IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 3, Issue 1, Feb-Mar, 2015
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Information Security In E-Governance: A Case Study Based Analysis

Dr. Abhishek Roy

Dept. of Comp. Sc., The University of Burdwan, Burdwan 713104, W.B, INDIA

Abstract
Information and Communication Technology (ICT) based E-Governance transaction have facilitated smart delivery of services to the doorstep of Citizen. However, the use of Internet have also enhanced the chances of infringement attempts during classified communication between Government and Citizen. To neutralize these attempts, we have proposed software cryptosystem based Citizen centric multivariate E-Governance system. During our research work, we have applied various cryptographic techniques in realistic manner to install information security during message communication. In this paper we have performed case study based analysis of our security features to explore scope for future enhancements in this field.

Keywords: *Information Security, E-Governance, Analysis.*

1. Introduction

Information and Communication Technology (ICT) based E-Governance transactions have facilitated smart delivery of services to the doorsteps of Citizen. Internet based message communication have helped Government and Citizen to communicate promptly in cost effective manner. Use of this open communication medium have also enhanced the chances of infringement attempts during these classified communication. To neutralize these attempts, we have proposed software cryptosystem based Citizen centric E-Governance system. Within our proposed E-Governance system, we have applied various cryptographic protocols in realistic manner to achieve Privacy, Integrity, Non-Repudiation and Authentication (PINA) during classified communication. However, to maintain utmost security features of our proposed E-Governance system, it should be analyzed thoroughly to find out its scope for further enhancements. To achieve this objective, we have performed case study based analysis of our proposed Citizen centric multivariate electronic smart card based E-Governance system.

In section - 2 we have discussed the objective of our proposed E-Governance system and its security features. In section - 3 we have performed the overall analysis of our proposed crypto-system. Section - 4 states the conclusion of the entire discussion. Finally, references are listed at the last part of this paper.

2. Objective.

As have already performed several literature survey **(10, 14, 16, 17, 18, 20)** here we will focus on the analysis of our proposed Citizen centric multivariate electronic smart card based E-Governance **(22, 21, 19, 15, 13, 12, 11, 9, 8, 7, 6, 5, 2, 4, 3, 1)** system to explore its future scope.

2.1 Problem Definition

In order to provide paper-less form of administration, Government is regularly launching E-Governance instruments, which is only an addition to the existing list. As a result Citizen are forced to carry multiple instruments to perform E-Governance transactions, which mostly comprises of common parameters of an individual. Simultaneously, Citizen are also forced to carry several smart cards issued by banking authorities to its account holders for financial transactions. As a result, attackers are getting wide scope to manipulate the details of an individual through these governmental and semi-governmental identities. To replace this usage of multiple smart cards and solve this problem, we have proposed a Citizen centric multivariate electronic smart card based E-Governance system, which is explained below.

2.2 Proposed E-Governance System

In Figure 1, we have shown the schematic diagram of our proposed E-Governance system. In our system we have proposed a smart card, Multipurpose Electronic Card (*MEC*), to perform all the communications between Citizen and Government through unique identification of the Citizen. The proposed system is further explained below:

i. Citizen will initiate E-Governance transaction with *MEC*.

ii. *MEC* will uniquely identify the Citizen through strong verification procedures installed within the proposed E-Governance mechanism.

iii. In case of successful verification, the Citizen is allowed the continue the transaction, else it is aborted by the E-Governance system.

iv. E-Service Server will en route the service request of the Citizen through its specific server.

v. Finally, Citizen communicate with the specific service server to complete its electronic transaction.

As this entire message communication is done through Internet, it highly susceptible to infringement attempts mounted by the adversaries. To defend those attempts we have imposed cryptographic security systems, which are discussed below.

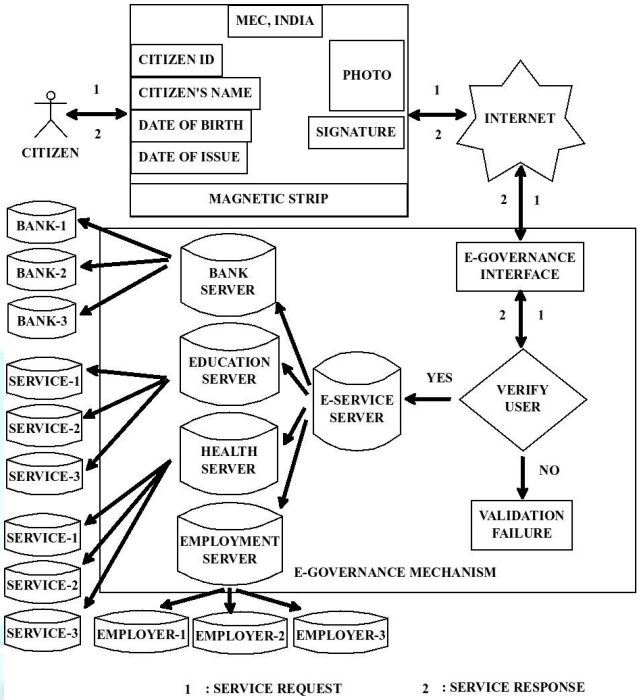

Fig. 1 Schematic diagram of proposed E-Governance system during C2G type of transaction.

