UML BASED MODELING OF ECDSA FOR SECURED AND SMART E-GOVERNANCE SYSTEM

Abhishek Roy [1] and Sunil Karforma [2]

[1] Department of Computer Science, The University of Burdwan, W.B, INDIA.
Department of Computer Application, Durgapur Society of
Management Science, W.B, INDIA.
abhishek.roy@aol.in
[2] Dept. Of Computer Science, The Univeristy of Burdwan, W.B, INDIA.
dr.sunilkarforma@gmail.com

ABSTRACT

In comparison to the conventional form of administration, nowadays the E-Governance have become the smart way of deployment of administration by the authority under its jurisdiction. Since this technique requires the transmission of sensitive information between the Government and the Citizen through the Internet, information scientists take pain to provide utmost information security, which can also be further qualitatively enhanced by the incorporation of object oriented software engineering paradigm. Hence, the authors have proposed a multifaceted smart card based secured E-Governance mechanism using Multipurpose Electronic Card (MEC). In this proposed model the authentication of Citizen is achieved by the tactful implementation of digital signatures, which is the key field of digital certificate. Security of digital signature is further improved by wrapping Elliptic Curve Digital Signature Algorithm (ECDSA) in different Object Oriented Analysis Design (OOAD) tools of Unified Modeling Language (UML).

KEYWORDS

Object Oriented Paradigm, Authentication, Integrity, E-Governance

1. INTRODUCTION

In comparison to the conventional form of administration, nowadays the E-Governance [1,2,3,5,6,7,9,10, 17, 18] have become the smart way of deployment of administration by the authority under its jurisdiction. Since this technique requires the transmission of sensitive information between the Government and the Citizen through the Internet, information scientists take pain to provide utmost information security, which can also be further qualitatively enhanced by the incorporation of object oriented software engineering paradigm. Hence, the authors have proposed a multifaceted smart card based secured E-Governance mechanism using Multipurpose Electronic Card (MEC). In this proposed model the authentication [8] of Citizen is achieved by the tactful implementation of digital signatures [4], which is the key field of digital certificates. Security of digital signature is further improved by wrapping Elliptic Curve Digital Signature Algorithm (ECDSA) in different Object Oriented Analysis and Design (OOAD) [11] tools of Unified Modeling Language (UML) [12]. Apart from strength-per-key-bit feature of Elliptic Curve Cryptography (ECC), to obtain high processing power, storage space, bandwidth and power consumption efficiency, Elliptic Curve Digital Signature Algorithm (ECDSA) [14] is used

Rupak Bhattacharyya et al. (Eds) : ACER 2013,
pp. 207–222, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3219

instead of Digital Signature Algorithm (DSA) in this proposed model. Unified Modeling Language (UML) have become the de-facto standard for the development of real world oriented or object oriented security systems. Unified Modeling Language (UML) is not a specific methodology, rather it is collection of several types of diagrams when used within any specific methodology, it helps to increase the acceptability of the system to its user. The Unified Modeling Language (UML) contains specialized diagrams and these diagrams uses the standardized symbols for depicting the proposed software system model in object oriented perspective. Though UML can be explained with wider perspective, here we have focused over the Unified Modeling Diagrams (UML) diagrams for the better description of the proposed smart card based E-Governance mechanism using Multipurpose Electronic Card (MEC). The standardized Unified Modeling Language (UML) diagrams depicted below are – Use case Diagram, Class Diagram, Sequence Diagram, State chart Diagram and Activity Diagram. With the extensive use of these Unified Modeling Diagrams (UML) tools various C2G type of E-Governance transactions using Multipurpose Electronic Card (MEC), like online payment of Income Tax, Telephone Bill, House Rent, ATM facility, etc are explained clearly.

Section – 2 discusses the background of Elliptic Curve Digital Signature Algorithm (ECDSA) in the context of C2G type of E-Governance transactions using Multipurpose Electronic Card (MEC). In the section – 3 the precise literature review is presented in tabular form. In the section – 4 the authors have presented the block diagram of the Multipurpose Electronic Card (MEC), the schematic diagram of C2G type of E-Governance model using MEC and its explanation in the context of object oriented software engineering. Finally, the section – 5 draws the conclusion from the above discussions. References are cited in section – 6.

2. ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA)

ECDSA [15, 16] is applied on C2G model of E-Governance for electronic identification of Citizen during these transactions with the Government –

To sign a message m, Citizen performs the following steps for ECDSA key generation:

Step 1 – Selects an Elliptic curve E defined over Z. The number of points in E(Z) should be divisible by a large prime number n.
Step 2 – Select a point $P \in E(Z_p)$ of order n.
Step 3 – Select a statistically unique and unpredictable integer d in the interval [1, n-1].
Step 4 – Compute Q = dP.
Step 5 – The Public key of Citizen is (E,P,n,Q) and the private key is d.
To sign a message m, the Citizen performs the following steps for ECDSA signature generation:
Step 1 – Select a statistically unique and unpredictable integer k in the interval [1, n-1].
Step 2 – Compute kP = (x,y) and r = x mod n. (Here *x* is regarded as an integer, for example by conversion from its binary representation.) If r = 0 then go to Step – 1.
Step 3 – Compute k^{-1} mod n.
Step 4 – Compute $s = k^{-1} \{h(m) + dr\}$ mod n, where h is the Secure Hash Algorithm (SHA-1).
Step 5 – If s = 0, then go to Step – 1.
Step 6 – The Citizen's signature for the message m is the pair of integers (r,s).

