International Journal of scientific research and management (IJSRM)
||Volume||2||Issue||8||Pages||1212-1221||2014||
Website: www.ijsrm.in ISSN (e): 2321-3418

Authentication of User in E-Governance: A Digital Certificate Based Approach

Abhishek Roy[1], Sunil Karforma[2]

[1]Research Scholar, Dept. of Computer Science, The University of Burdwan
Golapbag, Burdwan, W.B, India 713104.
URL: *www.abhishekroy.wix.com/home* Email: *abhishek.roy@aol.in*

[2]Associate Professor, Dept. of Computer Science, The University of Burdwan
Golapbag, Burdwan, W.B, India 713104.
Email: *dr.sunilkarforma@gmail.com*

Abstract:

The development of communication technology have motivated the Citizen and the Government to communicate through electronic medium. For successful communication, a multifaceted electronic instrument must act as an interface between the participants, which will uniquely identify the Citizen. A brief literature review of several relevant research works further validate this concept of electronic transactions. In India though we have several instruments, which claim to uniquely identify the Citizen, non of them have proved to be efficient enough for all type of transactions. As a part of collective functioning towards problem solving approach, the authors have proposed a multivariate electronic smart card based E-Governance model. The proposed instrument named as Multipurpose Electronic Card (MEC) will attempt to uniquely identify the Citizen during various types of electronic transactions. As the complete solution of this problem is beyond the reach of an individual, to strengthen the user authentication scheme of our proposed model, we have shown the initial design for Digital Certificate based security protocols during Citizen-to-Government (C2G) type of transaction. For validation of the Citizen's identity, initially we have used name and date of birth of the Citizen. To further strengthen the validation process, we intend to include other vital parameters of the Citizen in near future, which will also explore future scope of research works in this field. To summarize, we can say that, the main objective of this research paper is to show the user authentication protocol using Digital Certificates, based on the vital parameters of the Citizen during Citizen-to-Government (C2G) type of proposed E-Governance transaction.

Keywords: User Authentication; Digital Certificate; Object.

1. Introduction.

The development of communication technology have motivated the Citizen and the Government to communicate through electronic medium. For successful communication, a multifaceted electronic instrument must act as an interface between the participants, which will uniquely identify the Citizen. A brief literature review of several relevant research works further validate this concept of electronic transactions. In India though we have several instruments, which claim to uniquely identify the Citizen, non of them have proved to be
efficient enough for all type of transactions. As a part of collective functioning towards problem solving approach, the authors have proposed a multivariate electronic smart card based E-Governance model. The proposed instrument will attempt to uniquely identify the Citizen during multiple types
of electronic transactions. As the complete solution of this problem is beyond the reach of an individual, to strengthen the user authentication scheme of our proposed model, we have shown the initial design of Digital Certificate based security protocols during Citizen-to-Government (C2G) type of transaction. For validation of the Citizen's identity, initially wehave used name and date of birth of the Citizen. To furthe strengthen the validation process, we intend to include other vital parameters of the Citizen in near future, which will also explore future scope of research works in this field. To summarize, we can say that, the main objective of this research paper is to show the user authentication protocol using Digital Certificates based on the vital parameters of the Citizen during Citizen-to-Government (C2G) type of proposed E-Governance transaction.

Section - 2 mentions the origin of research work. Section - 3 discuss the relevant literature review. Section - 4 explains the concept of our proposed multivariate electronic smart card based E-Governance mechanism. Section - 5 shows the design of Digital Certificate based user authentication scheme within our proposed mechanism. As we have applied the concept of object based and event driven programming,

this section discusses its static structure, table structure, sample outputs and a relevant discussion. Section - 6 states the conclusion drawn over the entire literature. References are finally listed at the last part of the paper.

Origin Of Research Work.

The developing countries like India are facing severe challenges for providing good governance to the Citizen, mainly due to the severe global economic meltdown phenomena. Unfortunately the conventional paper-based form of governance have failed to defend this crisis due to its large man-power requirement along with other huge operational overheads. To solve this crisis, electronic administration must be launched in each and every level of society to reduce the budget expense of the Government. As this electronic administration, which is also known as E-Governance is solely dependent on the public communication medium like Internet, etc, it is highly susceptible to illegitimate attacks performed by intruders. In order to solve these security crisis, Citizen must possess an unique digital identity, which will help to perform all type of E-Governance transactions securely, like payment of telephone bill, income tax, house rent, road tax, land tax, electricity bill, insurance and other similar types of premium, etc, accessing various facilities like, voting facility, ration facility, health facility, employment facility, etc.

