SYNOPSIS ON INFORMATION SECURITY IN E-GOVERNANCE USING CRYPTOGRAPHY

Abhishek Roy
Research Scholar, Dept. of Comp. Sc., The University of Burdwan, Burdwan 713104, W.B, India.

ABSTRACT

Advancement of Information and Communication Technology (ICT) have explored wide scope for prompt delivery of electronic services in cost effective manner. For socio-economic development of the state, especially the Governments of developing countries may use it to provide good governance to its populace. As the entire message communication during Electronic Governance i.e E-Governance is conducted through public communication channel i.e Internet, it is highly susceptible to interceptions of the adversaries. To prevent these interceptions, strong cryptographic security protocols must be deployed during E-Governance transactions. In this paper we intend to present a synopsis of our research work conducted to achieve this objective.

Keywords : *Cryptography, E-Governance, E-Services, Information Security, Synopsis.*

1. INTRODUCTION.

In the present days of global economic meltdown government from developing countries are facing severe challenge in maintaining an efficient administration within an affordable budget. The Governments may use the advantages of Information and Communication Technology (ICT) to provide good governance to its populace for the overall socio-economic development of the state. As the entire message communication during Electronic Governance i.e E-Governance is conducted through public communication channel i.e Internet, it is highly susceptible to interceptions of the adversaries. In order to maintain the consistency of these systems, message communication should be conducted using encryption and decryption algorithms of Cryptography, which is the art and science of keeping the messages secret from the unauthorized access. The practitioners of this branch of science are known as the Cryptographers. Using this techniques, the cryptographers can encrypt the plain text into its corresponding cipher text using cryptographic algorithm. Simultaneously, the cipher text can also be decrypted to retrieve its corresponding plain text using specific algorithm. The entire process of encryption and decryption of the plain text is done based on specific parameter called Key, which is a specific sequence of bits known only to the valid sender and receiver of the message. In this method, the valid sender can encrypt the plain text using this key, and send the encrypted message through the Internet. Simultaneously, the valid receiver of the message will receive the encrypted message and decrypt it using the selected key to retrieve the plain text. It is just like transfer of precious item publicly from the sender to its receiver under a lock and key system. If this encryption and decryption of message is done using a single key i.e Secret Key, then it is called Secret Key Cryptography (SKC) and if it is done using a pair of keys, i.e Public Key and Private Key, then is is called

as Public Key Cryptography (PKC). In case of Secret Key Cryptography (SKC), as the entire operation is performed using a single key, the success of the cryptosystem is solely dependent on its secrecy. Any Secret Key Cryptography (SKC) based cryptosystem is assumed to be compromised if its Secret Key is divulged by some means. In case of Public Key Cryptography (PKC), the Private Key is known only to a specific participant whereas the Public Key is available publicly. The speciality of the Public Key is that it does not compromise the security of the algorithms and hence it can be easily distributed online. Thus, a shared secret is established between the participants by exchanging only Public Keys. Any other entity having access only over the public information, will be unable to calculate the shared secret unless it have access to the respective Private Key of the communicating parties. The Private Key and Public Key of a cryptosystem are interlinked to each other with the help of One-Way mathematical functions, where forward operation is easily possible but the reverse operation is almost impossible. In this cryptosystem, the forward operation of the one-way mathematical function is performed using the Private Key to obtain the Public Key. Any Public Key Cryptography (PKC) based cryptosystem is assumed to be compromised if Private Key can be retrieved easily from the Public Key by performing the reverse operation of the one-way functions. In this paper we intend to present a synopsis of our research work conducted to achieve information security using Cryptography during E-Governance transactions.

To defend the consistency of E-Governance system from the adversaries, its various risk factors are discussed in Section – 2 of this synopsis. To provide Citizen centric multivariate electronic smart card based governance, in Section – 3 we have proposed our E-Governance system. Conclusion drawn from the entire discussion in mentioned in Section – 4 of this synopsis. References at listed at the last part of this article.