To verify the Citizen's signature (r,s) over message m, the Government performs the following steps for ECDSA signature verification:

Step 1 – Obtain an authenticate copy of public key (E,P,n,Q) of the Citizen. Verify that r and s are integers in the interval [1, n-1].
Step 2 – Compute $w = s^{-1}$ mod n and h(m).

Step 3 – Compute $u_1 = h(m)\ w \bmod n$ and $u_2 = rw \bmod n$.
Step 4 – Compute $u_1P + u_2Q = (x_0, y_0)$ and $v = x_0 \bmod n$.
Step 5 – The signature is valid if and only if v = r, else the signature is declared as invalid.

3. LITERATURE REVIEW

The relevant literature review for implementation of authentication of the sensitive information which is transmitted during various E-Governance transactions is mentioned precisely in the tabular form –

Sl. no	Paper Title	Description
1	Design and implementation of an ECDSA-based identity authentication protocol on WSN [19].	In this paper the authors have proposed an identity based protocol using Elliptic Curve Digital Signature Algorithm (ECDSA) for deployment of authentication in Wireless Sensor Network (WSN). The authors have also claimed that this protocol can prevent the imitation of the enemy node under the passive attack, authenticate KAC (Key Assign Centre) and effectively avoid the attack of masquerading.
2	A Comparative Analysis of Signature Schemes in A New Approach to Variant on ECDSA [20].	In this paper the authors have studied various digital signature schemes and have extended this signature schemes to a Variant Scheme level of ECDSA which will produce the high level of security with the help of the parameters.
3	An Identity Based Digital Signature from ECDSA [21].	In this paper the authors have proposed an identity based digital signature protocol using ECDSA to achieve computational efficiency when compared to other identity based signature protocols.
4	Secure and Efficient Generalized Signcryption Scheme Based on a Short ECDSA [22].	In this paper the authors have proposed a secure and efficient generalized signcryption scheme based on short ECDSA. The authors have claimed that this scheme is more efficient in terms of cost and computation compared to Elliptic Curve Generalized Signcryption Scheme (ECGSC).
5	Accelerated Verification of ECDSA Signatures [23, 24]	In this paper the authors have proposed a accelerated method for verification of ECDSA signatures which is claimed to be 40% more efficient with no added implementation complexities compared to the standard verification methods of ECDSA digital signature. They have also claimed that this method can also be used for accelerated verification of other ElGamal – like signature algorithms, including DSA.
6	A Software Implementation of ECDSA on a Java Smart Card [25]	In this thesis report the author have presented the comprehensive description of the proposed prototype implementation of ECDSA to JAVA capable smart card environment.
7	Decentralized Authorization with ECDSA on a JAVA Smart Card – A Software Implementation [26]	In this paper the authors have presented a typical implementation of smart cards as the authorization tokens using ECDSA based public key cryptography.

8	Low complexity smart card-based physical access control system over IP networks [27]	In this paper the authors have presented a low complexity and low cost system to control the physical access to dependencies, provided that an IP intranet exists. This system is based on very simple smart cards and a central server allowing high flexibility of permission management. The proposed protocol is specifically designed to access the server securely via IP in order to authenticate the user/smart card. The authors have finally claimed that the presented protocol is also capable to detect the cloned cards.
9	Digital signature systems based on smart card and fingerprint feature [28]	In this paper the authors have proposed two signature systems based on smart cards and fingerprint features. In one signature system, the cryptographic key is stored in the smart card and is only accessible when the signer's extracted fingerprint features match his stored template. To resist being tampered on public channel, the user's message and the signed message are encrypted by the signer's public key and the user's public key, respectively. In the other signature system, the keys are generated by combining the signer's fingerprint features, check bits, and a rememberable key, and there are no matching process and keys stored on the smart card. Additionally, there is generally more than one public key in this system, that is, there exist some pseudo public keys except a real one.
10	Smart card initiative for South African E-Governance - A study [29]	In this paper the authors have presented a free and open source smart card based platform which is independent of card terminal vendor. This accelerates the smart card usage as the lack of vendor independence have been a barrier to smart card adoption. The thesis also proves the feasibility of integrating free and open source technologies in enhancing E-Government in the context of South Africa. This is important because adopting free and open source software allows African government the opportunity to roll out online government services at lesser costs and be in full control of localization and adaptation.
11	Digital Identities and the Promise of the Technology Trio: PKI, Smart Cards, and Biometrics [30]	In this paper the authors have dealt with the evolving crimes of the digital age i.e identity theft. As per this proposed technique the combination of biometrics, smart cards and PKI may be used to design a robust and trusted identification and authentication infrastructure. The article concludes that such infrastructure may provide the foundation for secured electronic transactions as it addresses the need for strong user authentication of virtual identities.

12	A New Remote User Authentication Scheme Using Smart Cards [31]	In this paper the authors have proposed a new remote user authentication scheme using smart cards. This techqniue is mainly dependent on the ElGamal's public key cryptosystem. In this paper the authors have claimed that the system does not require the password table to verify the legitimacy of the login users. Moreover this scheme is claimed to withstand the message replaying attack.
13	Efficient remote user authentication scheme using smart card [32]	In this paper the authors have proposed a new remote user authentication scheme using smart cards. The primary features of this proposed scheme are – [i] that it does not require any verification tables in the remote server and, [ii] only one hash function computation and one modular multiplication are computed in the smart card. Hence, the authors have claimed that their proposed scheme is more efficient comapred to other schemes.