In this current scenario, Indian Government is spending huge amount of money for launching several identity instruments for the Citizen like Birth Certificate, Ration Card, PAN (Permanent Account Number), Employment Card, Voter Card, Driving License, Aadhaar Card, Below Poverty Line (BPL) Card, Debit Card, Credit Card, etc, which mostly contains the common parameters of an individual with slight alterations. Though all of these instruments claim to uniquely identify the Citizen, they are yet to prove their claim mainly due to the following reasons :

(a) Launch of new instrument automatically questions the credibility of the identity instruments launched before it.

(b) Thus, mere existence of these multiple instruments, which requires huge resource utilization for its operations, prove the fact that, none of them are efficient enough to uniquely identify the Citizen during all types of E-Governance transactions.

That means, instead of using multipurpose single instrument, Citizen are compelled to use multiple instruments for multiple types of transaction. This scenario provides the intruder a scope to capture any of the identities of the Citizen and compel either the Citizen or the Government or both of them to negotiate in a compromising condition. To defend this situation, strong cryptographic system based security protocols should be deployed during the electronic transactions which will firmly verify the identity of the participant during the transactions. To fulfill this objective, researchers had worked out several applications, which are further explored by the following brief relevant literature review.

2. Literature Review.

The following list describes the research works carried out so far to achieve the above mentioned objective :

(a) Smart Power; a smart card electricity payment system **[20]** : In this paper the author have suggested the use of microprocessor based smart card for secure bill payment facility and automatic transfer of meter readings.

(b) Multi-application smart card with elliptic curve cryptosystem certificate **[19]** : In this paper the authors have overcome the limitations of memory size and processing power of smart cards using Elliptic Curve Cryptographic system (ECC). Finally a multi-application smart card based prototype have been developed with the help of digital certificate.

(c) Software architectural design model for e-governance systems **[27]** : In this paper the authors have explained the Software Architectural Design Model for E-Governance Systems (SADM-EGS).

(d) A framework for eGovernance solutions **[28]** : In this paper the authors have proposed a framework to simplify the various services of E-Governance through customized interfaces using multiple local languages.

(e) Use Cases for Identity Management in E-Government **[22]** : In this paper the authors have discussed the identity management system in E-governance through use case format in the perspective of New Zealand.

(f) Research on Framework of Public Crisis Management System under the Circumstance of E-Governance **[24]** : In this paper the authors have proposed a framework of crisis management system under E-Governance. It also provides detailed explanation of the subparts of the proposed framework.

(g) A smart card management and application system **[21]** : In this paper the author have implemented data security using Public Key Infrastructure (PKI) based smart card system containing two subparts named as Card Management System (CMS) and Application Management System (AMS).

(h) Secure E-Check payment model based on ECC **[25]** : In this paper the author have proposed a electronic check or E-Check based on ECC. The main objective

of this paper was to implement security within electronic payment system.

(i) Security Design for Electronic Medical Record Sharing System **[26]** : In this paper the authors have analyzed the electronic medical record sharing system using ECC to efficiently manage the security of user information within the electronic system.

(j) An effective framework for implementing electronic governance in developing countries : Bangladesh perspective **[23]** : In this paper the authors have proposed an effective framework for implementation of E-Governance in developing countries facing severe shortage of resources in various sectors.

The above discussion shows that researchers had tried in their own way to solve their problems using the concept of multivariate smart card based electronic applications. Thus, encouraged by these works, we have proposed a Citizen centric multivariate electronic smart card based E-Government system, which will attempt to solve the problems of the Citizen in India.

3. Proposed E-Governance Mechanism.

As mentioned earlier, in India, Government had issued several identity instruments one after another, to provide unique identity to the Citizen. Unfortunately, merely the presence of all these multiple identity instruments questions the credibility of the others. Hence, Citizen are forced to maintain multiple instruments for multiple transactions either through online or through off-line mode. Also the Government have to allocate huge resources to perform various online and off-line transactions using all these instruments. As a result, the administration is suppressed with huge operational overheads which finally hampers the national development, especially during the crisis moments of global economic meltdown. Also the situation becomes critical, as the intruder can attempt to capture any of these multiple identity instruments of an individual to fulfill their ill intentions.

