Volume 4, Issue 4, April 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Study on Implementation of Security in E-Governance using Cryptography

Abhishek Roy
Research Scholar,
Dept. of Comp. Sc., The University of Burdwan,
W.B, INDIA 713104, India
URL: abhishekroy.wix.com/home

Sunil Karforma
Associate Prof.,
Dept. of Comp. Sc.,
The University of Burdwan,
W.B, INDIA 713104, India

Abstract— In the present days of global economic meltdown the Government of the developing countries like INDIA are facing severe challenge in maintaining an efficient administration in its core and allied sectors within an affordable budget. The application of advanced Information and Communication Technology (ICT) will help to implement the Electronic Governance which will replace its conventional form to deliver services to the populace at reduced rate. To do so, the Citizen must possess a multivariate electronic instrument which will uniquely identify the Citizen in all respect and help to communicate with the Government. Though our Government have launched several identity instruments which claims to uniquely identify the Citizen w.r.t that respective nomenclature only, non so ever have the provision to become a complete E-Governance instrument, not even the latest Aadhaar Card. The authors have already proposed a Citizen centric multivariate smart card based secured E-Governance mechanism which will perform all the governmental transactions, including the financial ones also. The authors have entrusted the security system of the proposed model using object oriented modeling of RSA Digital Signature Algorithm, Elliptic Curve Digital Signature Algorithm (ECDSA) over G2C and C2G models of E-Governance respectively. The Software metrics have also been used to analyze the efficiency factor of the proposed model. Moreover, the authors have done the data modeling of the proposed mechanism using Entity Relationship Diagram (ERD). In this article, the authors intend to study the task accomplished yet, so that, this model can be implemented in the real-world scenario, which is actually beyond the scope of an individual.

Keywords— E-Governance, Information Security, User Authentication, Cryptography, Smart Card.

I. INTRODUCTION

In the present days of global economic meltdown the Government of the developing countries like INDIA are facing severe challenge in maintaining an efficient administration in its core and allied sectors like business, education, health, etc, throughout its jurisdiction within an affordable budget. This task becomes more difficult if the Indian Rupee (INR) regularly faces new highest of inflation due to recession. However, nobody will disagree that, to defend this recession, the Government must use its resources in a very skilful manner, so that existing budget expenses get reduced, thereby maintaining its efficiency level. The application of advanced Information and Communication Technology (ICT) will help to implement a Citizen centric Electronic Governance mechanism which will operate on behalf of the conventional form of Governance and will deliver services to the doorstep of the populace at reduced rate. To do so, the Citizen must possess a multivariate electronic instrument which will uniquely identify the Citizen in all respect and help to communicate with the Government. Though our Government have launched several identity instruments which claims to uniquely identify the Citizen w.r.t that respective nomenclature only, non so ever have the provision to become a complete E-Governance instrument, not even the latest Aadhaar Card. Focusing on this topic, the authors have already proposed a Citizen centric multivariate smart card based secured E-Governance mechanism which will be capable enough to perform all the governmental transactions, including the financial ones also.

The origin of the research work is mentioned in Section - II. The proposed E-Governance model is discussed in Section - III. Section - IV studies the user authentication technique using the Object oriented modeling of RSA and ECDSA digital signatures along with brief idea of data modeling for the proposed mechanism. Section - V draws conclusion obtained from the entire discussion. References are listed at the last part of this article.

II. ORIGIN OF RESEARCH WORK.

An efficient E-Governance mechanism must understand the requirements of the Citizen as they will be the ultimate end-users. In INDIA, the populace is severely suffering due to the menace of hybrid governance, which mostly comprises of conventional pattern incorporated with electronic pattern in a very unplanned manner. The situation have become so much critical that the Citizen are forced to carry multiple identity instrument to justify their identity during various electronic transactions, which mostly comprises of common parameters of an individual. For better understanding of the problem we may take example of Ration Card, Voter Card, Permanent Account Number (PAN) card, Aadhaar Card, etc

which displays almost the same information of an individual with addition of biometric parameter only in the case of Aadhaar Card. It becomes more confusing when it reveals that, though Aadhaar Card comprises of biometric parameter of an individual, yet it is incapable of performing all E-Governance transactions, as it does not contain any provision for electronic financial transactions. That means if Aadhaar Card is only meant to provide a valid identity to the Citizen, then we are already having our Voter Card, PAN Card for the same purpose. Furthermore to digitize the conventional ration system, Government is also launching the Digital Ration Cards for the Citizen, even after spending crores of money for implementation of Aadhaar Card. Though Government is spending crores of money to provide valid identity to the Citizen through the launch of several identity instruments, yet it failed to identify an individual as a whole with a single identification number irrespective of its nomenclature. As a result an individual is having unique identification number with reference to that particular nomenclature only. Each time Government is launching a new identity system, it is only adding to the existing count, with non so ever having the provision for electronic mode of financial transactions. On the other hand the Citizen are also forced to carry several smart cards like Debit Cards, Credit Cards, issued by the banks to its customers for performing financial transactions. To sum up, in this present situation Citizen have to carry all the identity instruments and the smart cards provided by Government, several banking houses, and other co-realted sectors. Hence, the attackers have an appropriate platform to materialize their ill-intentions as a Citizen can be addressed by multiple identification numbers and smart cards for various governmental transactions.