4. PROPOSED MODEL

In this section the authors have presented the block diagram of the Multipurpose Electronic Card (MEC), the schematic diagram of C2G type of E-Governance model using MEC and its description in object oriented paradigm which demonstrates the implementation of ECDSA in case of valid signatures as well as invalid signatures in this model.

The block diagram of the proposed Multipurpose Electronic Card (MEC) is as follows -

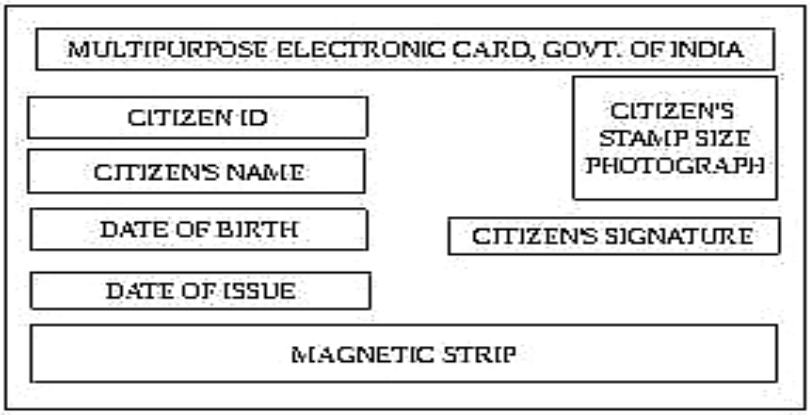


Fig 1 – Block diagram of the Multipurpose Electronic Card (MEC)

The proposed E-Governance model using this above mentioned Multipurpose Electronic Card (MEC) in Citizen to Government pattern is as follows –

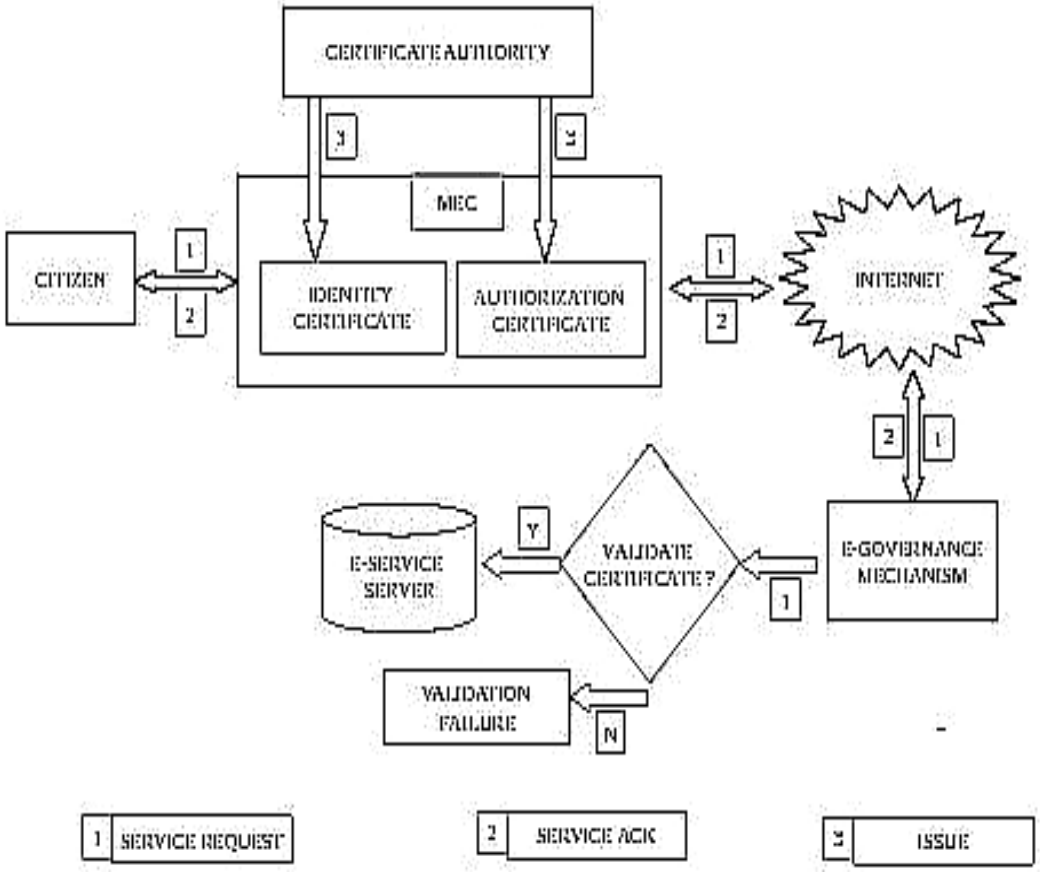


Fig 2 – Schematic diagram of proposed secured and smart C2G type of E-Governance model using MEC.

The algorithmic description of the above mentioned system is as follows –

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 of the Multipurpose Electronic Card (MEC).

Step 3: Multipurpose Electronic Card (MEC) connects to the E-Governance mechanism using the publicly available data transmission medium i.e Internet.

Step 4: E-Governance mechanism initiates validation procedure for the digital certificates used by the Citizen. This process checks both the identity and the access permission of the electronic services available to the Citizen.

Step 5: In case of successful validation, the Citizen access the E-Service server and proceeds to Step 8 for successful completion of the E-Governance transaction.