To dispose all these problems, we have proposed a Citizen centric multivariate electronic smart card based E-Governance system. The proposed instrument named as Multipurpose Electronic Card (MEC), will act as the primary interface between the Government and the Citizen, which will help to perform all type of transactions by providing unique identity to the Citizen. Even this instrument will help the Citizen to perform financial transactions through Internet. The conceptual diagram of the proposed E-Governance model during Citizen-to-Government (C2G) type of transaction is shown in Figure – 1.

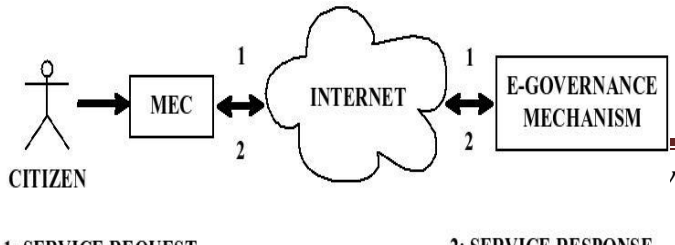


Fig 1: Conceptual diagram of proposed E-Governance mechanism.

Figure - 1 also shows that using the proposed instrument Multipurpose Electronic Card (MEC), Citizen can perform several types of electronic transactions with the Government. Even, Government can also promptly communicate to particular Citizen using this system. For better understanding of the proposed E-Governance mechanism its 3-tier architecture is shown in Figure - 2.

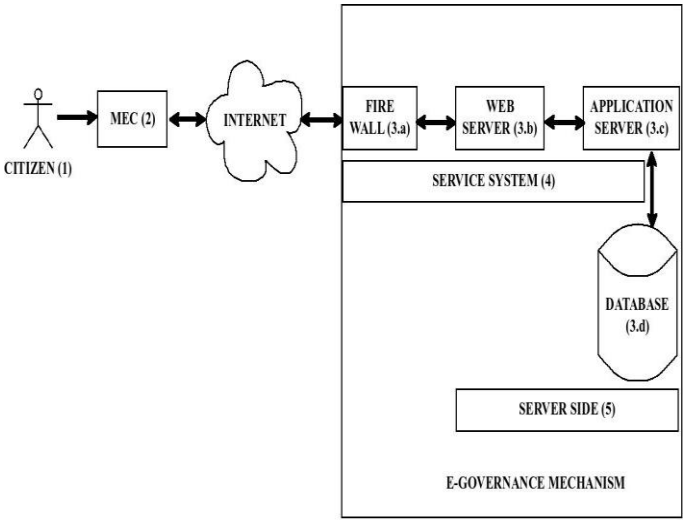


Fig 2: 3-tier architecture of proposed E-Governance mechanism.

Mainly, Figure - 2 depicts the necessity for installation of user authentication protocol within the proposed E-Governance mechanism to maintain its security and efficiency during electronic transactions. Thus, the description of the 3-tier architecture of the proposed mechanism may be stated as below :

(a) The Citizen initiate the electronic message communication through Multipurpose Electronic Card (MEC) to transmit its Service Request to the Government.

(b) Multipurpose Electronic Card (MEC) conveys the Service Request of the Citizen to the Government through the Internet.

(c) For secure handling of the sensitive information, the proposed E-Governance mechanism contain various components, which are mentioned below :

(i). Firewall - It helps to prevent the entry of spam ware, mal ware and other malicious elements within the E-Governance mechanism. Hence, it acts as a strong checkpoint to filter the

data before it proceeds further within the E-Governance mechanism.

(ii.) Web server - After passing through the Firewall, data enters the Web Server of the electronic mechanism. The transactions performed between the Citizen and the Government are reflected in this phase of message communication.

(iii). Application server - In this phase, data interacts with the Application Server of the proposed E-Governance mechanism.

(iv). Database - This component of our proposed E-Governance mechanism is used to act as the permanent storage of information for future use.

(d) The Service System of the proposed E-Governance mechanism contains the Firewall, Web Server and the Application Server of the application.

(e) The Server side of the proposed E-Governance mechanism contains the Web Server, Application Server and the Database storage of the application.