III. PROPOSED E-GOVERNANCE MODEL.

With the objective to provide smart, secured and an efficient Governance, we have proposed a Citizen centric multivariate smart card based Electronic Governance mechanism. In this model, the proposed electronic instrument named Multipurpose Electronic Card (MEC) will act as the ultimate interface between the Government and the Citizen. The conceptual diagram of the proposed E-Governance model during C2G type of transactions is shown in Fig - 1, where the Citizen performs E-Governance transactions using Multipurpose Electronic Card (MEC).

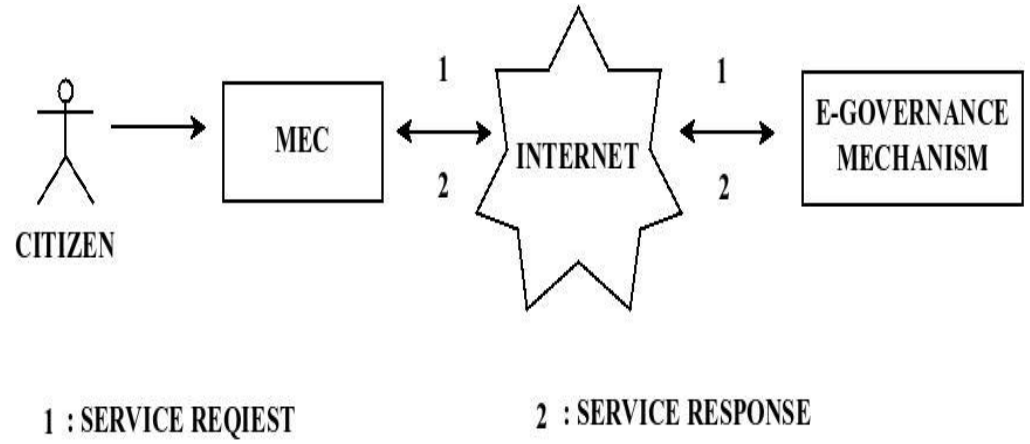

Fig. 1 Conceptual Diagram of the proposed E-Governance models.

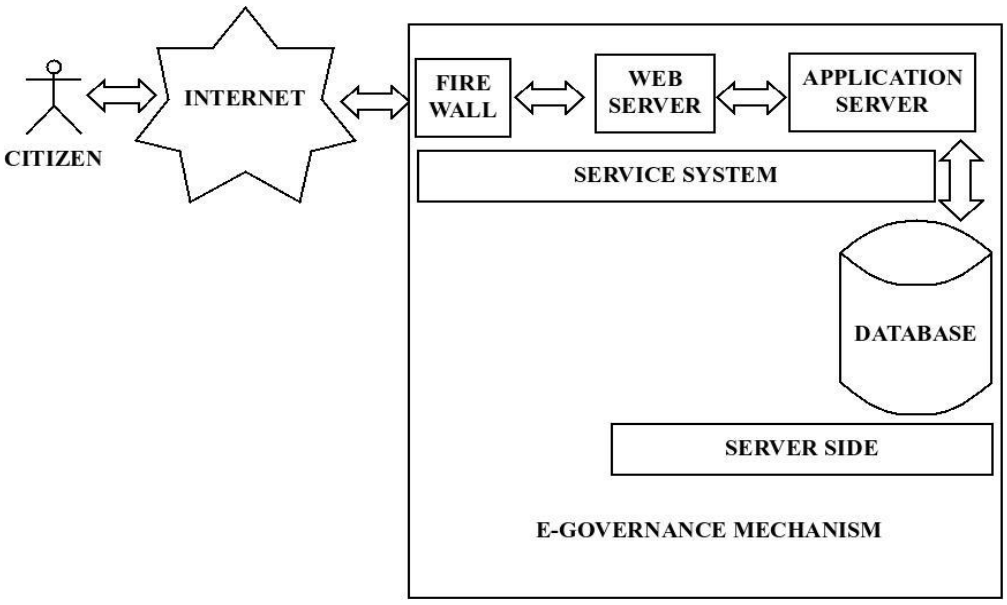

Fig. 2 3-tier architecture of the proposed E-Governance model.