2.3 Proposed Security Features

The security features of our proposed Citizen centric multivariate electronic smart card based E-Governance system is mentioned below:

i. We have imposed privacy of information through Object Oriented Modeling (OOM) of International Data Encryption Algorithm (IDEA) during G2C type of transaction.

ii. We have imposed authentication, integrity and non-repudiation of message communication using Object Oriented Modeling (OOM) of RSA Digital Signature Algorithm and Elliptic Curve Digital Signature Algorithm (ECDSA) during G2C and C2G type of transactions respectively.

iii. We have also shown the hybrid cryptosystem based user authentication through Object Oriented Modeling (OOM) of Stream Ciphers during C2G type of transaction.

iv. To understand the data flow within our proposed application, we have performed Data Modelling for Object Oriented Modeling

(OOM) of RSA Digital Signature Algorithm during G2C type of transaction.

v. To analyze the performance using dynamic metrics, we have performed the Software Metrics based analysis for Object Oriented Modeling (OOM) of RSA Digital Signature Algorithm and Elliptic Curve Digital Signature Algorithm (ECDSA) during G2C and C2G type of transactions respectively.

vi. For further enhancement of the proposed user authentication technique, we have also performed the Object Oriented Modeling (OOM) of Digital Certificates during C2G type of transactions.

As we have already discussed our proposed security features, here focus is given over its case study based analysis only

3. Analysis of Proposed Security Features

The brief analysis of our proposed security features are mentioned below:

i. Object Oriented Modeling (OOM) of International Data Encryption Algorithm (IDEA).

a. The proposed application is designed using four classes, named as *CommonFields, SecurityInterface, Sender* and *Receiver*.
b. In this application Government is represented by class *Sender*, and Citizen is represented by class *Receiver*.
c. The encryption and decryption of information is dependent over the message passing of these classes.
d. The Object Oriented Modeling (OOM) of International Data Encryption Algorithm (IDEA) is shown using Class Diagram and Sequence Diagram.
e. The implementation of this system is shown using valid message communication.

Scope for further research:

a. New classes may be introduced to expand the application of the proposed E-Governance system.
b. More Object Oriented Analysis and Design (OOAD) tools may be used for better understanding of the proposed cryptosystem.
c. As this system is applied only to denote successful message communication, it may be further tested to detect tampered message communication.
d. This application may be applied over other models of E-Governance transactions.
e. The time level efficiency of this system may be calculated further to enhance this work.

ii. Object Oriented Modeling (OOM) of RSA Digital Signature Algorithm.

a. The proposed application is designed using four classes, named as *Authentication, MEC, Government* and *Citizen*.
b. Object Oriented Modeling (OOM) of RSA Digital Signature Algorithm is shown using Class Diagram, Use Case Diagram and Inheritance Diagram.
c. The implementation of this system is shown using unaltered signature within altered message, unaltered signature within unaltered message and altered signature within unaltered message communications.

Scope for further research:

a. New classes may be introduced to expand the application of the proposed E-Governance system.
b. More Object Oriented Analysis and Design (OOAD) tools may be used for better understanding of the proposed cryptosystem.
c. This application may be applied over other models of E-Governance transactions.
d. The time level efficiency of this system may be calculated further to enhance this work.

iii. Object Oriented Modeling (OOM) of Elliptic Curve Digital Signature Algorithm (ECDSA).

a. The proposed application is designed using two classes, named as *Government* and *Citizen*.
b. Object Oriented Modeling (OOM) of Elliptic Curve Digital Signature Algorithm is shown using Class Diagram, Use Case Diagram and Sequence Diagram.
c. The implementation of this system is shown using valid signature verification and invalid or tampered signature detection.

Scope for further research:

a. New classes may be introduced to expand the application of the proposed E-Governance system.
b. Further focus may be given over the customization of Elliptic Curve Digital Signature

Algorithm (ECDSA) as per the programming requirements.

c. More Object Oriented Analysis and Design (OOAD) tools may be used for better understanding of the proposed cryptosystem.
d. This application may be applied over other models of E-Governance transactions.
e. The time level efficiency of this system may be calculated further to enhance this work.

iv. Object Oriented Modeling (OOM) of Stream Ciphers.

a. The proposed application is designed using two classes, named as *Government* and *Citizen*.
b. Object Oriented Modeling (OOM) of Stream Cipher is shown using Class Diagram and Message Passing Diagram.
c. The implementation of this system is shown using valid signature verification and invalid or tampered signature detection.