2. RISK AND REMEDIES OF E-GOVERNANCE SYSTEM.

Being an electronic system, the entire message communication among the participants of E-Governance are carried out using the publicly available Information and Communication Technology (ICT) based communication medium i.e Internet. That means all the classified information that are communicated in off line mode, will now be communicated using digital medium. Thus the network security related issues becomes the prime concern of the researchers, as they need to depend solely over such a communication channel which is highly vulnerable to the security infringement attempts made by the eavesdropper. Initially, the objective of the researchers should be to design the blue-print of an electronic system which will be free from all security threats.

2.1 RISK FACTORS OF E-GOVERNANCE SYSTEM.

The security threats of E-Governance system may be broadly categorized into two categories :

1. Active Attacks - The attacks which hampers the E-Governance system directly.
2. Passive Attacks - The attacks which hampers the E-Governance system indirectly.

The *modus operandi* of the above mentioned active and passive attacks may be further stated as below :

1. Eavesdropper or Intruder may attack and infiltrate the electronic system and thereby escalate its privileges to tampers its authorized operations.
2. Intruder may attack and compromise the communication channel of the electronic system which is mainly dependent on the Internet.
3. Intruder may pretend itself as the authenticated user and sabotage the electronic system.
4. Intruder may pretend itself as the authorized electronic system and continue the transactions keeping its authorized users completely unaware about the actual scenario.
5. intruder may infiltrate the electronic system just to listen the communication and use it for illegal or unauthorized operations.

Though there are no concrete remedies of these threats, yet there are some probable remedies which are discussed in the following sub – section.

2.2 PROBABLE REMEDIES.

Since E-Governance transaction takes place through Internet, deployment of network security parameters for covering these security pitfalls become an prime factor of research works. Various cryptographic algorithms like Digital Signature, Digital Certificate, Elliptic Curve Cryptosystem (ECC), Digital Certificate, etc are already available for defending these security pitfalls. To achieve this objective of Citizen centric E-Governance in a realistic manner, application of these standard cryptographic techniques must be combined with object oriented techniques. To reduce the above mentioned risk factors, the Citizen centric efficient E-Governance system must achieve the following objectives :

1. The efficient E-Governance system must successfully replace the present conventional form of governance.
2. It must bring efficiency through accuracy, timeliness within the various public and private service sectors of the society.
3. It must identify the Citizen as a whole using a single digitized identification number.
4. Government should be able to communicate with the Citizen directly for various governmental transactions using this electronic system.
5. Citizen must be able to access various facilities provided by the Government using that efficient electronic system.
6. Government should be able to collect customized information about the Citizen at various levels of administration.
7. Citizen must be able to perform all the financial transactions, thereby replacing the existing smart cards issued by the banks.
8. Moreover it should be technically sound enough to beef-up the national integrity by tracking the intruders during various public and private sector services.
9. Finally, the state should use this electronic system to deploy efficient governance over its core and allied areas for maximum benefit using less resources and manpower.

During our research work we have tried to achieve these features by proposing a Citizen centric multivariate electronic smart card based E-Governance system.

3. PROPOSED E-GOVERNANCE SYSTEM.

To design an efficient E-Governance system in India, we need to understand the requirements of the Citizen as they will be the ultimate end-users and beneficiaries of the proposed system. Here Citizen have to carry multiple instruments either issued by the Government or by the governmental agencies, like Bank, etc, to perform various transactions. All of these instruments claim to uniquely identify the Citizen during transactions, which mostly comprises of common parameters of an individual with slight alterations. For better understanding of the problem we can 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. Things become more confusing when it reveals that though Aadhaar Card comprises of biometric parameter of an individual, yet it is incapable of all E-Governance 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, etc for the same purpose. Furthermore to digitize the conventional ration system, the government is 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 locate an individual as a whole with a single identification number. 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 adding to the count with the existing identification numbers of the individual with non so far having the provision for complete electronic transactions. To find solution to this problem, during our research work we have proposed a Citizen centric multivariate electronic smart card (i.e Multipurpose Electronic Card (MEC) based E-Governance system, whose conceptual diagram is shown in Figure – 1.

