OBJECT-ORIENTED METRICS ANALYSIS FOR IMPLEMENTATION OF AUTHENTICATION IN SMART CARD BASED E-GOVERNANCE MECHANISM

Abhishek Roy,
Research Scholar
Department of Computer Science
The University of Burdwan, W.B, India.

Dr. Sunil Karforma,
Associate Professor
Department of Computer Science
The University of Burdwan, W.B, India.

ABSTRACT

The gradual scientific enhancements have made the present day society highly technology dependent in nature. To attend this community, nowdays the state owned agencies are extensively using ICT based governance mechanism called Electronic Governance. This paradigm shift from conventional form of governance to electronic form of governance have helped the Government and its Citizenry to a great extent. The administration can launch new developmental project for its Citizenry with less man power, operational cost and more promptness and accuracy. Whereas the Citizenry can access their facilities in-timely manner with ease and transparency. As a natural phenomenon to the real life application of this electronic mechanism, huge data traffic load will be mounted over the servers and the nodes of the system. Eventually the eavesdropper will attempt to breach the entire data transmission process and finally escalate their access to materialize their ill intentions. In this case, the security analyst must prevent the unauthorized access of these services and facilities at any cost. Considering this situation, the authors have already proposed an E-Governance model using object oriented software engineering approach, which is based on a multivariate electronic smart card called Multipurpose Electronic Card (MEC). This smart card will help to uniquely identify its original owner during E-Governance transactions including the financial transactions also. To validate our E-Governance model scientifically, in this paper we have performed the object oriented metrics analysis for authentication of the users using our proposed smart card based E-Governance mechanism.

Keywords: Authentication, Objects, Object-oriented metrics, E-Governance.

INTRODUCTION:

With the gradual scientific enhancements the present day society have become very much technology and electronic gadget dependent in nature for its day to day activities. To attend this technology based community, nowdays the state owned agencies are extensively using Information and Communication Technology (ICT) based governance mechanism called Electronic Governance (i.e E-Governance). This paradigm shift from conventional form of governance to electronic form of governance have helped both the Government and its Citizenry to a great extent. The governmental agencies are able to launch new project for the development of its Citizenry and deployment of administration under its jurisdiction with less man power, operational cost and more promptness and accuracy. Whereas the Citizenry can access their facilties granted by the governmental agencies in-timely manner with ease and transparency. In this way the successful implementation of Electronic Governance mechanism will prove to be an efficient instrument for deployment of corruption free and accurate administration, which is very much necessary specially in the socio-economic scenario of the developing countries. As a natural phenomenon to the real life application of this electronic mechanism, huge data traffic load will be mounted over the severs as well as the nodes of the system. Eventually the eavesdroppers will attempt to breach the data transmission process of E-Governance mechanism and finally escalate their access to materialize their ill intentions. In this case the security analysts will face challenge in true sense to grant access of the governmental services to its authorized and intended users only and prevent the unauthorized access of these services and facilities under any circumstances. To tackle this menace the E-Governance **[2, 3, 5, 9, 10, 11, 12, 13]** models must be designed in a very realistic approach which will cater solutions to all possible anomalies that will get generated during execution of the system. Considering the gravity of the situation, the authors have already proposed an E-Governance model using object oriented software engineering approach which is based on a multivariate electronic smart card called Multipurpose Electronic Card (MEC). This smart card will help to uniquely identify its original owner during any type of E-Governance transaction, even during the time of financial transactions also. To validate our E-Governance model scientifically, in this paper we have performed the object oriented metrics **[8]** analysis for authentication **[1, 6, 7]** of the users using our proposed smart card based E-Governance mechanism

In section – 2 the background of object oriented metrics is discussed. Application of object oriented metrics in context of our proposed E-Governance model is explained in section – 3. The conclusion drawn from the above discussions is mentioned in section – 4. Finally the references are listed in section – 5.

Background Of Object Oriented Metrics:

As in the real world scenario, everything is treated as object which exhibits its distinct parameters, to implement a software system efficiently in this enviornment, it should be designed and analysed in the context of object oriented software engineering methodology. This is the reason why the quality of these software systems need to be analysed dynamically at the early phase. Though the Unified Modeling Language (UML) models are used to capture the static and dynamic aspects of the application, but it is unable to provide the dynamic model simulation of the system. These applications are usually modeled as executable designs prior to deployment in a working environment. This quality metric which relate to external quality attribute of a design includes maintainability, reusability, error-proneness and understandibility. The interaction between the classes or within the classes shows the complexity of the design. Empirical studies revealed that coupling and cohesion techniques have direct impact on the quality of the software and hence shows the interlinking of classes and strength of classes.