The bi-directional transmission of information shown in Figure – 1 and Figure – 2 includes the Service Request of the Citizen through Path – 1, and corresponding Service Response of the Government through Path – 2. Since, this proposed mechanism uniquely identifies the Citizen, it will detect the trespassers by preventing them from access of various facilities provided by the Government for the Citizen. That means, depending on the input provided by the Citizen through Service Request, the corresponding Service Response may be either affirmative or negative in nature. To establish the security features of our proposed E-Governance **[3]** mechanism, we have performed the following tasks :

As the part of ground work, we have studied the state of E-Governance **[18]** in Indian scenario to understand the real scenario before designing the blue-print of our proposed E-Governance model.

We have performed extensive literature review about various security features of E-Governance **[16]** mechanism , which defend the privacy and integrity of the mechanism from the intruders.

We have studied various risk factors of E-Governance **[14]** mechanism and tried to estimate its probable remedies to safe guard those risk factors.

We have defended the privacy of information from the intruders, within our proposed Citizen centric multivariate electronic smart card based E-Governance mechanism, using the Object Oriented Modeling (OOM) of International Data Encryption Algorithm (IDEA) **[17]** during Government-to-Citizen (G2C) type of transactions.

To impose authenticity and integrity of information within our proposed E-Governance mechanism, we have performed an extensive literature review of various features of Digital Signature **[10]** algorithm based applications.

To impose authenticity and integrity of information within our proposed mechanism, we have applied Object Oriented Modeling (OOM) of RSA Digital Signature Algorithm **[15]** during Government-to-Citizen (G2C) type of E-Governance transactions.

We have performed the Data Modeling **[1]** for Object Oriented Modeling (OOM) of RSA Digital Signature Algorithm during Government-to-Citizen (G2C) type of proposed E-Governance transaction.

We have performed extensive literature review on application of Biometric **[6, 12, 13]** techniques for authentication of information within electronic mechanisms. We also consider the application of the Biometric techniques within our proposed E-Governance mechanism as the future scope of our research work.

We have further strengthened the authenticity and integrity of information using Object Oriented Modeling (OOM) of complex cryptographic systems, like Elliptic Curve Digital Signature Algorithm (ECDSA) **[7, 8, 11]** during Citizen-to-Government (C2G) type of E-Governance transactions.

We have analyzed the efficiency of our proposed Object Oriented Modeling (OOM) of RSA Digital Signature Algorithm **[4]** and Elliptic Curve Digital Signature Algorithm (ECDSA) **[5]** during Government-to-Citizen (G2C) and Citizen-to-Government (C2G) type of E-Governance transactions respectively using various Software Metrics.

We have also applied Object Oriented Modeling (OOM) of Stream Ciphers **[2]** for authentication of user during Citizen-to-Government (C2G) type of proposed E-Governance transactions.

Even, we have modeled the Object Oriented approach of Digital Certificate **[9]** based user authentication technique using Unified Modeling Language (UML) Diagrams, during Citizen-to-Government (C2G) type of proposed E-Governance transactions, whose web-based application is shown further in this paper.

The objective of the above mentioned applications was to improve the security parameters of our proposed Citizen centric electronic smart card based E-Governance mechanism. As this proposed mechanism have to operate over the public communication medium like, Internet, etc which is very much susceptible to infringement attempts, in

this paper we have further strengthened the user authentication technique by the web-based application of Digital Certificates through object based and event driven programming approach.

4. User Authentication Using Digital Certificates.

In our application we have implemented the user authentication technique using the object based and event driven approach of Digital Certificates during Citizen-to-Government (C2G) type of E-Governance transactions. To fulfill this objective we have used the vital parameters of the Citizen, like name, date of birth, etc, to generate a Digital Certificate, which will help to uniquely identify that particular Citizen during various electronic transactions, carried out using our proposed Citizen centric multivariate electronic smart card based E-Governance mechanism. These Digital Certificates are used to encrypt the plain text, which is further transmitted by the Citizen to the Government. On the receiver side, the Government decrypts the cipher text and compares the received Digital Certificate with its counterpart obtained through algorithmic calculations. It is only after the successful verification of the Digital Certificates, the other vital parameters of the Citizen, like Father's name, sex, etc, can be accessed further.