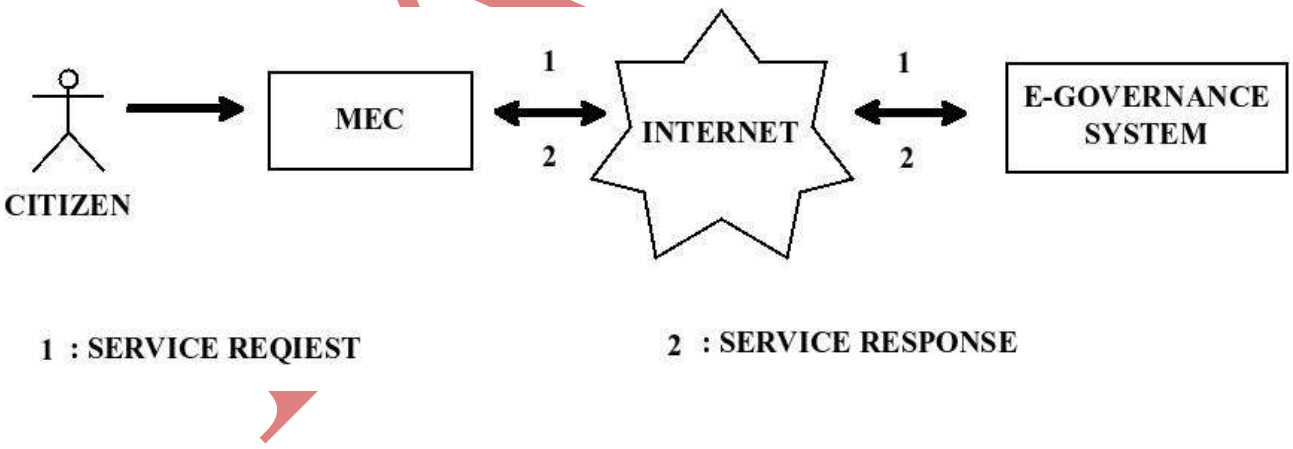

Figure 1 : Conceptual diagram of proposed E-Governance system.

Figure – 1 shows that the Citizen is performing Citizen to Government (C2G) type of E-Governance transactions using the proposed Multipurpose Electronic Card (MEC). The block diagram of the proposed smart card is shown in Figure – 2.

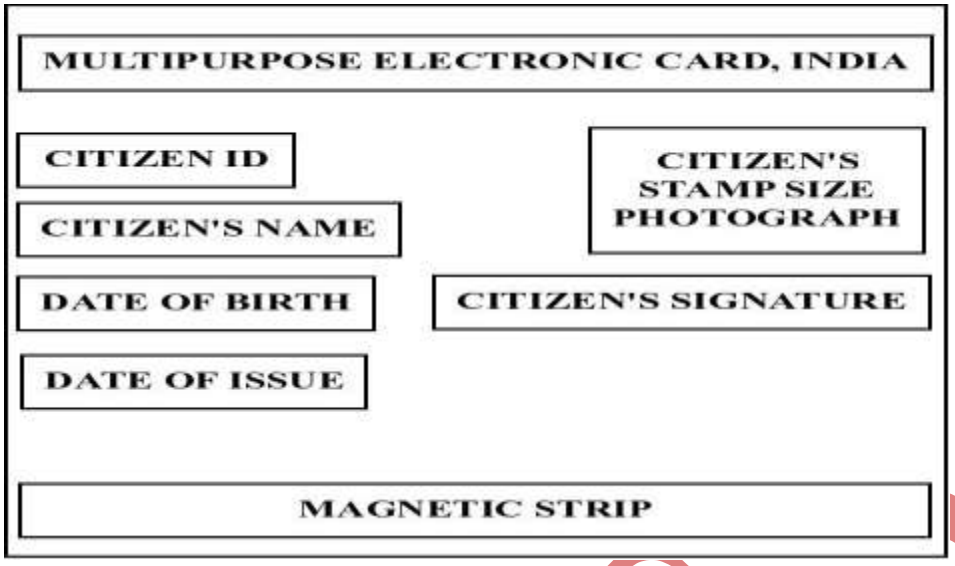

Figure 2 : Block diagram of proposed smart card.

Figure – 2 shows the block diagram of the proposed smart card, using which Citizen will perform all type of E-Governance transactions. Since this multivariate smart card will become the main interface for the message communication between the Government and the Citizen, it must contain security parameters installed within its architecture for the privacy of the classified information. So, the 3-tier secured architecture of the proposed E-Governance system is shown in Figure – 3.