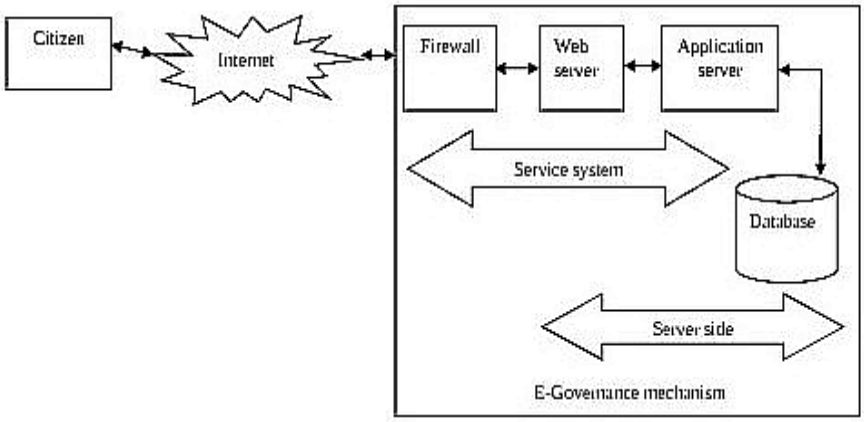
Step 6: The Citizen fails to access the E-Service server due to authentication failure.

Step 7: A negative acknowledgement is send to the Citizen via same route.

Step 8: The E-Governance transaction terminates.

The typical 3-tier architecture for supporting the proposed E-Governance mechanism is mentioned below –

Fig 3 – Three tier architecture of the proposed C2G type of smart E-Governance model.



Object oriented approach of the proposed system in terms of digital signature generation as well as verification between the Citizen and the Government is explained with the help of following primary Object Oriented Analysis and Design (OOAD) tools available in Unified Modeling Language (UML) –

Use Case Diagram, Class Diagram, Sequence Diagram, State chart Diagram and Activity diagram.

4.1 Use Case Diagram

As the primary responsibility, the Use case diagram is typically used to communicate the high-level functions of the system. The following diagram clearly depicts the main function of the Citizen is to access the E-Governance services like online payment of Income Tax, Telephone Bill, House Rent, ATM facility, etc which are being granted by the Government after proper

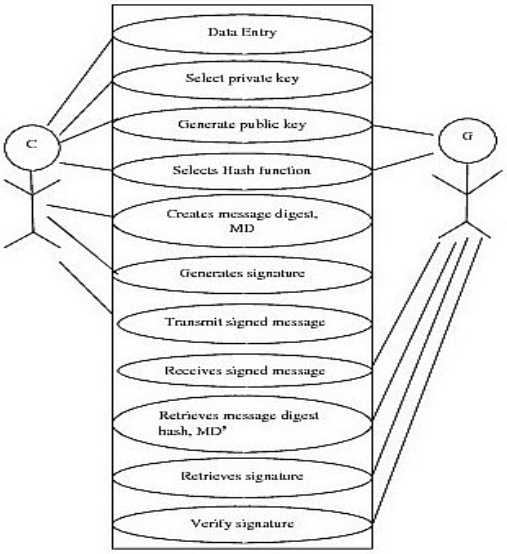


Fig 4 – Use case diagram of the proposed C2G type of smart E-Governance model [C- Citizen, G-Government].

verification of identity. The corresponding use case diagram of the above depicted proposed E-governance model is as follows –

Textual description of the above shown use case diagram is as follows –

U1: Data Entry – This step is initiated by the Citizen. In this step the Citizen inputs the relevant personal information for getting access of E-Governance service.

U2: Select Private Key – This step is initiated by the Citizen. In this step the Citizen selects the private key randomly with the help of Multipurpose Electronic Card (MEC).

U3: Generate Public Key – In this step the public key is computed mathematically and is made available publicly.

U4: Select Hash function – This step is initiated by the Citizen. In this step the Citizen selects a hash function which is already publicly available.

U5: Create Message Digest, MD – This step is initiated by the Citizen. In this step the Citizen calculates the message digest MD using the hash function and the message.

U6: Generate Signature – In this step the signature is generated for use over the message.

U7: Transmit signed message – This step is initiated by the Citizen. In this step the Citizen transmit the signed message to the Government.

U8: Receives signed message – This step is initiated by the Government. In this step the Government receives the transmitted message of the Citizen.

U9: Retrieves Message Digest hash, MD' – This step is initiated by the Government. In this step the Government retrieves the message digest hash, MD' i.e the message digest which have been transmitted by the Citizen.

U10: Retrieves Signature – This step is initiated by the Government. In this step the Government retrieves the digital signature used by the Citizen.

U11: Verify Signature – This step is initiated by the Government. In this step the Government verifies the signatures transmitted by the Citizen with the signatures obtained computationally after retrieving the message digest MD' along with the public key.

Scenario 1 (Mainline sequence): The authentication test completes successfully –
1. The Citizen is allowed to access the E-Governance services.
2. Finally the electronic transaction terminates successfully.

Scenario 2 (Mainline sequence): The authentication test terminates unsuccessfully –
1. The Citizen is barred from access of the E-Governance services.
2. Finally the electronic transaction terminates unsuccessfully.

4.2 Class Diagram

The class diagram depicts the internal relationships among the different entities like Citizen, Government, etc. In other words it can be stated that the class diagram shows the static structures of the system thereby displaying its logical platform to the user.