Scope for further research:

a. As an example of hybrid cryptosystem using Secret Key Cryptography (SKC) i.e Stream Cipher and Public Key Cryptography (PKC) i.e Elliptic Curve Digital Signature Algorithm, this application have wide scope of expansion for the security of transmitted information.
b. To provide more E-Services to the Citizen, new classes must be added within the application.
c. More Object Oriented Analysis and Design (OOAD) tools may be used for better understanding of the proposed cryptosystem.
d. This application may be applied over other models of E-Governance transactions.
e. The time level efficiency of this system may be calculated further to enhance this work.

v. Object Oriented Modeling (OOM) of Digital Certificates.

a. The proposed application is designed using four classes, named as *_Default, Connection, CodeClass* and *EncodeDecode*.
b. Object Oriented Modeling (OOM) of Digital Certificate is shown using Use Case Diagram and Sequence Diagram.
c. The implementation of this system is shown using encryption of messages and corresponding decryption of messages through web-based interface.

Scope for further research:

a. Apart from name and date of birth of Citizen, other attributes must be used to generate the Digital Certificate for an individual.
b. New classes may be added to provide wide range of E-Services to the Citizen.
c. More Object Oriented Analysis and Design (OOAD) tools may be used for better understanding of the proposed cryptosystem.
d. This application may be applied over other models of E-Governance transactions.
e. The time level efficiency of this system may be calculated further to enhance this work.

4. Conclusion

In this case study based analysis, the main objective was to analyze our proposed cryptosystems. As it will be an impractical approach to perform the detailed analysis all at a time, thereby taking into account all the technical aspects of our proposed cryptosystems, we have just shown the path through which further critical analysis can be conducted to provide secure and smart E-Governance services to the Citizenry.

References

[1] **Roy A**, *Synopsis on Information Security in E-Governance using Cryptography*, International Journal of Advanced Technology in Engineering and Science (IJATES), September 2014, Volume No 02 Special Issue No 01, Pp: 432-445, ISSN (Online) 2348-7550.

[2] **Roy A**, Karforma S, *Authentication of user in E-Governance : A Digital Certificate based approach*, International Journal of Scientific Research and Management (IJSRM), August 2014, Volume 2 Issue 8, Pp: 1212-1221, ISSN 2321-3418.

[3] **Roy A**, Karforma S, *E-Governance To E-Commerce : A Smart Transition*, International Journal of Emerging Research in Management and Technology (IJERMT), July 2014, Volume 3 Issue 7, Pp: 82-86, ISSN 2278-9359.

[4] **Roy A**, Karforma S, *E-Governance To E-Health : A Smart Road Map For Society*, The International Journal of Science and Technoledge (The IJST), July 2014, Volume 2 Issue 7, Pp: 217-221, ISSN 2321-919X.

[5] **Roy A**, Karforma S, *Data Modeling of a multifaceted electronic card based secure E-Governance system*, Chapter No: 12 of Book *Emerging Mobile and Web 2.0 Technologies for Connected E-Government* by Dr. Zaigham Mahmood, University of Derby, United Kingdom (UK), Published by: IGI Global, USA, Pp: 280-299, DOI: 10.4018/978-1-4666-6082-3.ch012

[6] **Roy A**, Karforma S, *Stream cipher based user authentication technique in E-Governance transactions*, International Society of Thesis Publication Journal of Research in Electrical and Electronics Engineering (ISTP-JREEE), May 2014, Volume 3 Issue 3, Pp: 31-37, ISSN 2321-2667.

[7] **Roy A**, Karforma S, *A Study on implementation of security in E-Governance using cryptography*, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), April 2014, Volume 4 Issue 4, Pp: 652-659, Print ISSN 2277 6451 Online ISSN 2277 128X.

[8] **Roy A**, Karforma S, *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.

[9] **Roy A**, Karforma S, *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.

[10] Sarkar S, **Roy A**, *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.

[11] **Roy A**, Karforma S, Banik S, *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

[12] **Roy A**, Karforma S, *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

[13] **Roy A**, Karforma S, *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.

[14] **Roy A**, Karforma S, *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.

[15] Hoda A, **Roy A**, Karforma S, *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.

[16] Sarkar S, **Roy A**, *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.

[17] **Roy A**, Sarkar S, Mukherjee J, Mukherjee A, *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.

[18] **Roy A**, Karforma S, *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.

[19] **Roy A**, Banik S, Karforma S, *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.

[20] **Roy A**, Karforma S, *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.

[21] **Roy A**, Banik S, Karforma S, Pattanayak J, *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.

[22] Sur C, **Roy A**, Banik S, *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.