The Coupling **[14]** technique measures the relative interdependency between various classes as one class have the connection with the another class. Therefore Coupling can be states as the degree at which a class is connected with other classes in the system. A class is said to be highly coupled with other classes if there are many connections and loosely coupled if there are less connections. The Cohesion technique is measured as the strong bonding among the internal attributes of the class. This the technique which implements intra-modular connectivity of the class. Coupling and Cohesion are always correlated to each other in inverse order i.e if Coupling is high, the Cohesion will be low and vice versa. The best object oriented software design is expected to have low Coupling and high Cohesion level. As the object oriented software designs, which are diagrammatically depicted by Unified Modelling Language (UML) class diagram usually contains both the Independent Classes (IC's) and Dependent Classes (DC's), the Cohesion and Coupling technique are calculated taking them into account. The Independent Classes (IC's) are those which are not dependent on the attributes of other classes of the software system. The Dependent Classes (DC's) are those which are dependent on the

attributes of other classes of the software system. The formula to get the Total number of Classes (TC's) of the object oriented software system is as follows –

Total number of Classes (TC's) = Number of Independent Classes (IC's) + Number of Dependent Classes (DC's)

The Degree of Coupling (DC) is computed after calculating the number of Dependent Classes (DC's) and the number of Independent Classes (IC's). Specifically, Degree of Coupling (DC) can be stated as the ratio of number of Message Received Coupling (MRC) to the Message Passed Coupling (MPC), where Message Received Coupling (MRC) is the number of messages received by a class from the other classes and Message Passed Coupling (MPC) is defined as the number of message passed among objects of the classes within the software system. Hence –

Degree of Coupling (DC) = Message Received Coupling (MRC) / Message Passed Coupling (MPC)

The Degree of Coupling (DC) is designed and represented by Message Calling Graph (MCG), which is demonstrated below using sample diagram –

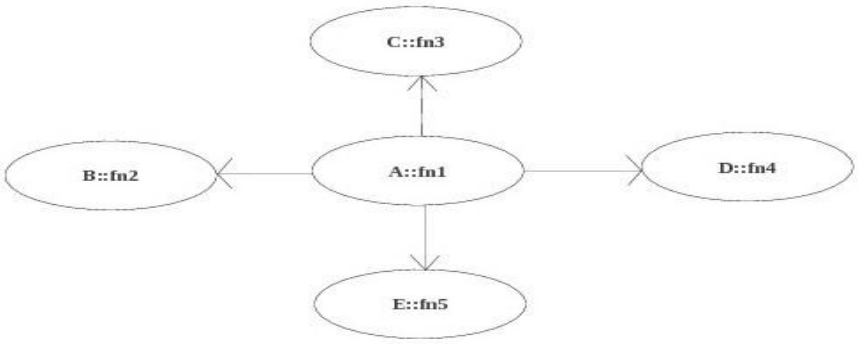

Fig 1 – Sample Message Calling Graph (MCG)

The above shown sample Message Calling Graph (MCG) depicts that fn1( ) method of class A is called by fn2( ) method of class B, fn3( ) method of class C, fn4( ) method of class D and fn5( ) method of class E.

The Degree of Cohesion (DCH) finds the functional strength of associated attributes within a class which shows how strongly a method is depending on the attributes of that class. This is calculated at the attribute level as the ratio of the Number of Attributes Used (NAU) to the Total Number of Attributes (TNA). Hence –

Degree of Cohesion (DCH) = Number of Attributes Used (NAU) / Total Number of Attributes (TNA)

The Degree of Cohesion is designed and represented by Attribute Calling Graph (ACG) which is demonstrated below using sample diagram –

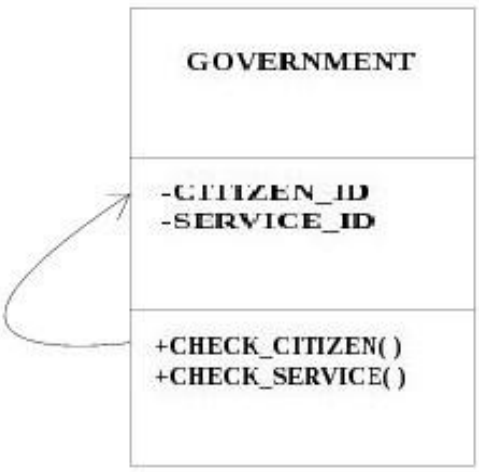

Fig 2 – Sample Attribute Calling Graph (ACG)

The above shown Attribute Calling Graph (ACG) depicts that within the Independent Class (IC) named as GOVERNMENT, the method CHECK_CITIZEN( ) is accessing the attribute of that same class named as CITIZEN_ID for its successful execution.