The generic class diagram of Citizen and Government in the proposed E-Governance model is as follows –

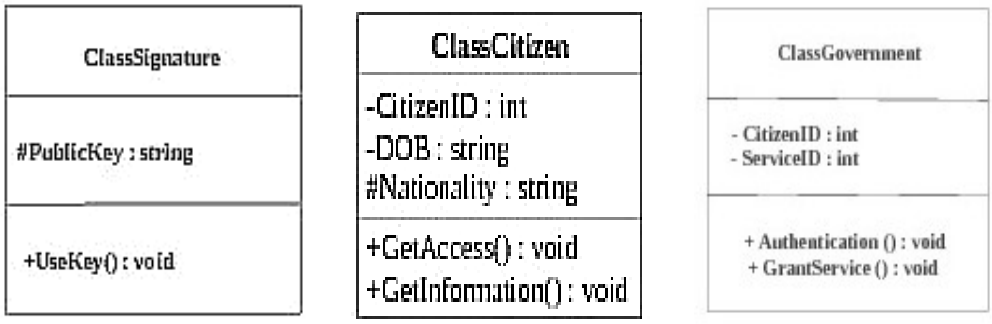


Fig 5 – ClassSignature, ClassCitizen and ClassGovernment.

ClassCitizen represents the "Citizen", ClassSignature will represent the "Signature" class and ClassGovernment will represent the Government. The corresponding sample code segment in C++ is as follows –

```
// ---------------------------------------------------------------------------
// Sample C++ code for the above class diagrams are as follows.
// ---------------------------------------------------------------------------
#include <iostream.h>
class ClassSignature          //--- This class represents the Signature
{
protected:  char PublicKey [20];
public: void UseKey (void) { }
};
class ClassCitizen            // ---This class represents the Citizen
{
private: int CitizenID; char DOB [20];
protected: char  Nationality [20];
public: void GetAccess (void) { }
void GetInformation (void) { }
};
class ClassGovernment     // ---This represents the Government.
{
private: int CitizenID; int ServiceID;
public: void Authentication (void) { }
void GrantService (void) { }
};
int main ( )
{
 ClassCitizen c;   //--- 'c'  denotes individual Citizen.
return 0;
}
```

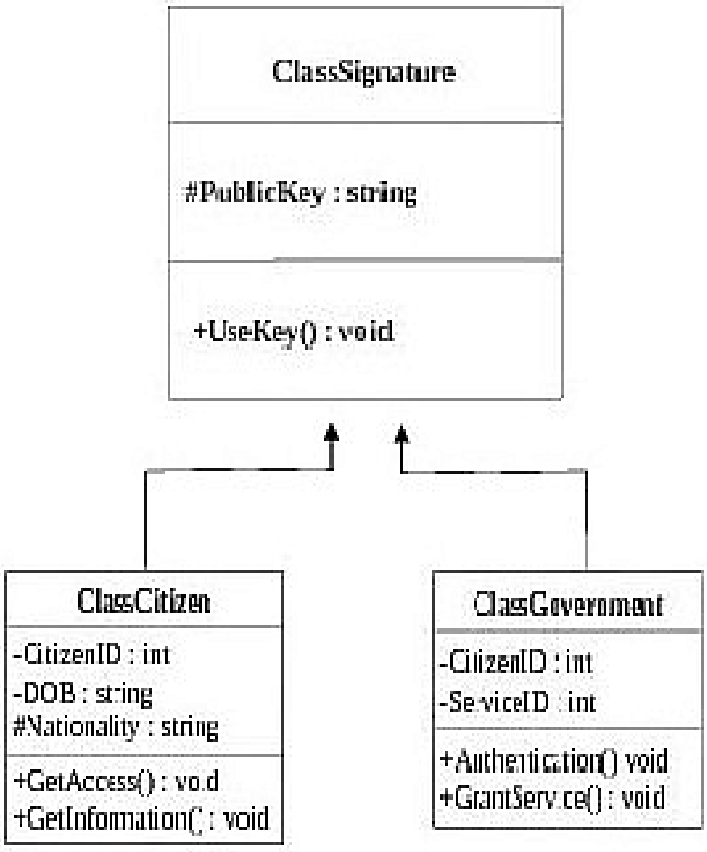


Fig 6 – Inheritance Diagram of the E-Governance model.

4.3 Sequence Diagram

The Sequence diagram is read from the top left most corners to depict the message passing among various objects of the system with respect to the time line. In this diagram the authentication of the Citizen using Elliptic Curve Digital Signature Algorithm (ECDSA) is performed by the Government during the C2G model of E-Governance transaction using Multipurpose Electronic Card (MEC).