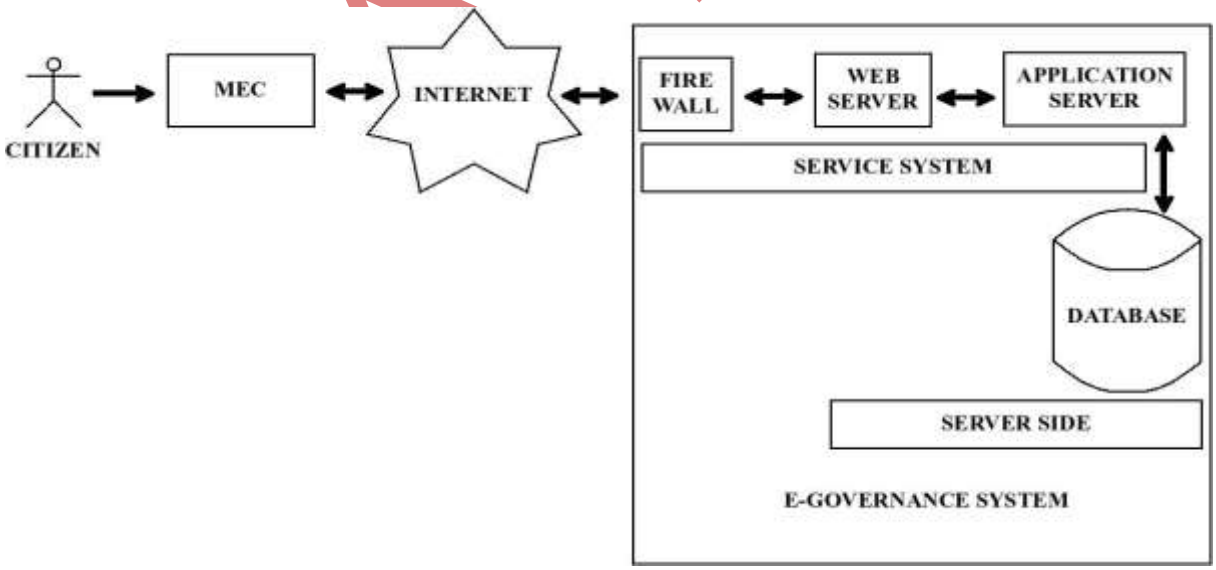

Figure 3 : 3-tier architecture of proposed E-Governance system.

Figure – 3 shows the 3-tier architecture of the proposed E-Governance system, where Citizen denotes the first tier,

Service System denotes the second tier and Server Side denotes the third tier of system. This architecture may be further explained as below –

a. The Citizen will communicate with the Government with the Multipurpose Electronic Card (MEC).

b. This electronic instrument will further interact with the E-Governance system through Internet.

c. The Electronic system will contain the following segments for handling the sensitive data in a secured manner –

i. Firewall – Firewall will prevent the entry of spam ware, malware and other malicious elements within the system. This will act as the strong guard which will perform the database management very securely.

ii. Web server – After passing through the Firewall the data enter the Web Server of the electronic system. Here the alteration of the data will be performed as per the requirement of the transaction. Here various web based technologies will be installed with the web server for the smooth progress of the operation.

iii. Application server – In the next phase the data will perform the necessary interaction with the Application Server of the system.

iv. Database – Finally the resultant data set of these entire operations will be stored in the database for further reference. Hence, it is very clear that huge load will be mounted on this database as it will be containing all the vital information of the citizenry so that governmental agencies can access them instantly. We have shown this database using a single database structure just to get a simple view of the complex structure. However in practical scenario the distributed database management system will be exercised in this phase to avoid the database server failure.

d. The Service System of the proposed E-Governance system comprises of the Firewall, Web Server and the Application Server.

e. The Server side comprises of the Web Server, Application Server and the Database storage.

f. The entire data transmission through this system will proceed in bidirectional manner which includes request from the Citizen and its corresponding reply from the Government.