In the subsequent segment we have implemented this Coupling and Cohesion techniques for authentication of user in our proposed E-Governance model using Multipurpose Electronic Card (MEC).

APPLICATION OF OBJECT ORIENTED METRICS IN THE PROPOSED E-GOVERNANCE MODEL:

For successful implementation of E-Governance mechanism within a hazardous environment we have already proposed a model using Multipurpose Electronic Card (MEC). This smart card will help to authenticate the identity of the Citizen and thereby facilitate the access of the governmental services granted for that intended user only. This proposed smart card will act as the one stop alternative for the following existing governmental instruments with options for further enhancements –

a. Birth Certificate b. Ration Card c. Educational Record d. Employment Card
e. Voter Card f. Driving License g. Insurance Card h. Bank Record
(i.e Debit Card, etc) i. Tour & Travels Record. j. Death Certificate.

For better performance of the proposed model in the real world scenario, the entire mechanism have been implemented in the context of object oriented software engineering paradigm. Since this smart card will also be able to perform financial transactions just like debit cards along with other governmental transactions, it will be very beneficial for the governmental agencies to track the monetary transactions carried out by the Citizenry, which will finally help to crack down the corruption rates as well as the insurgent activities within the state. This will only happen if no other smart cards except this Multipurpose Electronic Card (MEC) remain operational under the jurisdiction of the state owned authority. The conceptual diagram of the proposed Citizen to Government (C2G) type of E-Governance model using Multipurpose Electronic Card (MEC) is as follows –

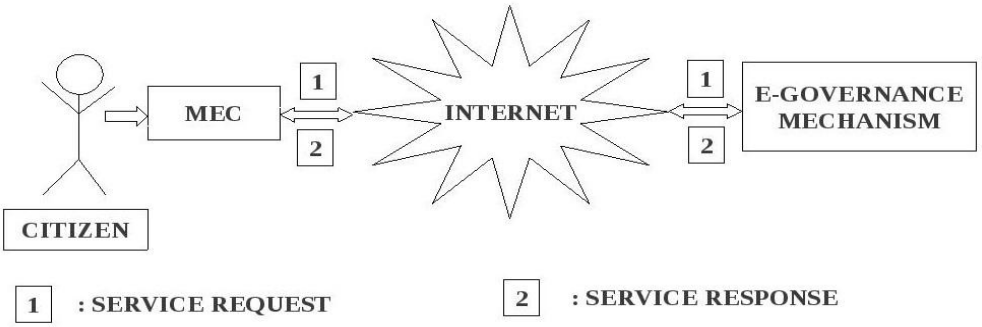

Fig 3 – Conceptual diagram of the proposed E-Governance model in C2G pattern.

The above diagram shows that in C2G type of E-Governance model, the Citizen will initiate the transaction using the Multipurpose Electronic Card (MEC). Multipurpose Electronic Card (MEC) will connect to the E-Governance mechanism along with the user inputs through Internet. The E-Governance mechanism will contain the user verification system deployed within itself, which will first verify the identity of the Citizen from the inputs of Multipurpose Electronic Card (MEC). In case of successful user authentication, the Citizen will be allowed to access the facilities granted by the Government, whereas in case of unsuccessful user authentication, the Citizen will be barred from the access of the services. Considering the sensitivity of the information that will be transmitted using this Multipurpose Electronic Card (MEC), we have tried to implement user authentication through Citizen to Government (C2G) type of E-Governance transaction in the context of Object Oriented Modeling (OOM) of Elliptic Curve Digital Signature Algorithm (ECDSA). Hence, the schematic diagram of our proposed implementation is as follows –

