This class is also used to generate the hash function. Class Admin has one private data member and three public member functions. This class is used to generate the signature (r,s) and sends it to class Student. Student class receives the signature and verifies it. To achieve this goal, the Student class uses seven member functions. With the help of this class diagram, we will find the values of the metrics below.

Object Oriented Metrics

The advantages of object oriented analysis and design helps the designer to reuse the code, maintenance cost is less, data hidden property can also be achieved and many more. We can characterize the object oriented metrics into the five categories like localization, encapsulation, information hiding, inheritance and data abstraction[8,9]. Though there are so many object oriented metrics proposed by so many persons, the two most used object oriented metrics are Chidamber and kemerer metrics (CK-metrics) and Metric for Object Oriented Design metric (MOOD-metric) and they are also complement to each other. Here we will discuss the metric in brief and then analyze the values of the metrics in respect of our proposed system.

CK-metrics include the following metrics for the object oriented design[10]. First we will shortly discuss on these and then analyze them by using our proposed class diagram using table and charts below[11,12]:

Weighted Methods per Class (WMC): It counts the total number of methods of a class. Less value gives better result.

Coupling Between Object Classes (CBO): CBO is the number of the other classes to which it is coupled. The value should be kept low.

Depth of Inheritance Tree (DIT): The depth of the inheritance tree is calculated by the depth of the class in the inheritance hierarchy. If the value become higher, then it becomes difficult to maintain.

Number of Children (NOC): It is also related with the inheritance. The value of NOC is the number of subclasses directly inherits from that class.

Response For a Class (RFC): The value of the RFC is measured by the sum of the number of methods of the class and the number of methods called by any of those methods[6]. It represents the complexity of the class. If the value is too much high, then it becomes difficult to maintain.

Table 1: Metrics of signature generation and verification using DSA algorithm

Classes of proposed diagram	Object Oriented quality metrics				
	WMC	CBO	DIT	NOC	RFC
Base	3	2	0	2	13
Admin	3	0	1	0	6
Student	7	0	1	0	10

Now, we will plot the values of the above analyzed data of CK-metrics to draw graphs and make some discussion on these values. The value of WMC helps us to predict how much time and effort is required to develop and maintain a class. Fig. 1 shows the graphical representation of WMC. Since, the value of WMC is kept down, so our system is ok.

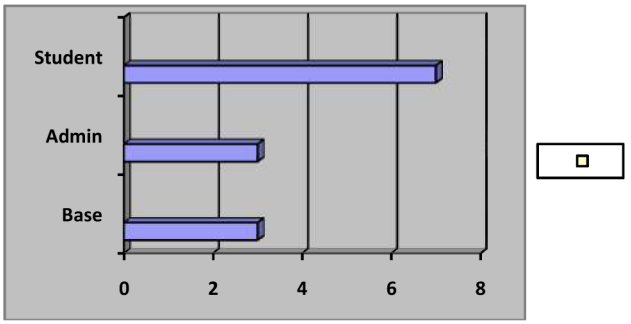

Fig. 1: WMC

Fig 2 shows the graphical representation of CBO of our proposed model, through which we can measure the coupling level of the proposed system. In our model, its value is low, which is preferable.

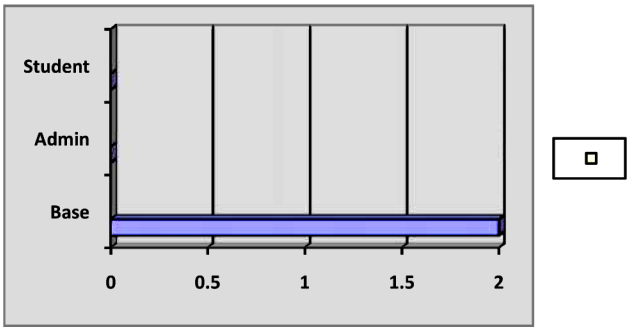

Fig. 2: CBO

Fig 3 shows the graphical representation of the value of DIT, which is mainly used to represent the complexity of a class. Here, the maximum DIT value is 1, which is quite ok.

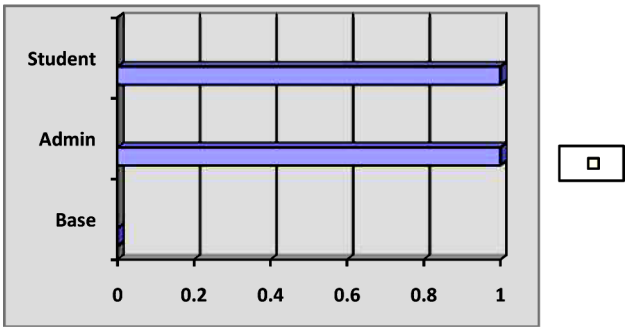

Fig. 3: DIT

Fig. 4 represents the graphical representation of the value of NOC, whose maximum value of our system is 2, which is quite ok.

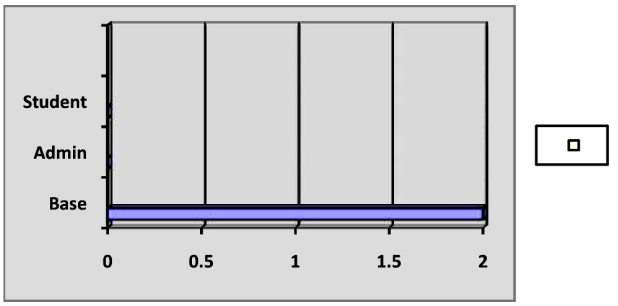

Fig. 4: NOC

The value of RFC is shown graphically in Fig 5. If this value increases, then it becomes difficult to maintain, but here the maximum value is 13, which is very much under control.