Figure – 3 also indicates that for successful execution of the proposed smart card based E-Governance system, the identity of the user must be verified carefully so that unauthorized users are not allowed to fulfill their ill-intentions. For this reason we have concentrated our research work over the authentication of the user using complex cryptographic algorithms like RSA, Elliptic Curve Digital Signature Algorithm (ECDSA), etc blended with object oriented software engineering. The objective achieved so far to propose our secured E-Governance system, is stated below –

1. We have studied the state of E-Governance **[21]** in Indian scenario.
2. We have studied the security features of E-Governance **[19]** system.
3. We have discussed the various risk factors and their probable remedies for E-Governance **[17]** transaction.
4. We have performed extensive literature survey on Digital Signatures **[13]** and its applications.
5. Based on these studies, we have proposed our Citizen centric multivariate electronic smart card based E-Governance system. To impose privacy of information, we have also performed Object Oriented Modeling (OOM) of International Data Encryption Algorithm (IDEA) **[20]** during Government-to-Citizen (G2C) type of E-Governance transaction. Since encryption and decryption of entire message incurs huge budget expense of our proposed E-Governance system, further we have focused on authentication of user through the application of various Digital Signature Algorithms.
6. To impose other security features like authentication, integrity, non repudiation, etc, we have performed Object

Oriented Modelling (OOM) of RSA Digital Signature Algorithm **[18]** and Elliptic Curve Digital Signature Algorithm (ECDSA) **[10, 11, 14]** during Government-to-Citizen (G2C) and Citizen-to-Government (C2G) type of proposed E-Governance transactions respectively. To further enhance the user authentication technique of proposed system, we have designed hybrid cryptosystem through Object Oriented Modelling (OOM) of Stream Ciphers **[5]** during Citizen-to-Government (C2G) type of transaction. In this hybrid cryptosystem we have performed encryption of plain text using Stream Ciphers and generation of digital signature using Elliptic Curve Digital Signature Algorithm (ECDSA).

7. We have modelled our RSA Digital Signature Algorithm **[4]** based cryptosystem during Government-to-Citizen (G2C) type of transaction, mainly to analyze its dynamic aspects using Software Metrics **[7, 8]** .
8. We have tried to build trust based relations between Government and Citizen through Object Oriented Modelling (OOM) of Digital Certificates **[1, 12]** . The Unified Modeling Language (UML) based explanation of our proposed cryptosystem is discussed further in this synopsis.
9. Finally, using our proposed E-Governance **[6]** system we have explored the scope of interdisciplinary research work in E-Commerce **[2]**, E-Health **[3]**, etc, using strict user authentication techniques like Biometric **[9, 15, 16]** applications.

Hence, schematic diagram of our proposed E-Governance system is shown in Figure – 4.