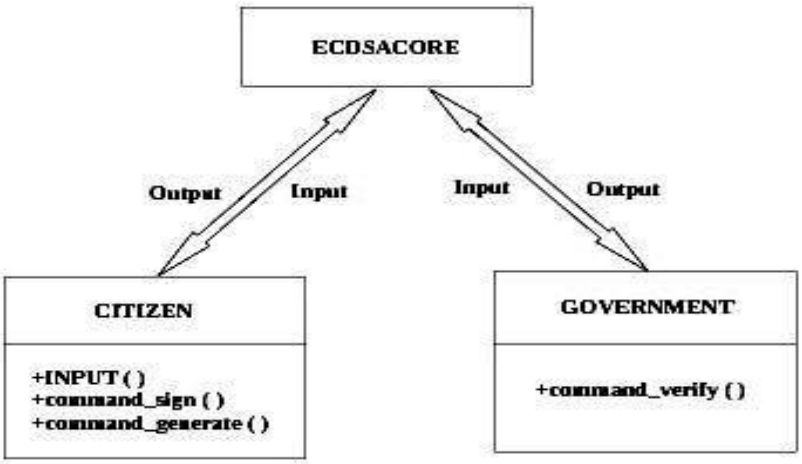

Fig 4 – Schematic diagram for the proposed C2G type of E-Governance model

To implement the above depicted model we have used two Independent Classes (IC's) namely, CITIZEN and GOVERNMENT. The class CITIZEN represents the Citizen. The class GOVERNMENT represents the Government. These classes passes inputs to the publicly available algorithms for hashing, signing and verifying the signature through a executable file named as ECDSACORE. Hashing of the message is done using MD5 algorithm. ECDSACORE file implements the respective algorithms based on the inputs received from the CITIZEN and GOVERNMENT class and generates the corresponding output. Hence, ECDSACORE can be considered as a open source platform which is accessible to all uniformly. It is the inputs send to this executable file which matters for the successful implementation of the proposed multifaceted smart card based E-Governance model. The Independent Classes (IC's) used in our design are mentioned below –

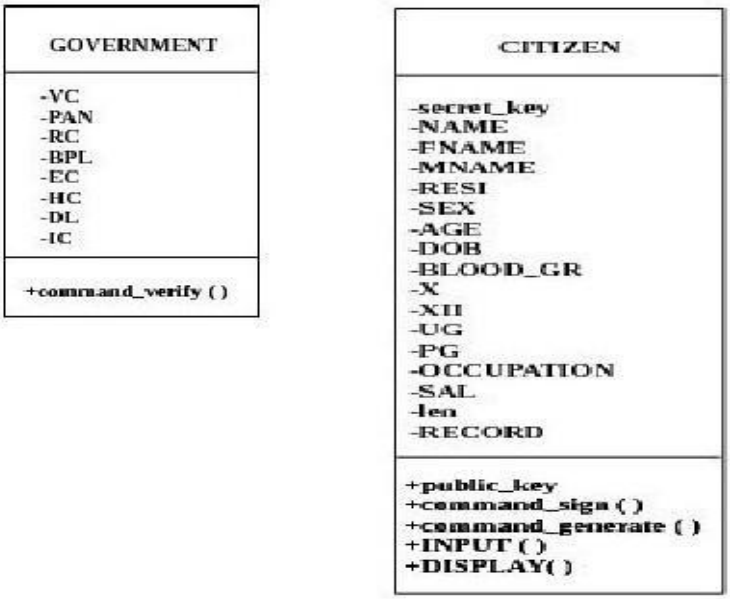

Fig 5 – Class GOVERNMENT and Class CITIZEN used in Object Oriented Modeling (OOM) of ECDSA.

As both of the classes GOVERNMENT and CITIZEN are performing their data input and output operations through file handling, there is no direct connection established between them. Hence, we are not providing the Message Calling Graph (MCG) in this case. The Degree of Cohesion (DCH) calculated in the attributes level of our design are mentioned below –

Table 1 – Degree of Cohesion (DCH) analysis in Object Oriented Modelling (OOM) of ECDSA.

Name of the Class	Object Oriented Metrics		
	Number of Attributes used (NAU)	Total number of Attributes (TNA)	Degree of Cohesion (DCH)
CITIZEN	17	18	17 / 18
GOVERNMENT	3	8	3 / 8

The corresponding Attribute Calling Graph (ACG) of the proposed E-Governance model using Multipurpose Electronic Card (MEC) are as shown below.