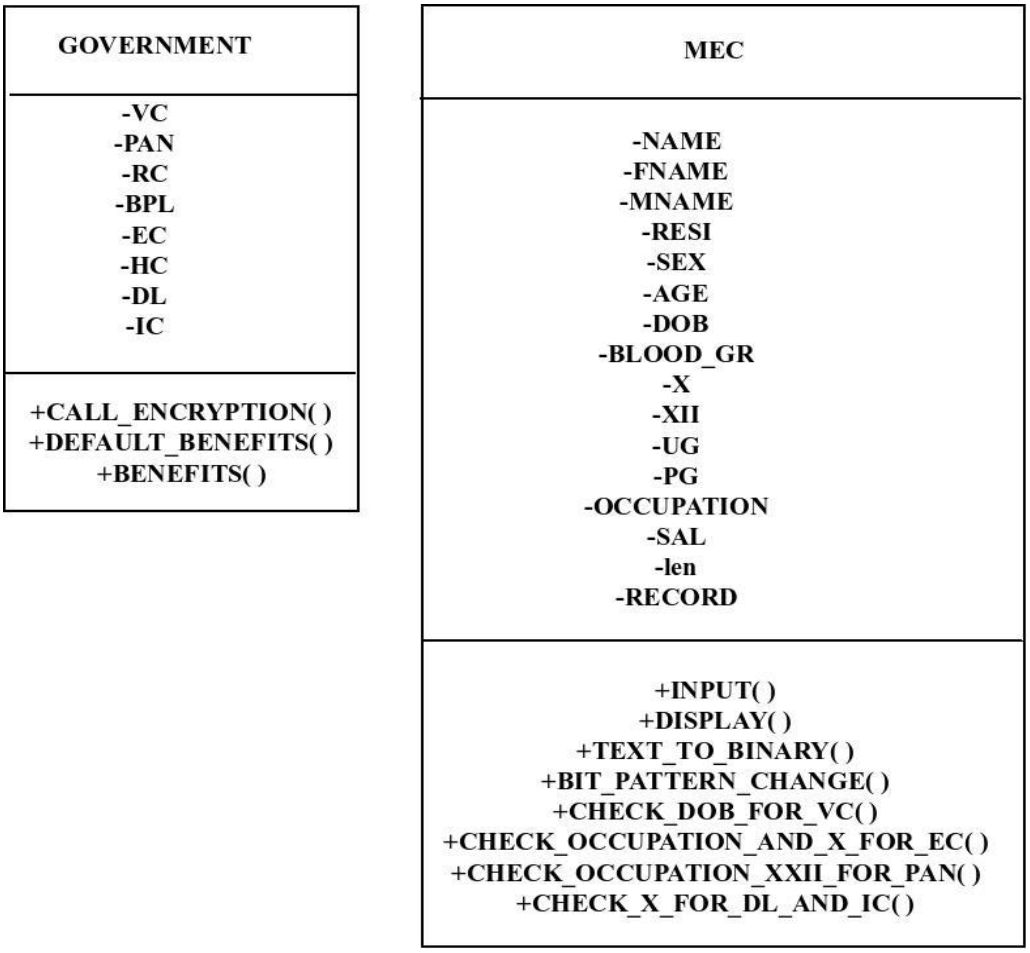

Fig. 3 Class Government and MEC for OOM of RSA Digital Signature.

The 3-tier architecture of the proposed model during C2G type of transactions is shown in Fig - 2, whose further description is as follows -

1. The Citizen intend to communicate with the Government using Multipurpose Electronic Card (MEC).
2. Multipurpose Electronic Card (MEC) will further interact with the E-Governance mechanism through internet.
3. The Electronic mechanism contain the following components for handling the sensitive data in a secured manner.

3.1 Firewall - Firewall will prevent the entry of spam ware, malware and other malicious elements within the mechanism. This will act as the strong checkpoint to perform the further database management securely.

3.2 Web server - After the data passes through the firewall, it enters the Web Server of the electronic mechanism. The alteration of the information performed during governmental transactions are reflected here. The application of various web based technologies will prove to be beneficial in this phase.

3.3 Application server - In this phase the data performs the necessary interaction with the Application Server of the system.

3.4 Database - The resultant data set of the final E-Governance transaction are stored in the database for future use.

Since this proposed electronic instrument will act as the ultimate interface between the Government and the Citizen during E-Governance transactions, it is clear that huge load will be mounted over the database. We have shown it using a single database structure just to get a simple view of the complex structure. However in practical scenario the application of distributed database management system will help to avoid the database server failures.

4. The Service System of the proposed E-Governance mechanism comprises of the Firewall, Web Server and the Application Server.
5. The Server side comprises of the Web Server, Application Server and the Database storage.
6. The entire data transmission through this mechanism will proceed in bi-directional manner which includes request from the Citizen and its corresponding reply from the Government.