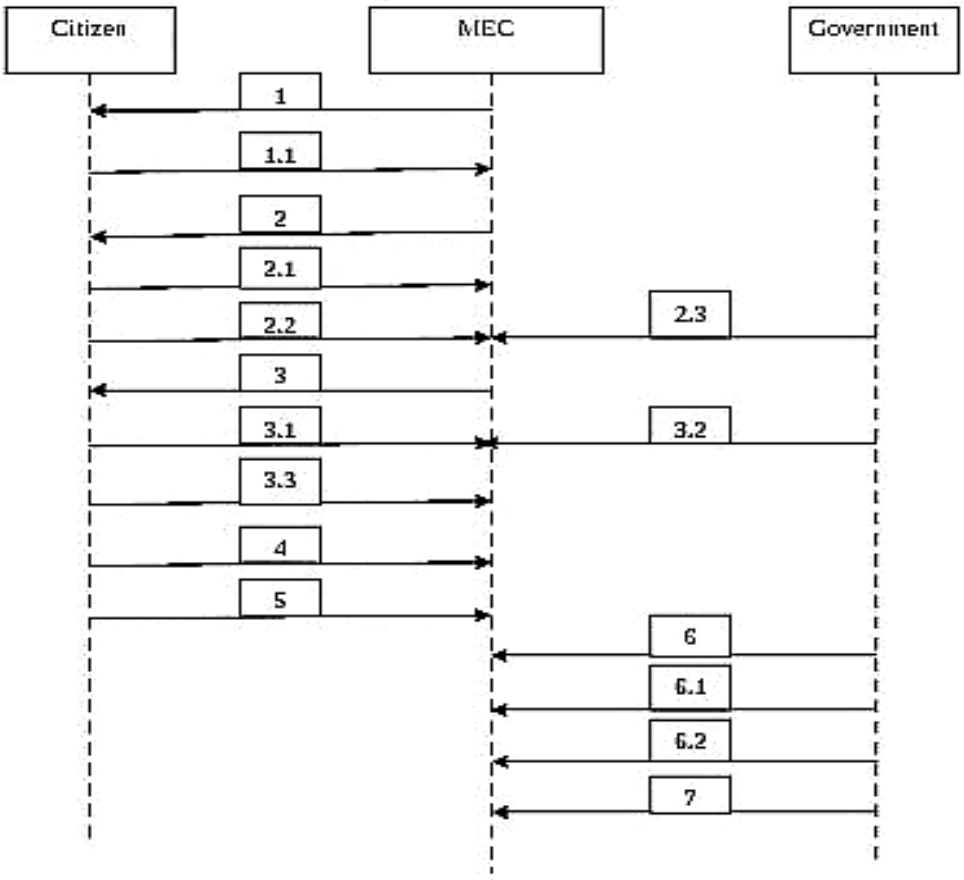


Fig 7 – Sequence diagram of the proposed C2G type of smart E-Governance model.

Steps –

1. MEC asks the Citizen for user input.
   1.1 Citizen provides the user input.
2. MEC asks the Citizen to select the private key randomly.
   2.1 Citizen selects the private key randomly.
   2.2 Public key is computed from the private key.
   2.3 Public key is made available openly for access of the Government.
3. MEC asks the Citizen to select the secure hash function.
   3.1 Citizen selects the secure hash function.
   3.2 The secure hash function selected by the Citizen is informed to the Government.
   3.3 The Message digest is computed with the help of secure hash function selected by the Citizen.
4. The digital signature is generated with the help of computed message digest and the private key selected randomly by the Citizen.
5. The Citizen transmits the digitally signed message to the Government.
6. The Government receives the digitally signed message transmitted by the Citizen.
   6.1 The Government retrieves the message digest hash, MD' from the received signed message of the Citizen.
   6.2 The Government retrieves the digital signature using the computed the message digest hash, MD'.

7. The Government initiates digital signature verification operation with the help of Multipurpose Electronic Card (MEC).

4.4 State chart Diagram

The State chart diagram depicts the various states of a class within a system. It also describes the several transitions that a particular class undertakes from state to state. The respective State chart diagram depicts various C2G type of E-Governance transaction using Multipurpose Electronic Card (MEC), like online payment of Income Tax, Telephone Bill, House Rent, ATM facilities, etc.

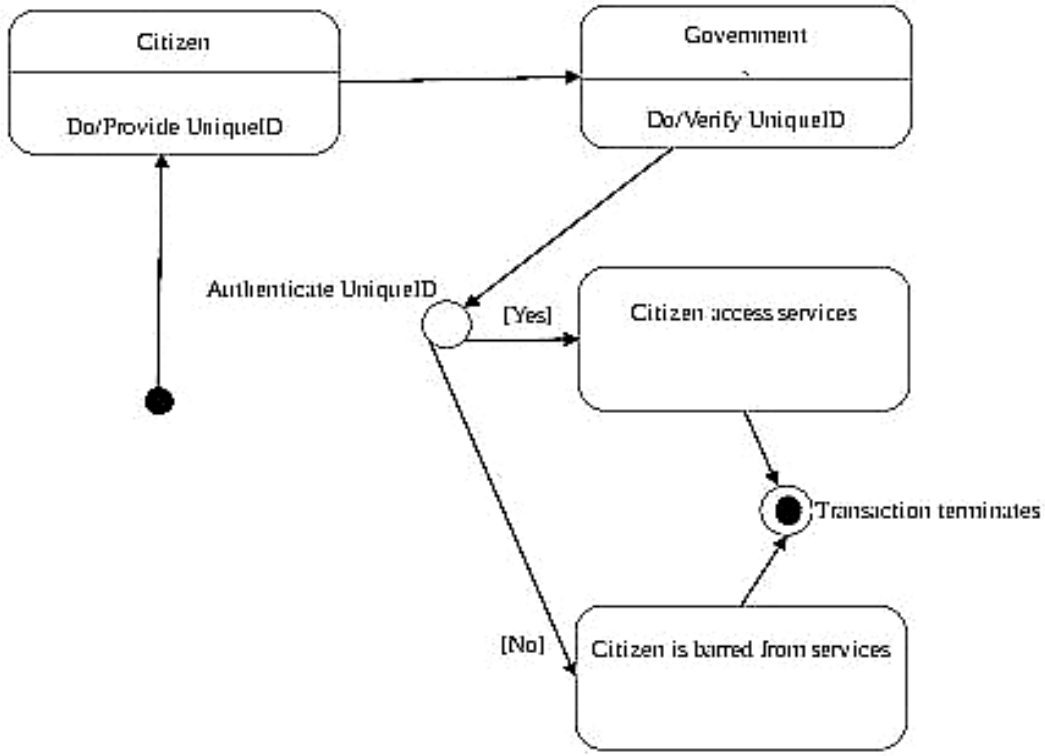


Fig 8 – State chart diagram of the proposed C2G type of smart E-Governance model.