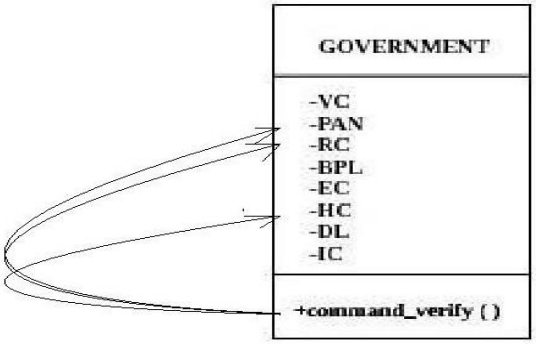

Fig 6 – Attribute Calling Graph (ACG) for the class GOVERNMENT in C2G type of E-Governance model.

The above diagram depicts that, in case of valid user authentication the GOVERNMENT initially accesses the PAN (i.e Permanent Account number), RC (i.e Ration Card) and HC (i.e Health Card) attributes of its Citizen out of the other attributes named as VC (i.e Voter Card), BPL (i.e Below Poverty Line), EC (i.e Employment Card), DL (i.e Driving Licence) and IC (i.e Insurance Card).

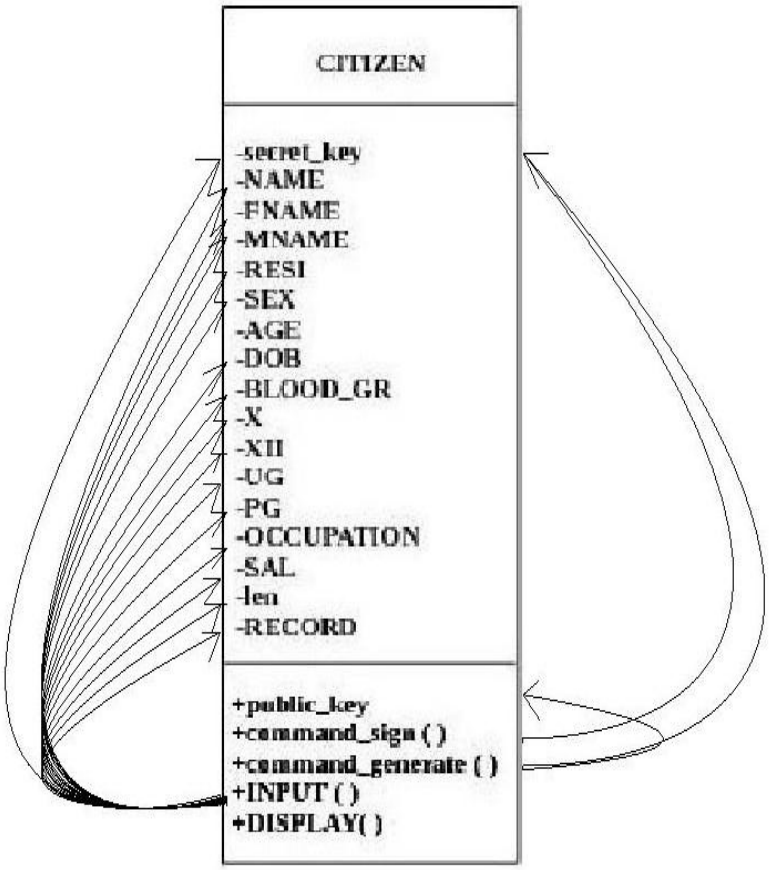

Fig 7 – Attribute Calling Graph (ACG) for the class CITIZEN in C2G type of E-Governance model.

The above diagram shows that in the initial the CITIZEN accesses its 17 attributes out of total 18 attributes using member methods command_generate( ) and command_sign( ).

CONCLUSION:

From the above discussions it is clear that our proposed Multipurpose Electronic Card (MEC) will prove to be beneficial in nature for both the GOVERNMENT and CITIZEN during electronic governance transactions. Since this instrument have been successfully implemented over Citizen to Government (C2G) model of E-Governance using Elliptic Curve Digital Signature Algorithm (ECDSA), we also believe that it will be equally efficient over other models of E-Governance. Finally we have analyzed our design using the metrics of object oriented technology. As the future scope of this work, we will consider to implement our proposed model through software engineering approach using other industry standard digital signature **[4]** and digital certificate algorithms accompanied by object oriented metrics analysis.