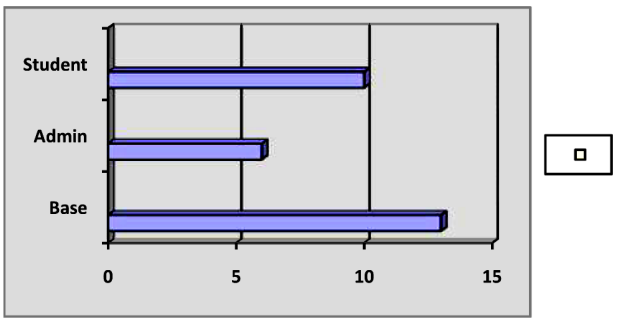

Fig. 5: RFC

Now, we will discuss some of the metrics of the metric for object oriented design (MOOD) metrics related to the transmission of study material using the DSA algorithm from administrator to student in any e-learning system.

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

Where $M_d(C_i) = M_v(C_i) + M_{h'}(C_i)$ where $M_d(C_i)$= methods defined in class C, $M_v(C_i)$ = methods visible in class C and $M_{h'}(C_i)$= methods hidden in class C

Table 2: MHF metrics of proposed system

	Classes of proposed system			
	Base	**Admin**	**Student**	**Summation (∑)**
$M_{h'}(C_i)$	0	0	0	0
$M_{v'}(C_i)$	3	3	7	13
$M_{d'}(C_i)$	3	3	7	13
MHF		0/13=0		

Table 2 shows the value of MHF metric of our proposed system in tabular form. The low value of MHF means our system is very simple.

- Equation for **AHF (Attribute Hiding Factor)** = $\sum_{i=1}^{TC} A_h(C_i) / \sum_{i=1}^{TC} A_d(C_i)$

$A_d(C_i) = A_v(C_i) + A_h(C_i)$, 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

Table 3: AHF metrics of proposed system

	Classes of proposed system			
	Base	**Admin**	**Student**	**Summation (∑)**
$A_h(C_i)$	1	1	0	2
$A_v(C_i)$	4	0	0	4
$A_d(C_i)$	5	1	0	6
AHF		2/6=0.33		

Table 3 shows the AHF value of MOOD metric in respect to our proposed system. This value is less than 1, which is ok.

- Equation for **MIF (Method Inheritance Factor)** = $\sum_{i=1}^{TC} M_i(C_i) / \sum_{i=1}^{TC} M_a(C_i)$

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

Table 4: MIF metrics of proposed system

	Classes of proposed system			
	Base	**Admin**	**Student**	**Summation (∑)**
$M_d(C_i)$	3	3	7	13
$M_i(C_i)$	0	3	3	6
$M_a(C_i)$	3	6	10	19
MIF		6/19=0.316		

From table 4, we can see that the value of MIF of our proposed system is 0.316, which is not too much high or too much low, which is quite ok.

- Equation for **AIF**=$\sum_{i=1}^{TC} A_i(C_i) / \sum_{i=1}^{TC} A_a(C_i)$

Where $A_a(C_i) = A_d(C_i) + A_i(C_i)$, $A_a(C_i)$=number of attributes available, $A_d(C_i)$= number of attributes defined and $A_i(C_i)$= number of attributes inherited

Table 5: AIF metrics of proposed system

	Classes of proposed system			
	Base	**Admin**	**Student**	**Summation (∑)**
$A_d(C_i)$	5	1	0	6
$A_i(C_i)$	0	4	4	8
$A_a(C_i)$	5	5	4	14
AIF			6/14=0.43	

Table 5 shows the AIF value of our proposed system, which is 0.43, which indicate that our system is quite ok.

Conclusion

We have made object-oriented analysis to achieve authenticity regarding transmission of study material from administrator to students in an e-learning system using class diagram of DSA algorithm. This proposed model can also be useful in transmission of other documents like mark sheets, admit cards, registration numbers etc. in any e-learning system. This system may also be applicable in the transmission of documents in other kinds of online systems, like, E-commerce, E-governance etc. To make this system better, we can apply digital watermarking, which is beyond the scope of this paper.

References

1. Graff, J.C., 2001, Cryptography and E-commerce, John Wiley & Sons, New York.
2. Weippl, R.E., 2005, Security in E-Learning, Springer.
3. Rajib Mall, 2006, Fundamentals of Software Engineering, Prentice Hall of India, New Delhi.
4. http://cybarlab.com/ooad.
5. http://ce.sharif.edu/courses/8586/1/ce924/resources/root/4.%20Kamandi_OOMetrics.pdf.
6. https://en.wikipedia.org/wiki/Class_diagram.
7. Ghosh, A. and Karforma S. July 2014, Object Oriented Modeling of DSA for Authentication of Student in E-learning, *International Journal of Science and Research,* 2319-7064, **3**(7): 2293-2297.
8. Edward, V. Berard, Metrics for Object-Oriented Software Engineering, The Object Agency, Inc.
9. Balagurusami, E. 2006, Object oriented programming with C++, Tata McGraw Hill, New Delhi.
10. Karforma, S. and Banerjee S. 2012, DIPRM in E-Commerce system-A UML based approach (Ph.D theses- 2012).
11. Banerjee, S., Karforma, S., Sept. 2015, Object oriented metric based analysis of AElGamal digital signature algorithm for study material authentication, *International Journal of Science Technology and Management,* 2394-1537, **4**(01): 522-530.
12. Banerjee, S. and Karforma, S. 2016, Object oriented metrics based analysis of DES algorithm for secure transmission of mark sheet in e-learning, *International Journal of Computer Sciences and Engineering,* 2347-2693, **4**(1): 093-098.