As we have initially simulated the Digital Certificate based user authentication protocol using the name, date of birth of the Citizen within our proposed E-Governance mechanism, we have ample scope to claim for its better performance and security *w.r.t* other similar applications designed by the researchers throughout the world. Mainly, the objective of this research paper is to show the initial implementation of Digital Certificate based user authentication protocol using our proposed Citizen centric electronic smart card (i.e Multipurpose Electronic Card) based E-Governance mechanism, so that we can explore the areas for further enhancements.

In our web-based cryptographic system, we have used C# programming language to design the user interface, which also serves both the object based and event driven approach of our application. We have used SQL Server to perform the various database handling operations within our cryptographic system. Thus, the sequential description of our application during Citizen-to-Government (C2G) type of transaction is as follows:

At Citizen side:

(a) User initiates the E-Governance transaction.

(b) User input information for the parameters like Name, Date of Birth, Sex and Father's Name.

(c) User click the "Save" button to store the information.

(d) Digital certificate is generated using the Name and Date of Birth of the Citizen after activation of the event i.e "Save" button.

At Government side:

(a) User enters the encrypted digital certificate of the Citizen for verification.

(b) User click the "Check Decode" button to retrieve the plain text i.e name and date of birth of the Citizen. The verification of the Digital Certificate is initiated after activation of the event i.e "Check Decode" button.

(c) It is only in the case of successful verification of Digital Certificate, the actual plain text will be generated for display purpose.

(d) Once successful verification of the Digital Certificate is over, the user can further display the other vital parameters of the Citizen like, name, father's name, date of birth, sex, etc, through activation of another event, i.e "Search" button.

To explore our object based approach, the vital classes used within the application, and the table structure used to manage the corresponding databases are discussed below.

5. 1 Classes used within the application.

(a) *_Default*: This class loads the default page of the application. It contains two parts, one of which generates the design of the application and the other executes the coding of the application. The vital methods used within this class to activate various events are as follows :

(i). *btnproceed_Click (object sender, EventArgs e) { }* : This method is used by the Citizen to input information in our web-based application.

(ii). *linkedit_Click (object sender, EventArgs e) { }* : This method is used to *edit* data present in our application.

(iii). *lbldelete_Click (object sender, EventArgs e) { }* : This method is used to *delete* data from our application.

(iv). *SaveItem ( ) { }* : This method is used to *save* data to the database of the application.

(v). *FillGridView ( ) { }* : This method is used to show details in the *gridView* of the application.

(vi). *FillControl ( ) { }* : This method is used to display the details after fetching it from the database.

(vii). *delete ( ) { }* : This method is used to *delete* details from the database.

(b) Connection : This class is used to establish the trusted connection within our application.

(c) CodeClass : This class mainly contains a method named as *ScalerReturnString ( ) { },* which accepts a string as an argument and return string as the output. The main objective of this method is to activate Structured Query Language (SQL) commands to perform database operations.

(d) *EncodeDecode* : This class contains two vital methods, named as *base64Encode ( ) { }* and *base64Decode ( ) { }*. Both of these methods accepts string as arguments and return string as the output. The description of these methods are as follows :

(i). *base64Encode ( ) { }* : This method accepts plain text as an argument and return the cipher text as the output. Based on the call of the Citizen through the activation of an event, i.e "Save" button, this method encrypts the plain text using exception handling approach.

(ii). *base64Decode ( ) { }* : This method accepts cipher text as an argument and return plain text as the output. Based on the call of the Government through the activation of an event, i.e "Check Decode" button, this method decrypts the cipher text using exception handling approach.

Thus, from the description of the static structure of our web-based cryptographic system, it is clear that, both the participants i.e the Government and the Citizen have to deal with huge load of classified information during its operation. So, the database used to deal with this huge load is explained further in the form of table structure of our web-based cryptographic system.

5. 2 Table structure of the application.