REFERENCES:

[1] **Roy, A.**, Karforma, S., Banik, S. (2013). *Implementation of authentication in E-Governance – An UML Based Approach*. LAP Lambert Academic Publishing, Germany, ISBN: 978-3-659-41310-0.

[2] **Roy, A.**, Karforma, S. (2013). *UML based modeling of ECDSA for secured and smart E-Governance system*. Computer Science & Information Technology (CS & IT - CSCP 2013), Proceedings of National Conference on Advancement of Computing in Engineering Research (ACER13), pp: 207 - 222, ISSN: 2231 - 5403, ISBN: 978-1-921987-11-3, DOI: 10.5121/csit.2013.3219.

[3] **Roy, A.**, Karforma, S. (2012). *Object Oriented approach of Digital certificate based E-Governance mechanism.* Computational Intelligence and Communication Engineering, International Joint Conference

on CIIT, CENT, CSPE and CIITCom 2012 Proceedings, LNICST **Springer** Chennai, INDIA, pp: 360 - 366, ISSN: 1867-8211.

[4] **Roy, A.**, Karforma, S. (2012). *A Survey on digital signatures and its applications*. Journal of Computer and Information Technology Vol: 03 No: 1 & 2, pp: 45-69, ISSN: 2229-3531.

[5] Hoda, A., **Roy, A.**, Karforma, S. (2012). *Application of ECDSA for security of transaction in E-Governance*. Proceedings of Second National Conference on Computing and Systems - (NaCCS - 2012) organized by the Department of Computer Science, The University of Burdwan, pp: 281-286, ISBN: 978-93-80813-18-9.

[6] Sarkar, S., **Roy, A.** (2012). *A Study on Biometric based Authentication*. Proceedings of Second National Conference on Computing and Systems - 2012 (NaCCS - 2012) organized by the Department of Computer Science, The University of Burdwan, pp: 263-268, ISBN: 978-93-80813-18-9.

[7] **Roy, A.**, Sarkar, S., Mukherjee, J., Mukherjee, A. (2012). *Biometrics as an authentication technique in E-Governance security*. Proceedings of UGC sponsored National Conference on "Research And Higher Education In Computer Science And Information Technology, RHECSIT-2012" organized by the Department of Computer Science, Sammilani Mahavidyalaya in collaboration with Department of Computer Science and Engineering, University of Calcutta, Vol: 1, pp:153-160, ISBN: 978-81-923820-0-5.

[8] Saxena, V., Kumar, S. (2012). *Impact of Coupling and Cohesion in Object-Oriented Technology*. Journal of Software Engineering and Applications, Vol. 5, No. 9, pp: 671-676, DOI: 10.4236/jsea.2012.59079.

[9] **Roy, A.**, Karforma, S. (2011). *Risk and Remedies of E-Governance Systems*. Oriental Journal of Computer Science & Technology (OJCST), Vol: 04, No: 02, pp: 329-339, ISSN: 0974-6471.

[10] **Roy, A.**, Banik, S., Karforma, S. (2011). *Object Oriented Modelling of RSA Digital Signature in E-Governance Security*. International Journal of Computer Engineering and Information Technology (IJCEIT), Summer Edition, Vol. 26, Issue No. 01, pp: 24-33, ISSN: 0974-2034.

[11] **Roy, A.**, Karforma, S. (2011). *A Survey on E – Governance Security*. International Journal of Computer Engineering and Computer Applications (IJCECA). Fall Edition, Vol. 08, Issue No. 01, pp: 50-62, ISSN: 0974-4983.

[12] **Roy, A.**, Banik, S., Karforma, S., Pattanayak, J. (2010). *Object Oriented Modeling of IDEA for E-Governance Security*. Proceedings of International Conference on Computing and Systems (ICCS 2010), organized by Department of Computer Science, The University of Burdwan, West Bengal, INDIA, pp:263-269, ISBN: 93-80813-01-5.

[13] Sur, C., **Roy, A.**, Banik, S. (2010). *A Study of the State of E-Governance in India*. Proceedings of National Conference on Computing and Systems (NACCS 2010), organized by Department of Computer Science, The University of Burdwan, West Bengal, INDIA, pp- (a)-(h), ISBN: 8190-77417-4.

[14] *Dynamic Metrics for Object Oriented Designs*. Retrieved June 28, 2013, from http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?arnumber=809725.