To establish our proposed E-Governance model, the task accomplished so far may be listed as below -

1. We have studied the state of E-Governance [1, 2, 4, 5, 6, 8, 10, 11, 12, 13, 14, 15] in Indian scenario, to understand the real scenario.
2. Performed extensive literature survey on the security features of E-Governance which becomes the main factor for launching of effective E-Governance model.

3. Discussed the risk factors and their probable remedies in E-Governance to analyse the pit falls of the E-Governance transactions.

4. Performed extensive literature survey on Digital Signatures [7] and its applications to find its application in our proposed E-Governance model.

5. Implemented data security and privacy using object oriented modeling of International Data Encryption Algorithm (IDEA) in G2C model of proposed E-Governance mechanism.

6. Performed Object Oriented Modeling (OOM) of RSA digital signature in G2C model of proposed E-Governance mechanism.

7. Applied ECDSA in C2G model of E-Governance for optimum resource utilization during transactions.

8. Object Oriented Modeling (OOM) of ECDSA in C2G model of proposed E-Governance mechanism.

9. Performed analysis of our proposed mechanism using software metrics.

10. Performed extensive literature survey for application of biometric [3,9] techniques for authentication of users in electronic mechanism to find its suitability in our proposed model.

11. Performed Unified Modeling Language (UML) based modeling of our model using Digital Certificate (DC).

Furthermore, the implementation of security parameters over our proposed Citizen centric smart card based E-Governance model, which are mentioned above, are discussed below in a brief manner. As we have already done extensive literature review over various aspects of cryptographic security protocols, henceforth we will concentrate over the study of our implementations only.

IV. AUTHENTICATION OF USER IN PROPOSED E-GOVERNANCE MECHANISM.

Fig - 2 also indicates that for successful execution of the proposed smart card based E-Governance mechanism, the identity of the user must be verified carefully so that the intruder is not allowed to enter the E-Governance mechanism and fulfill its ill-intentions thereafter. We have already implemented the user authentication technique over our proposed E-Governance mechanism using complex cryptographic algorithms like RSA and Elliptic Curve Digital Signature Algorithm (ECDSA) blended with the Object Oriented Software Engineering (OOSE) approach, which are briefly mentioned below.

A. OBJECT ORIENTED MODELING OF RSA DIGITAL SIGNATURE.

We have implemented the user authentication technique in our proposed E-Governance mechanism using Object Oriented Modeling of RSA digital signature over G2C type of transactions. The classes used during this implementation are shown in Fig - 3, which explains the static structure of class Government and class MEC, whereas Fig - 4 shows the static structure of class Citizen and class Authentication. In our application, encryption of information is done based on the call of the Government, whereas the decryption of information is done based on the call of the Citizen. For better understanding of these message passing and their corresponding replies, the Inheritance Diagram of Object Oriented Modeling (OOM) of RSA Digital Signature is shown in Fig - 5, which states that Government initiates the transactions and subsequent encryption of messages, whereas the Citizen responds for subsequent decryption of the encrypted messages.

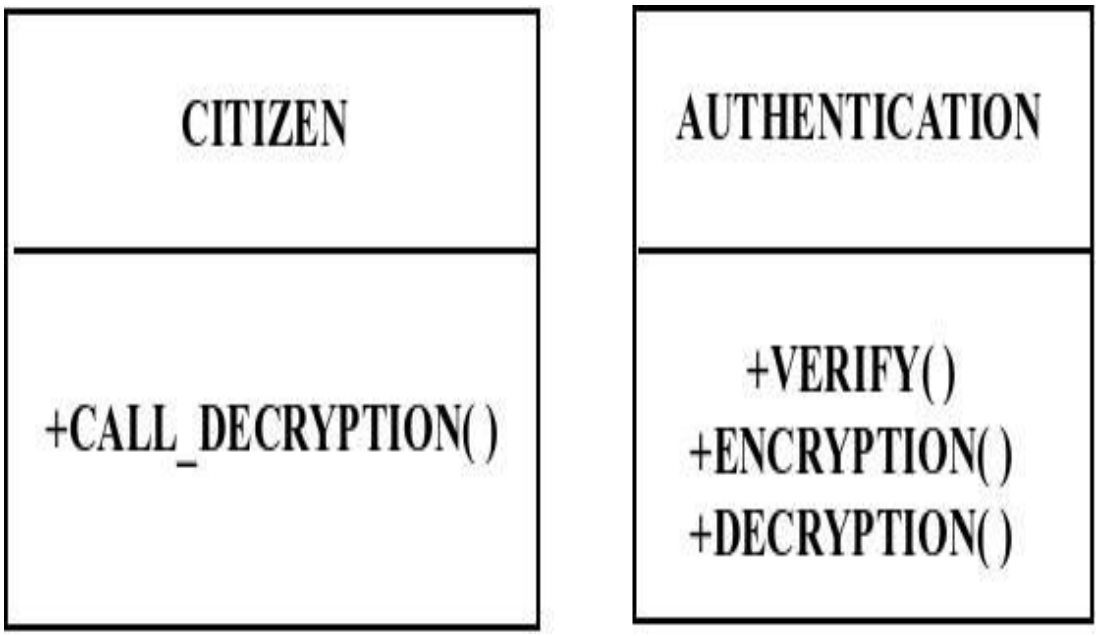

Fig. 4 Class Citizen and Authentication for OOM of RSA Digital Signature.