As the primary objective of this web-based cryptographic system was only to show the application of Digital Certificates for authentication of users during Citizen-to-Government (C2G) type of E-Governance transactions, we have sufficient scope of improvements in the database management part of our application. As we are yet to implement this application in practical scenario, just to maintain the simplicity of the database structure, we have used only one database table to store the information of Citizen, which is further mentioned below :

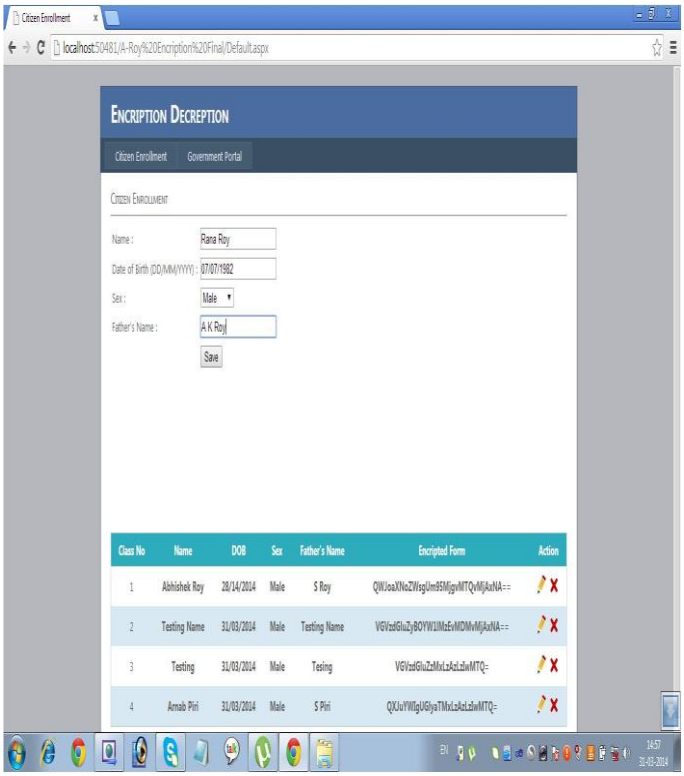
Database Name : ARoy

```
CREATE TABLE [dbo].[Encodeing] (
    [Id] [bigint] IDENTITY (1,1) NOT NULL,
    [Name] [varchar] (50) NULL,
    [DOB] [varchar] (50) NULL,
    [Sex] [varchar] (50) NULL,
    [FathersName] [varchar] (50) NULL,
    [EncriptedForm] [varchar] (1000) NULL,
CONSTRAINT [PK_Encodeing] PRIMARY KEY CLUSTERED (
    [Id] ASC
)
WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON
) ON [PRIMARY] ) ON [PRIMARY] GO
```

The sample outputs obtained after successful execution of our software based cryptographic system are further shown below.

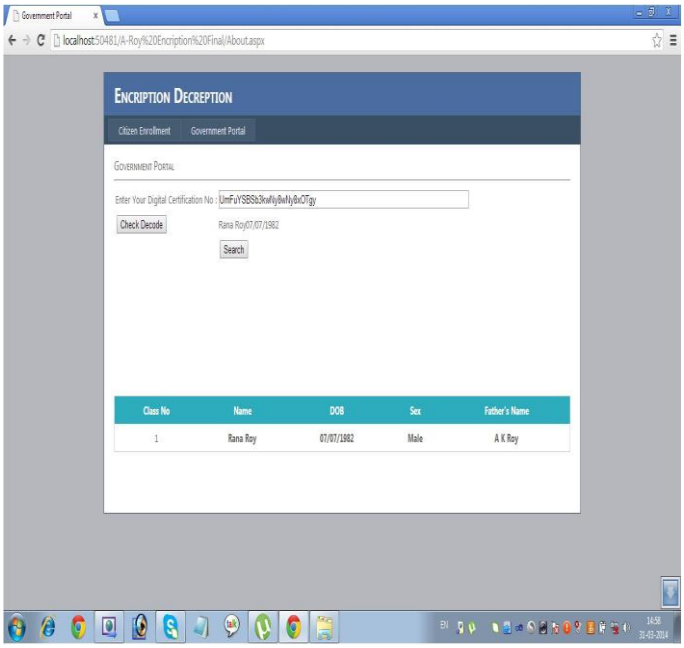
5. 3 Sample Outputs.

The following sample output shows the Digital Certificate based encryption of plain text through click of the "Save" button, during enrollment of the Citizen within our web-based application.



Sample Output – 1 : Encryption of information for generation of Digital Certificate.

The following sample output shows the Digital Certificate based decryption of cipher text through click of the "Check Decode" button, during verification of Digital Certificates by the Government. After successful verification of the Digital Certificate, the user can display the further details on click of the "Search" button.