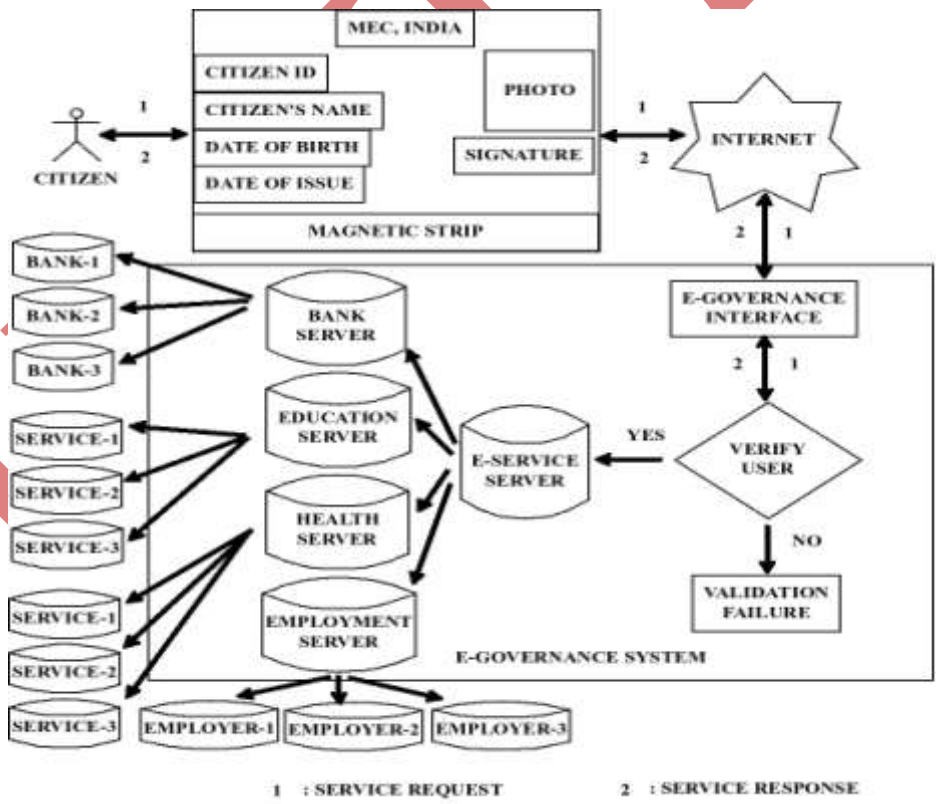

Figure 4 : Schematic diagram of proposed E-Governance system

Figure – 4 shows the schematic diagram of our proposed E-Governance system during Citizen to Government (C2G) transaction. The Digital Certificate **[1, 12]** based application of our proposed system is further explained below :

Step 1 – Citizen initiates the E-Governance transaction using Multipurpose Electronic Card (MEC).

Step 2 – The Trusted Third Party (TTP) i.e the Certificate Authority (CA) generates the Identity Certificate and the Authorization Certificate using the unique ID / Citizen ID of the MEC.

Step 3 – MEC connects to the E-Governance system using the ICT i.e Internet.

Step 4 – E-Governance system initiates validation procedure for the digital certificates used by the Citizen.

Step 4.1 – In case of successful validation, the Citizen access the E-Service server for completion of its transaction and proceeds to Step 5.

Step 4.2 – In case of unsuccessful validation the Citizen fails to access the services and receives a negative acknowledgement via same route.

Step 5 – The E-Governance transaction terminates.

The role of Citizen and the Government in this proposed Citizen-to-Government (C2G) type of E-Governance system is shown through Use Case Diagram in Figure – 5.

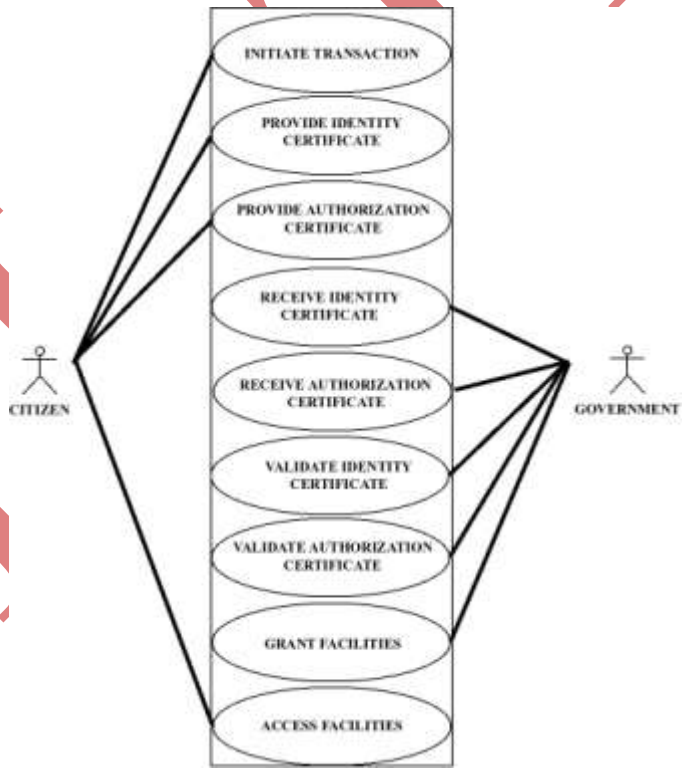

Figure 5 : Use Case Diagram in Citizen-to-Government (C2G) type of E-Governance transaction.