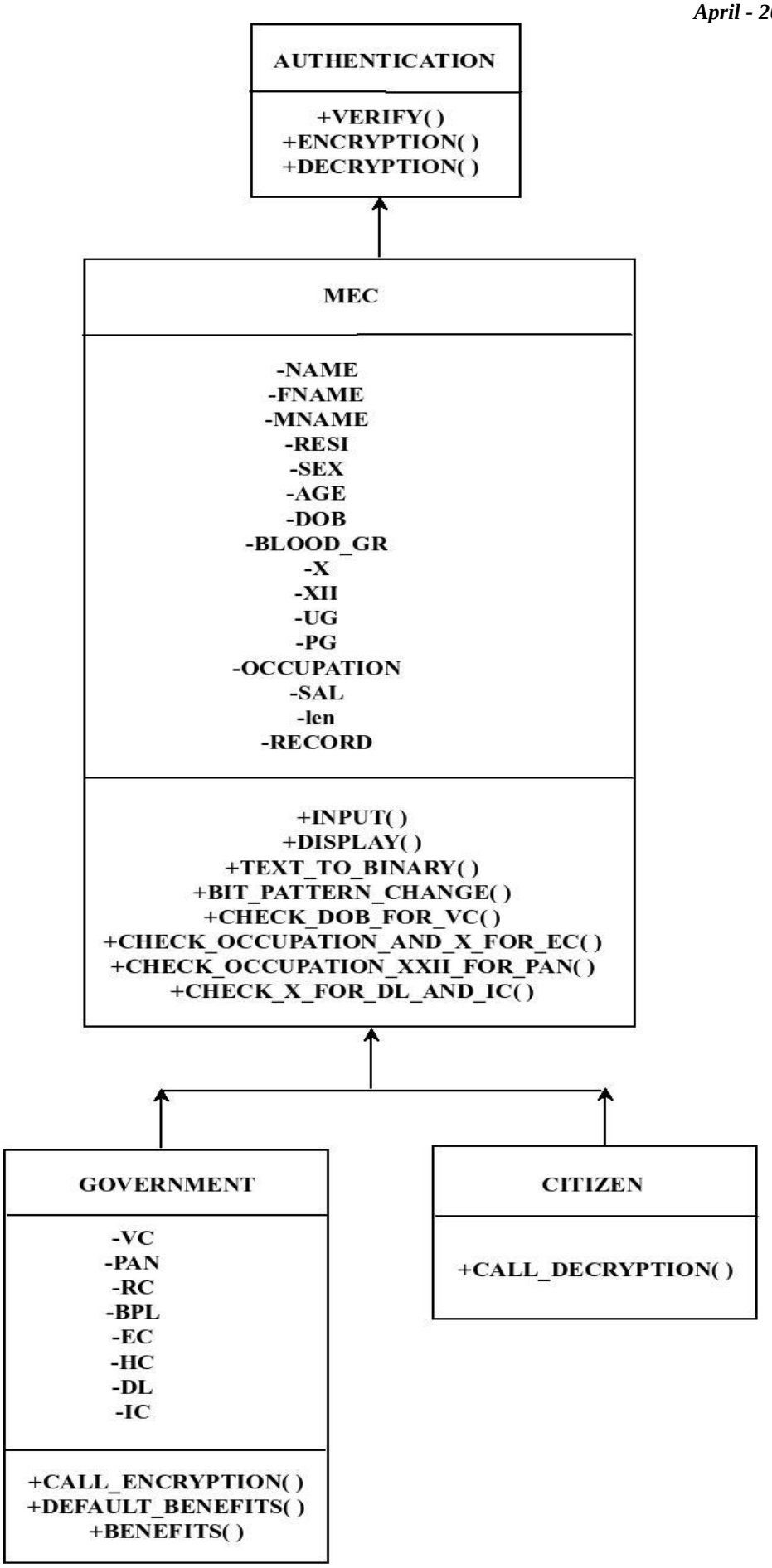

Fig. 5 Inheritance Diagram for OOM of RSA.

B. OBJECT ORIENTED MODELING OF ECDSA.

We have also implemented the user authentication technique in our proposed E-Governance using Object Oriented Modeling (OOM) of Elliptic Curve Digital Signature Algorithm (ECDSA) over C2G type of transactions. The classes Citizen and Government used during the said implementation are shown in Fig - 6, whereas the schematic diagram of this application is shown in Fig – 7.