Sample Output – 2 : Decryption of information for verification of Digital Certificate.

5. 4 Discussion.

In our web-based cryptographic system, we have mainly shown the application of Digital Certificates for authentication of user during Citizen-to-Government (C2G) type of E-Governance transactions. Initially we have used the name and date of birth of the Citizen for generation of Digital Certificates, which may be enhanced further during practical implementation of our model. As it will be an unscientific approach to claim about complete security for any cryptographic system, we can conclude that there is always scope for further enhancements for each and every cryptographic system.

Apart from this, experts may note for less personal privacy of information, within our proposed E-Governance mechanism. However, in that case, we can only say that, in India the Government had already destroyed it by launching several identity instruments one after another. At least we have tried to relieve the Citizen by proposing a multivariate electronic instrument based E-Governance mechanism, which will attempt to replace all the existing instruments and hence will provide more personal privacy of information compared to the current situation.

5. Conclusion.

From the entire discussion we can summarize that, we have shown the application of Digital Certificates for authentication of user during Citizen-to-Government (C2G) type of proposed E-Governance transaction. As we have shown the authentication of user during message communication through Internet, we expect that, with further enhancements, Citizen can access our proposed application efficiently, using various Internet based electronic gadgets like tablets, smart phones, etc. Hence, to make this application realistic and user friendly in nature, we have used the object based and event driven approach of programming. The object based approach of our application will help to accommodate future changes using the basic features of Object Oriented Paradigm (OOP). Moreover the user friendly interface of our proposed application, which is designed through event driven programming approach, will motivate the Citizen to use it easily based on few events. It may be possible that other researchers had also applied the Digital Certificates for similar purposes within their cryptographic system, however the application of Digital Certificates to find solutions to our own problems may be considered as the uniqueness of our model. Apart from the application of Digital Certificates, we have also applied the Digital Signatures, Stream Ciphers, etc for authentication of user within our proposed model. Finally, as no cryptographic system can be claimed to be completely secured from the infringement attempts of the intruders, we also have scope

for further enhancements in the field of certificate generation and database management system, which may be considered as the future scope of our research work.

References.

1. **A Roy**, S 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 Zaigham Mahmood of University of Derby, U.K, Published by IGI Global, USA, Pp: 280-299 DOI:10.4018/978-1-4666-6082-3.ch012

2. **A Roy** and S 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.

3. **A Roy** and S 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, ISSN 2277 128X.

4. **A Roy** and S Karforma, *Coupling and cohesion analysis for implementation of authentication in E-Governance*. Fourth International Joint Conference - Advances in Engineering and Technology (AET) 2013, December 13-14, 2013, NCR, INDIA, (Elsevier), Pp: 544-554, ISBN 978-93-5107-193-8.

5. **A Roy** and S 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.

6. S Sarkar and **A 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.

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

8. **Roy A** and 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), March 22 - 23, 2013, Pp: 207-222, ISSN 2231-5403, ISBN 978-1-921987-11-3, DOI: 10.5121/csit.2013.3219.

9. **A Roy** and S 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, Chennai, INDIA, (Elsevier), Pp: 380-386, ISBN 978-93-5107-194-5.

10. **A Roy** and S 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.

11. A Hoda, **A Roy** and S Karforma, *Application of ECDSA for security of transaction in E-Governance*. Proceedings of Second National Conference on Computing and Systems - 2012 (NaCCS - 2012), March 15 - 16, 2012, W.B, INDIA, 1st Edition – 2012, Pp: 281-286, ISBN 978-93-80813-18-9.

12. S Sarkar and **A Roy**, *A Study on Biometric based Authentication*. Proceedings of Second National Conference on Computing and Systems - 2012 (NaCCS - 2012), March 15 - 16, 2012, W.B, INDIA, 1st Edition – 2012, Pp: 263-268, ISBN 978-93-80813-18-9.

13. **A Roy**, S Sarkar, J Mukherjee and A 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, February 21 – 22, 2012, Calcutta, INDIA, Vol: 1, Pp:153-160, ISBN 978-81-923820-0-5.

14. **A Roy** and S 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.

15. **A Roy**, S Banik and S 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.

16. **A Roy** and S 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.

17. **A Roy**, S Banik, S Karforma and J 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, W.B, INDIA, Pp: 263-269, ISBN 93-80813-01-5.