Figure – 5 displays the Use Case Diagram of the proposed E-Governance model in Citizen to Government (C2G) type of transactions whose step-wise explanation is as follows :

U1: INITIATE TRANSACTION – Here the Citizen initiates the E-Governance transaction using the Multipurpose Electronic Card (MEC) for accessing the electronic facilities.

Scenario 1: Mainline sequence.

1 – Citizen initiates the E-Governance transaction.

2 – Internet communicates with the E-Governance system.

3 – E-Governance system gets ready to accept further inputs from the Citizen.

U2: PROVIDE IDENTITY CERTIFICATE – Here the Citizen provides its Identity certificate to the E-Governance system.

Scenario 1: Mainline sequence.

1 – Citizen uses the Multipurpose Electronic Card (MEC) to produce its identity certificate electronically.

2 – Internet communicates the identity certificate of the Citizen to the E-Governance system.

U3: PROVIDE AUTHORIZATION CERTIFICATE – Here the Citizen provides its Authorization certificate to the E-Governance system.

Scenario 1: Mainline sequence.

1 – Citizen uses the Multipurpose Electronic Card (MEC) to produce its authorization certificate electronically.

2 – Internet communicates the authorization certificate of the Citizen to the E-Governance system.

U4: RECEIVE IDENTITY CERTIFICATE – Here the E-Governance system receives the identity certificate of the Citizen.

Scenario 1: Mainline sequence.

1 – E-Governance system communicates with the Internet.

2 – E-Governance system receives the identity certificate of the Citizen.

U5: RECEIVE AUTHORIZATION CERTIFICATE – Here the E-Governance system receives the authorization certificate of the Citizen.

Scenario 1: Mainline sequence.

1 – E-Governance system communicates with the Internet.

2 – E-Governance system receives the authorization certificate of the Citizen.

U6: VALIDATE IDENTITY CERTIFICATE – Here the E-Governance system validates the identity certificate of the Citizen.

Scenario 1: Mainline sequence.

1 – The system matches the identity certificate accepted from the Citizen with its counterpart stored in the E-Governance server.

Scenario 2: At step-1 of mainline sequence.

1 – If match is found the transaction proceeds further.

Scenario 3: At step-1 of mainline sequence

1 – If match is not found the transaction terminates unsuccessfully.

2 – Citizen is notified about the unsuccessful termination of the E-Governance transaction.

U7: VALIDATE AUTHORIZATION CERTIFICATE – Here the E-Governance system validates the authorization

certificate of the Citizen.

Scenario 1: Mainline sequence.

1 – The system matches the authorization certificate accepted from the Citizen with its counterpart stored in the E-Governance server.

Scenario 2: At step-1 of mainline sequence.

1 – In case the match is found, the transaction proceeds further.

Scenario 3: At step-1 of mainline sequence.

1 – In case the match is not found, the transaction terminates unsuccessfully.

2 – Citizen is notified about the unsuccessful termination of the E-Governance transaction.

U8: GRANT FACILITIES – Here the E-Governance system grants permission to access the electronic facilities to the Citizen.

Scenario 1: Mainline sequence.

1 – E-Governance system communicates with the Internet.

2 – E-Governance system grants access permissions to the Citizen.

3 – Internet communicates with the Citizen via Multipurpose Electronic Card (MEC) to convey the access permissions.

U9: ACCESS FACILITIES – Here the Citizen accesses the permitted facilities.

Scenario 1: Mainline sequence.

1 – Citizen becomes online using Multipurpose Electronic Card (MEC).

2 – Internet communicates with the E-Governance system.

3 – Citizen accesses the permitted facilities from the E-Governance system.

4 – Citizen disconnects communication with the E-Governance system after the successful transaction.

The Sequence Diagram of the proposed Digital Certificate based cryptosystem *w.r.t* time frame in shown in Figure – 6.