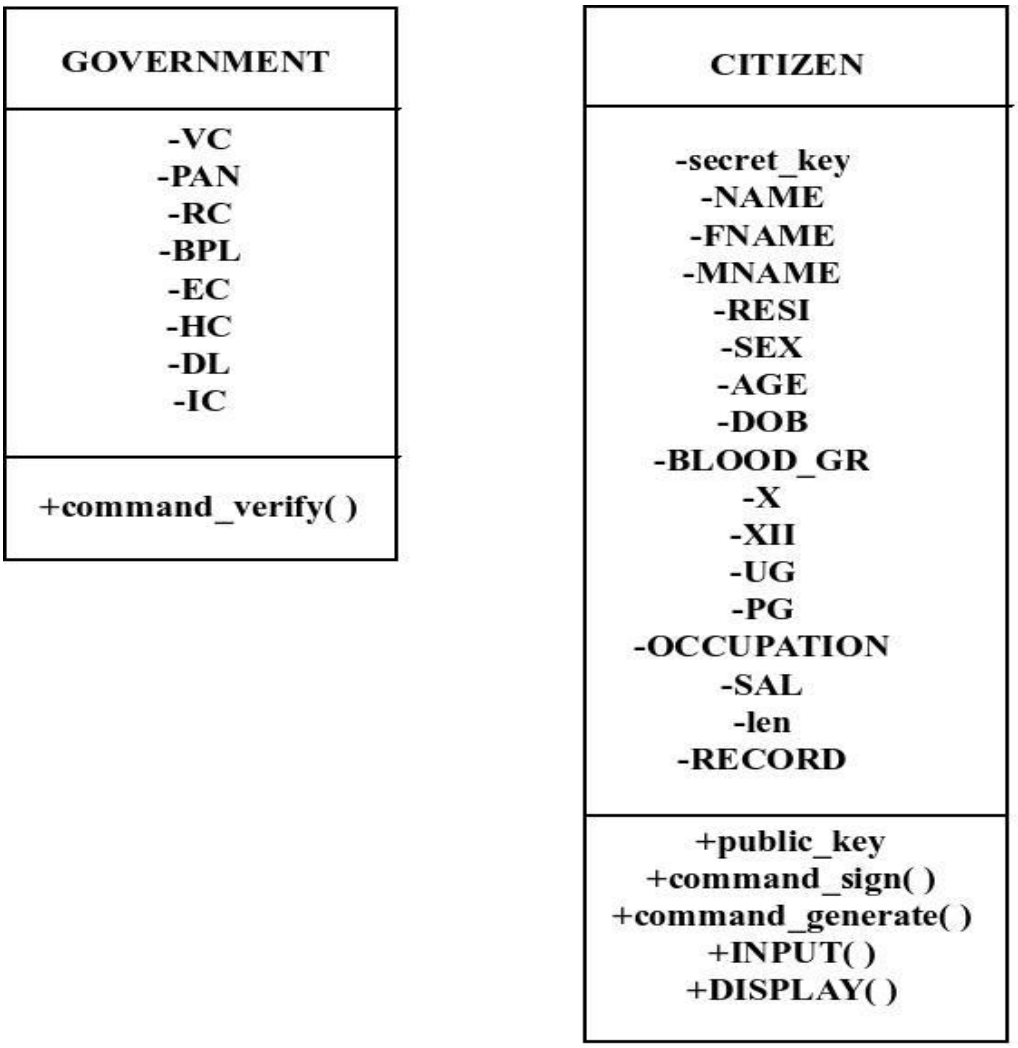

Fig. 6 Class Government and Citizen for OOM of ECDSA.