The above shown State chart diagram demonstrates the process by which the Citizen can access the E-Governance services after proper identity verification of the Citizen using digital signature. It starts from the initial position thereby assuming that the Citizen have its own digitally signed UniqueID or CitizenID which is provided to the Government for verification purpose. The Government collects the UniqueID or CitizenID submitted by the Citizen and initiates the verification procedure. After this verification test is over probably two cases will arise as output –
Case 1. The verification test is successful. In this case the Citizen is allowed to access the E-Governmental services and the E-Governance transaction terminates.
Case 2. The verification test is unsuccessful. In this case the Citizen is barred from accessing the E-Governmental services and the E-Governmental transaction terminates.

4.5 Activity diagram

Activity diagrams display the procedural flow of control between two or more class objects during execution of an activity. The respective activity diagram is as follows –

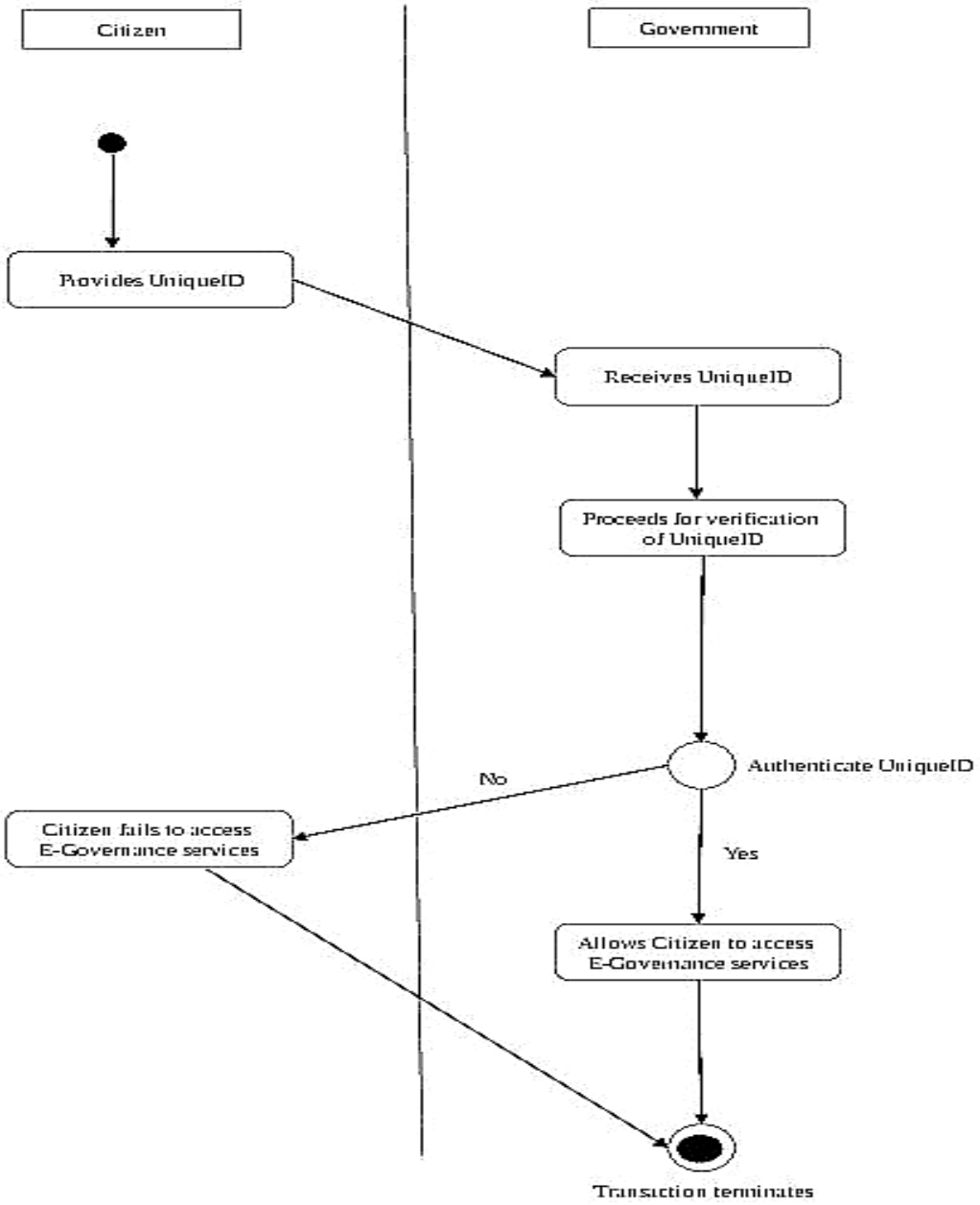


Fig 9 – Activity diagram of the proposed C2G type of smart E-Governance model.

In our diagram, two swim lanes have been shown. This is because we have depicted two different objects i.e Citizen and the Government which control separate activities within the process. In the initial stage of this process the Citizen provides its own digitally signed CitizenID or UniqueID to the Government. The Government initiates the authentication process of the CitizenID or UniqueID received from the Citizen. If the authentication process brings positive result, i.e in case of authenticated Citizen, the access to the E-Governance services is granted, else the Citizen is barred from the access of the E-Governance services.