18. C Sur, **A Roy** and S 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, W.B, INDIA, Pp: a-h, ISBN 8190-77417-4.

19. J K Liu, V K Wei, C Siu, R L Chan and T Choi, *Multi-application smart card with elliptic curve cryptosystem certificate*, EUROCON'2001, Trends in Communications, International Conference on, July 2001,Vol 2, Pp: 381-384, DOI 10.1109/EURCON.2001.938143.

20. M C S Simpson, *Smart Power; a smart card electricity payment system*, UK Electricity Prepayment Systems, IEE Colloquium on, Birmingham, January 23, 1996, Pp: 3/1-3/4, DOI 10.1049/ic:19960288.

21. M Mohandes, *A smart card management and application system*, Progress in Informatics and Computing (PIC), 2010 IEEE International Conference on, December 2010, Vol 2, Pp: 1220-1225, DOI 10.1109/PIC.2010.5687971.

22. R McKenzie, M Crompton and C Wallis, *Use Cases for Identity Management in E-Government*, Security Privacy, IEEE, March 2008, Vol 6 Number 2, Pp: 51-57, DOI 10.1109/MSP.2008.51, ISSN 1540-7993.

23. M M Rahman and S A Ahsan Rajon, *An effective framework for implementing electronic governance in developing countries: Bangladesh perspective*, Computer and Information Technology (ICCIT), 2011 14th International Conference on, December 2011, Pp: 360-365, DOI 10.1109/ICCITechn.2011.6164814

24. Hu Da-li, Wang Hua-lin and Wu Chang-nan, *Research on Framework of Public Crisis Management System under the Circumstance of E-Governance*, Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on, October 2008, Pp: 1-4, DOI 10.1109/WiCom.2008.2163

25. Xe Rui, *Secure E-Check Payment Model Based on ECC*, Information Engineering (ICIE), 2010 WASE International Conference on, August 2010, Volume 2, Pp: 109-112, DOI 10.1109/ICIE.2010.121.

26. Qingzhang Chen, Zhehu Wang and Wangqiao Zhang, *Security Design for Electronic Medical Record Sharing System*, Biomedical Engineering and Computer Science (ICBECS), 2010 International Conference on, April 2010, Pp: 1-4, DOI 10.1109/ICBECS.2010.5462323.

27. D N Murthy and R V P Kumar, *Software architectural design model for e-governance systems*, TENCON 2003. Conference on Convergent Technologies for the Asia-Pacific Region, October 2003, Volume 1, Pp: 183-187, DOI 10.1109/TENCON.2003.1273310.

28. P A Mittal, M Kumar, M K Mohania, M Nair, N Batra, P Roy, A Saronwala and L Yagnik, *A framework for eGovernance solutions*, IBM Journal of Research and Development, September 2004, Volume 48 Number 5.6, Pp: 717-733, DOI 10.1147/rd.485.0717, ISSN 0018-8646

Author Profiles –

ABHISHEK ROY [AUTHOR]: He is currently pursuing his Ph.D. Degree in Computer Science under Department of Computer Science, The University of Burdwan, W.B, India 713104. He have almost seven (07) years of professional experience, which includes industry as well as academia. The author acts as the Life Member of various reputed research societies, like Cryptology Research Society of India (CRSI), Indian Statistical Institute (ISI) and Society for Research in Information Security and Privacy (SRISP), Jadavpur University. He also acts as the Editorial / Reviewer Board Member of various reputed international journals. He had published research papers in various reputed international and national platforms. He finds his research interest in E-Governance, Information Security, Cryptography, etc.

For further details please visit the followings : URLs: https://sites.google.com/site/diaryofaroy
http://abhishekroy.wix.com/home Email: abhishek.roy@aol.in

DR. SUNIL KARFORMA [CO-AUTHOR]: He is currently working as the Associate Professor & Head under Department of Computer Science, The University of Burdwan, W.B, India 713104. He had done his bachelor degree and master degree in Computer Science and Engineering from Jadavpur University and Ph.D. from The University of Burdwan, W.B, India. He had published various research papers in reputed international and national platforms. He finds his research interest in E-Governance, E-Commerce, E-Learning, etc. For further details :

Emails: sunilkarforma@yahoo.com dr.sunilkarforma@gmail.com