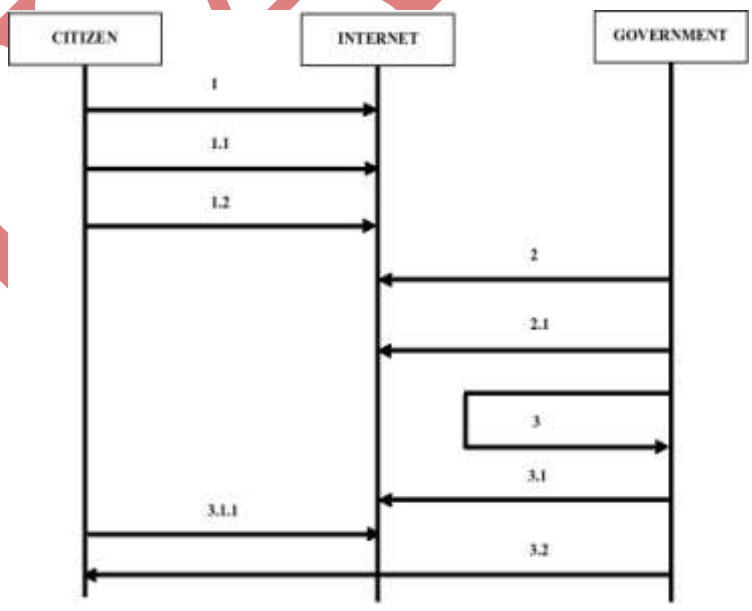

Figure 6 : Sequence Diagram in Citizen-to-Government (C2G) type of E-Governance pattern.

Figure – 6 displays the message communication among the Citizen and the Government with reference to time frame whose step-wise explanation is as follows :

1 – Citizen initiates the particular E-Governance transaction.

1.1 – Citizen provides its Identity Certificate to establish its identity during the electronic transactions.

1.2 – Citizen provides its Authorization Certificate to access its facilities during the electronic transactions.

2 – Government receives the Identity Certificate used by the Citizen.

2.1– Government receives the Authorization Certificate used by the Citizen.

3 – Government initiates the validation procedure for the used certificates of the Citizen.

3.1 – In case of successful validation, the Citizen is allowed to access the electronic facilities.

3.1.1 – Citizen accesses the electronic facilities.

3.2 – In case of unsuccessful validation, the Citizen is not allowed to access the electronic facilities with proper notification.

Since the successful implementation of this proposed Citizen centric multivariate electronic smart card based E-Governance system is beyond the scope of an individual, only the conclusion drawn from the entire discussion is stated further in this synopsis.

4. CONCLUSION.

During our research work we have studied the application of information security using various cryptographic algorithms in E-Governance system. For that purpose initially we have studied various security aspects of E-Governance **[13, 19, 21]** system to locate its risks **[17]** factors. To provide Citizen centric efficient governance system, we have proposed Multipurpose Electronic Card based E-Governance **[20]** system and imposed its privacy of information using Object Oriented Modelling of International Data Encryption Algorithm (IDEA). We have imposed other security features like authentication, integrity and non-repudiation using Object Oriented Modelling of RSA Digital Signature Algorithm **[18]**, Elliptic Curve Digital Signature Algorithm (ECDSA) **[10, 11, 14]**, Stream Ciphers **[5]**, Digital Certificates **[1, 12]**, etc. We have also modelled our E-Governance system using RSA Digital Signature Algorithm **[4]** during Government-to-Citizen (G2C) type of transaction to analyze its dynamic aspects using Software Metrics **[7, 8]**. Finally to give new dimension to our research work we have used the proposed E-Governance **[6]** system to explore scope of interdisciplinary research work in E-Commerce **[2]**, E-Health **[3]**, etc, applying strict user authentication techniques like Biometric **[9, 15, 16]** applications.

5. REFERENCES

[1]. **Abhishek Roy**, Sunil Karforma, *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.

[2]. **Abhishek Roy**, Sunil Karforma, *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.

[3]. **Abhishek Roy**, Sunil Karforma, *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.

[4]. **Abhishek Roy**, Sunil Karforma, *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

[5]. **Abhishek Roy**, Sunil Karforma, *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.

[6]. **Abhishek Roy**, Sunil Karforma, *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.

[7]. **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.

[8]. **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.

[9]. 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.

[10]. **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

[11]. **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

[12]. **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.

[13]. **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.

[14]. 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.

[15]. 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.

[16]. **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.

[17]. **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.

[18]. **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.

[19]. **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.

[20]. **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.

[21]. 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.