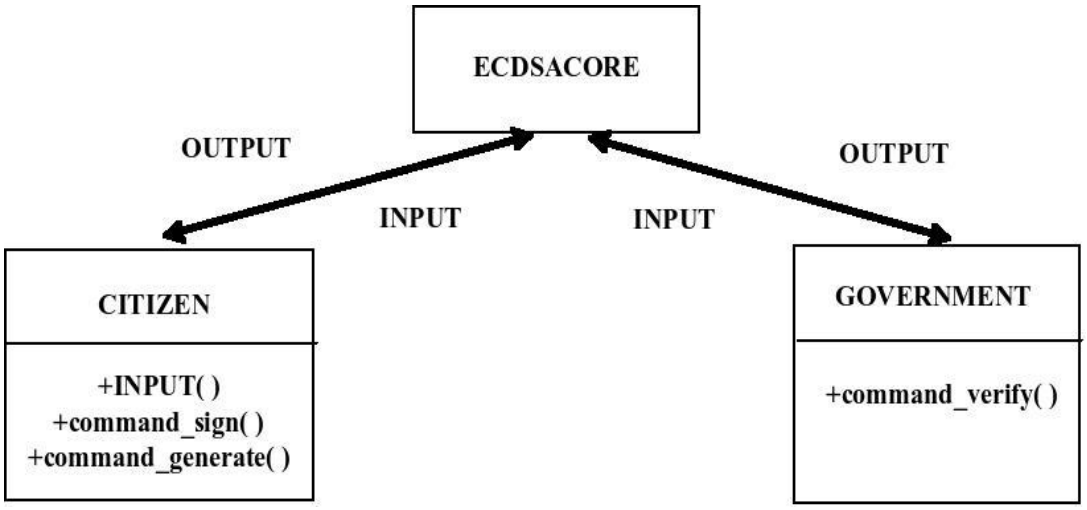

Fig. 7 Schematic Diagram for OOM of ECDSA.

In our application two classes Citizen and Government passes input 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 algorithm based on the inputs received from the class CITIZEN and GOVERNMENT and generates the corresponding output. Hence, ECDSACORE can be considered as an open source platform. 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. In our application Citizen initiates the encryption of information and Government performs the decryption of information.

C. DATA MODELING.

As this electronic instrument will act as the ultimate interface between the Government and the Citizen, it is expected to handle huge data load. For secure handling of these classified information, in Fig - 8 we have shown the data modeling using Entity Relationship Diagram (ERD) during implementation of user authentication by Object Oriented Modeling (OOM) of RSA Digital Signature Algorithm over G2C type of E-Governance. The attributes of the Government and the Citizen displayed in this Entity Relationship Diagram (ERD), are already shown through Fig - 3 and Fig - 4 of this article. Thus, the Entity Relationship Diagram (ERD) may be further described as below -

1. INPUT DATA - Citizen provides the essential information to the Government through Multipurpose Electronic Card (MEC).
2. USER AUTHENTICATION - Citizen authenticates its identity for access of benefits granted by the Government. The entire transaction is done with the help of Multipurpose Electronic Card (MEC).
3. STORE SERVICE - Government stores the services provided to the Citizen in a E-Service server.
4. BENEFITS - E-Service server allows the access of the services to the Citizen after proper authentication.

Though we have tried to demonstrate the relations between the entities in a simpler fashion, in practical scenario the situation will certainly change as distributed database management needs to be incorporated for successful management of huge databases.

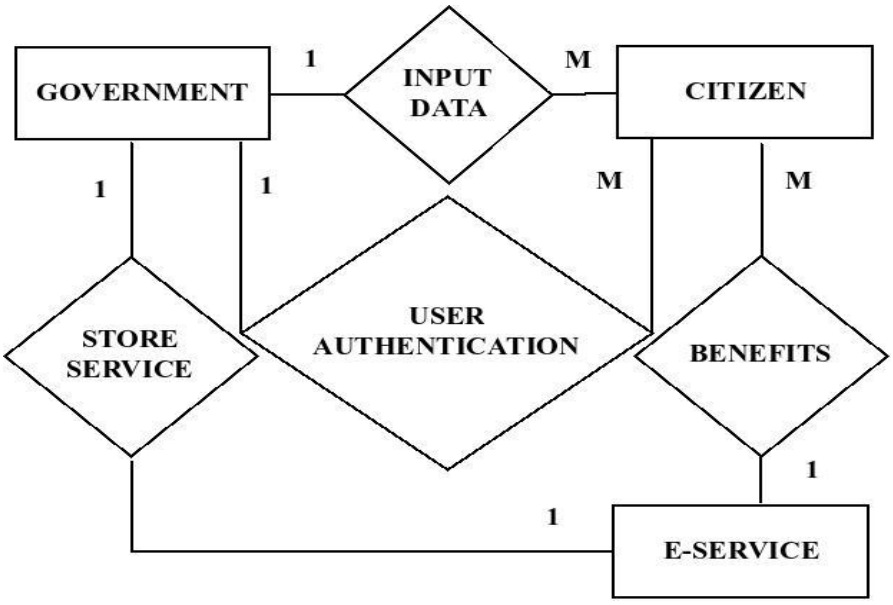

Fig. 8 Entity Relationship Diagram for OOM of RSA digital signature.

V. CONCLUSION.

We have implemented the user authentication in our proposed E-Governance mechanism using Object Oriented Modeling (OOM) of RSA and ECDSA digital signature algorithm. We have also briefly discussed the data modeling in our model through Entity Relationship Diagram (ERD) during object oriented implementation of RSA digital signature algorithm for authentication of the user. Even we have performed the analysis of our proposed E-Governance mechanism using various software metrics. However, as the entire application is till date in conceptual level only, we expect further enhancements during its practical implementation, which can be considered as the future scope of this research work.