5. CONCLUSION

From the above depicted Unified Modeling Language (UML) diagrams it is clear that Multipurpose Electronic Card (MEC), which is proposed by the authors, can be successfully implemented in E-Governance for authentication of Citizen very smartly and securely. In this paper authors have wrapped OOAD tools of UML with ECC for E-Governance transaction. However, the efficiency measurement of this proposed model in the context of object oriented metrics [13] can be considered as the future scope for this research work.

REFERENCES

[1] **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.

[2] **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.

[3] **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.

[4] **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.

[5] **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

[6] **Roy A**, Karforma S, Object Oriented approach of Digital certificate based E-Governance mechanism, Computational Intelligence and Communication Engineering, International Joint Conferences on CIIT, CENT, CSPE and CIITCom 2012 Proceedings (Springer), December 03-04, 2012, Pp: 360-366, Chennai, INDIA. ISSN 1867-8211

[7] **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.

[8] 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.

[9] 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.

[10] 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.

[11] Advantages and Disadvantages of Object Oriented Approach http://www.dba-oracle.com/t_object_oriented_approach.htm Date of access – January 20, 2013.

[12] UML basics: An Introduction to the Unified Modeling Language, http://www.nyu.edu/classes/jcf/g22.2440-001_sp06/handouts/UMLBasics.pdf Date of access - January 26, 2013.

[13] Object Oriented Metrics http://agile.csc.ncsu.edu/SEMaterials/OOMetrics.htm Date of access – January 26, 2013.

[14] Elliptic Curve Digital Signature Algorithm, http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf Date of access – January 26, 2013.

[15] Elliptic Curve Digital Signature Algorithm, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.132.3788 Date of access – January 28, 2013.
[16] Elliptic Curve Digital Signature Algorithm, http://msdn.microsoft.com/enus/library/system.security.cryptography.ecdsa.aspx Date of access - 28, 2013
[17] E-Governance, http://www.it.iitb.ac.in/~prathabk/egovernance/egov.html Date of access - January 28, 2013.
[18] E-Governance, http://india.gov.in/e-governance Date of access - January 28, 2013.
[19] Design and implementation of an ECDSA-based identity authentication protocol on WSN, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5355821 Date of access – February 08, 2013.
[20] A Comparative Analysis of Signature Schemes in A New Approach to Variant on ECDSA, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5381160 Date of access – February 08, 2013.
[21] An Identity Based Digital Signature from ECDSA, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5459073 Date of access – February 08, 2013.
[22] Secure and Efficient Generalized Signcryption Scheme Based on a Short ECDSA, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5636048 Date of access – February 08, 2013.
[23] Accelerated Verification of ECDSA Signatures, http://link.springer.com/chapter/10.1007%2F11693383_21 Date of access – February 10, 2013.
[24] Accelerate Verification of ECDSA Signatures, http://www.mathnet.or.kr/mathnet/preprint_file/cacr/2005/cacr2005-28.pdf Date of access – February 10, 2013.
[25] A Software Implementation of ECDSA on a Java Smart Card, http://amadousarr.free.fr/crypto/ECDSAJAVACARD.pdf Date of access – February 10, 2013.
[26] Decentralized Authorization with ECDSA on a Java Smart Card – A Software Implementation, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.36.675&rep=rep1&type=ps, Date of access – February 10, 2013.
[27] Low complexity smart card-based physical access control system over IP networks, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=1347052 Date of access – February 10, 2013.
[28] Digital signature systems based on smart card and fingerprint feature, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6071693 Date of access – February 10, 2013.
[29] Smart card initiative for South African E-Governance - A study, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=1626048 Date of access – February 10, 2013.
[30] Digital Identities and the Promise of the Technology Trio: PKI, Smart Cards, and Biometrics, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.165.9564&rep=rep1&type=pdf Date of access – February 10, 2013.
[31] A new remote user authentication scheme using smart cards, http://www.it.iitb.ac.in/~satish/phd/smartcard/ieee/2%20%20a%20new%20remote%20user%20authentication%20scheme%20using%20smart%20cards.pdf Date of access – February 12, 2013.
[32] Efficient remote user authentication scheme using smart card, http://www.sciencedirect.com/science/article/pii/S1389128605000460 Date of access – February 12, 2013.

AUTHORS

Abhishek Roy He was born at the 08th day of July in the year of 1982 at Burdwan, W.B, INDIA. He had done B.Sc in Information Technology (Hons) and M.Sc in Computer Technology from The University of Burdwan, W.B, INDIA. Presently he is working as a registered candidate for the degree of Ph.D in Computer Science under The Department of Computer Science from The University of Burdwan, W.B, INDIA. As the Life Member of Cryptology Research Society of India he finds his research interest in the application of cryptography for implementation of information security in E-Governance. He is also associated with the Second International Conference on Computing & Systems 2013 as the member of the organizing committee which will be organized by Department of Computer Science under The University of Burdwan. Apart from this, he is currentl y working as an Assistant Professor at Durgapur Society of Management Science (DSMS) which is affiliated under the West Bengal University of Technology (WBUT), W.B, INDIA. He had more than four years of teaching and research experiences in the arena of computer science. He had already published his research papers in various reputed national and international journals and conference proceedings. For further details may visit the homepage – https://sites.google.com/site/diaryofaroy

Dr. Sunil Karforma He had done B.E (Computer Science and Engineering) and M.E (Computer Science and Engineering) from Jadavpur University, W.B, INDIA. He has completed his Ph.D in the field of Cryptography. Presently he is working as an Associate Professor under The Department of Computer Science at The University of Burdwan, W.B, INDIA. He had already published his research papers in various reputed national and international journals and conference proceedings. His research interest is in E-Governance, E-Commerce, etc.