References

1. Abhishek Roy, Sunil Karforma, *Coupling and cohesion analysis for implementation of authentication in E-Governance*, ACEEE Conference Proceedings Series 02, Fourth International Joint Conference - Advances in Engineering and Technology (AET) 2013, December 13-14, 2013 (Elsevier), Pp: 544-554, Organized by: The Association of Computer Electronics and Electrical Engineer (ACEEE), The Association of Mechanical and

Aeronautical Engineers (AMAE), The Association of Civil and Environmental Engineers (ACEE), Sponsored by : Indian Society for Technical Education (ISTE), NCR, INDIA. ISBN 978-93-5107-193-8.

2. Abhishek Roy, Sunil Karforma, *Object oriented metrics analysis for implementation of authentication in smart card based E-Governance mechanism*, Researchers World – Journal of Arts, Science and Commerce, October 2013, Volume – IV Issue – 4(2) Pp: 103 – 109 Print ISSN 2231-4172 Online ISSN 2229-4686.
3. Sumita Sarkar, Abhishek Roy, *Survey on Biometric applications for implementation of authentication in smart Governance*, Researchers World – Journal of Arts, Science and Commerce, October 2013, Volume – IV Issue – 4(1) Pp: 103 – 114, Print ISSN 2231-4172 Online ISSN 2229-4686.
4. Abhishek Roy, Sunil Karforma, Subhadeep Banik, *Implementation of authentication in E-Governance – An UML Based Approach*, Book published by LAP Lambert Academic Publishing 2013 1 *Ed*, Germany, ISBN 978-3-659-41310-0
5. Abhishek Roy, Sunil Karforma, *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) organized by Global Institute of Management and Technology, March 22 - 23, 2013, Pp: 207 - 222, ISSN 2231 - 5403, ISBN 978-1-921987-11-3, DOI: 10.5121/csit.2013.3219
6. Abhishek Roy, Sunil Karforma, *Object Oriented approach of Digital certificate based E-Governance mechanism*, ACEEE Conference Proceedings Series 03, International Conference on IPC&ITEeL ACT&CIIT CENT&CSPE 2012 Proceedings, December 03-04, 2012 (Elsevier), Pp: 380-386, Organized by: The Association of Computer Electronics and Electrical Engineer (ACEEE), Chennai, INDIA. ISBN 978-93-5107-194-5.
7. Abhishek Roy, Sunil Karforma, *A Survey on digital signatures and its applications*, Journal of Computer and Information Technology Vol: 03 No: 1 & 2, August 2012 Pp- 45-69, ISSN 2229-3531.
8. Anamul Hoda, Abhishek Roy, Sunil Karforma, *Application of ECDSA for security of transaction in E-Governance*, Proceedings of Second National Conference on Computing and Systems - 2012 (NaCCS - 2012) organized by the Department of Computer Science, The University of Burdwan, March 15 - 16, 2012, 1st Edition - 2012, Pp: 281-286, ISBN 978-93-80813-18-9.
9. Sumita Sarkar, Abhishek Roy, *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, March 15 - 16, 2012, 1st Edition - 2012, Pp: 263-268, ISBN 978-93-80813-18-9.
10. Abhishek Roy, Sumita Sarkar, Joydeep Mukherjee, Arindom Mukherjee, *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, February 21 – 22, 2012, Vol: 1, Pp:153-160, ISBN 978-81-923820-0-5.
11. Abhishek Roy, Sunil Karforma, *Risk and Remedies of E-Governance Systems*, Oriental Journal of Computer Science & Technology (OJCST), Vol: 04 No:02, Dec 2011 Pp- 329-339. ISSN 0974-6471.
12. Abhishek Roy, Subhadeep Banik, Sunil Karforma, *Object Oriented Modelling of RSA Digital Signature in E-Governance Security*, International Journal of Computer Engineering and Information Technology (IJCEIT), Summer Edition 2011, Vol 26 Issue No. 01, Pp: 24-33, ISSN 0974-2034.
13. Abhishek Roy, Sunil Karforma, *A Survey on E-Governance Security*, International Journal of Computer Engineering and Computer Applications (IJCECA). Fall Edition 2011, Vol 08 Issue No. 01, Pp: 50-62, ISSN 0974-4983.
14. Abhishek Roy, Subhadeep Banik, Sunil Karforma, Jayanta Pattanayak, *Object Oriented Modeling of IDEA for E-Governance Security*, Proceedings of International Conference on Computing and Systems 2010 (ICCS 2010), November 19-20, 2010, Pp: 263-269, Organized by: Department of Computer Science, The University of Burdwan, West Bengal, INDIA. ISBN 93-80813-01-5.
15. Chayan Sur, Abhishek Roy, Subhadeep Banik, *A Study of the State of E-Governance in India*, Proceedings of National Conference on Computing and Systems 2010 (NACCS 2010), January 29, 2010, Pp: a-h, Organized by : Department of Computer Science, The University of Burdwan, West Bengal, INDIA. ISBN 8190-77417-4.

