ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Advanced E- Governance Security Using Certificate less Effective Key Management

F.Jerlinmary[1], Dr.M.Deepamalar[2]

M.Phil Scholar, Post Graduate and Research, Department of Computer Science, Parvathy's Arts and Science College, Dindigul, India[1]

Asst. Professor, Post Graduate and Research, Department of Computer Science, Parvathy's Arts and Science College, Dindigul, India[2]

ABSTRACT: E-governance is the latest technological trend in the governance process all over the world whose application attribute can be variety, embedded, rabidly, year – round symbol, moral, ample, responsive and transparent, in the short very smart process are called e-governance. The e-governance system data should deliver speedy, space efficient, cost effective and secure way among other governments and its citizens. In e-governance large amount of packets would be transferred between governments to government using internet which is insure and time consuming. Intruders can change the information and communication technologies impose data integrity, privacy, and authenticity which must maintained with less communication costs using available bandwidth. Addressing key security requirements such as node authentication, data integrity and confidentiality is crucial for the success of critical e-governance application this paper propose a certificate less effective key management protocol for secure communication in dynamic e-governance applications characterized by node mobility. This proposed L-EKM supports efficient key revocation for compromised nodes and minimizes the impact of a node compromise on the security of other communication links. A security analysis of the proposed scheme shows that CL-EKM protocol is effective in defending against various attacks.

KEYWORDS: E-Government, Cryptography, Certificate effective key management.

I.INTRODUCTION

The best utilization of the information and communication technology (ICT) to improve efficient service delivery to the citizen is called e-governance. E-governance is the process of delivering information to the user or client in an efficient way for the benefit of both client &government. In the present days of global economic meltdown the Government of the developing countries like INDIA are facing severe challenge in maintaining an efficient administration in its core and allied sectors within an affordable budget. The application of advanced Information and Communication Technology (ICT) will help to implement the Electronic Governance which will replace its conventional form to deliver services to the populace at reduced rate. To do so, the Citizen must possess a multivariate electronic instrument which will uniquely identify the Citizen in all respect and help to communicate with the Government.

A.E-governance

Governance is a process of information sharing, disseminating between the Government and Citizens, Government and Businesses and Government and Government. E-Governance also covers all these relationships as follows:

(a)G2C (Government to Citizens)

E-Governance to Citizens in two-way communication allows citizens to instant message directly with public administrators, and cast remote electronic votes (electronic voting) and instant opinion voting. Transactions such as payment of services, such as city utilities, can be completed online or over the phone. Mundane services such as name

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

or address changes, applying for services or grants, or transferring existing services are more convenient and no longer have to be completed face to face.

(b)G2E (Government to Employees)
E-Governance to Employee partnership (G2E) is one of four main primary interactions in the delivery model of E-Governance. It is the relationship between online tools, sources, and articles that help employees maintain communication with the government and their own companies. E-Governance relationship with Employees allows new learning technology in one simple place as the computer. Documents can now be stored and shared with other colleagues online.
(c)G2G (Government to Government)
E-government brings many advantages into play such as facilitating information delivery, application process/renewal between both business and private citizen, and participation with constituency. There are both internal and external advantages to the emergence of IT in government, though not all municipalities are alike in size and participation.
(d) G2B (Government to Business)
Government-to-Business (G2B) is the online non-commercial interaction between local and central government and the commercial business sector with the purpose of providing businesses information and advice on e-business 'best practices'.

II. RELATED WORK

A suitable encryption key algorithm are used to secure data and communication .In this paper, a certificate less – effective key management (CL-EKM) algorithm is proposed to have a secure communication in E-governance characterized by node mobility. The CL-EKM algorithm supports an E-government communication for key updates and manages once a node joins or leaves a cluster and ensures forward and backward key secrecy.CL-EKM is a scheme that provides security by avoiding the key escrow and eliminating the drawback of identity-based cryptography. Several certificateless models have been proposed to enhance the efficiency and overcome adversaries attacks. In this paper, we survey various public key encryption schemes on certificate less setting with the security model and discuss the performance. Cryptography for the generation of digital certificates and also provide data encryption.

By implementing those concepts we can get more confidentiality sharing information in the cloud and also get more efficiency for generation of digital certificates. In this approach we can also provide semi trusted for the authentication of users in the E-governance. If the user is authenticated we will provide provision for the decryption of retrieving dataIf the user is not authenticated it will not get the decryption process. In this schema the accessing control of data owner is to perform the encryption of data and stored the data into E-governance. For the encryption of data items the data owner will use one of the symmetric cryptography techniques. The advantage of our schema is that easy generation of secret key and also provides more confidentiality of sharing information in the E-governance.

III. CRYPTOGRAPHY

Cryptography is securitypurpose of the world using. Every intruder can hacks information from the network.avoide the abstractly using cryptography.The many scheme used for encryption constitute the area of study known as **cryptography**. Such as scheme is known as **cryptographic system** or a **cipher**. Techniques used for deciphering message without any knowledge of the enciphering details fall into area called as **cryptanalysis**.The area of cryptography and cryptanalysis together are called **cryptology**. As millions of electronic messages that traverse the Internet each day, it is easy to see how a well placed network sniffer might capture a wealth of information that users would not like to have disclosed to unintended readers. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of cryptography, to prevent intruders from being able to use the information that they capture. Encryption is the process of translating information from its original form (called plain text) into an encoded, incomprehensible form(called cipher text)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

.A. CryptographyTerminology

Basic Terms

- **Plain Text:** The original message that the person wishes to communicate with the other is defined as Plain Text. For example, a person named alice wishes to send "Hello Friend how are you" message to the person Bob. Here "Hello Friend how are you" is a plain text message.
- **Cipher text:** The message that cannot be understood by any one or a meaningless message is what we call as Cipher text. Suppose, "Ajd672#@91ukl8*^5%" is a Cipher Text produced for "Hello Friend how are you"**.** The transformed message.
- **Cipher:** An algorithm for transforming an intelligible message to unintelligible by transposition.
- **Key**: Some critical information used by the cipher, known only to the sender & receiver. A key is a numeric or alpha numeric text or may be a special symbol. the key is used when encryption takes place on the plain text and at the time of decryption takes place on the cipher text. For example, if key of 3 is uses by the Alice to encrypt the plain text "President" then cipher text produced will be "Suhylghqw".
- **Encipher** :(Encode) the process of converting plaintext to cipher text using a cipher and a key. A process of converting plain text into cipher text is called as Encryption. This process requires two things- an encryption algorithm and a key. algorithm means the technique that has been used in encryption. Encryption of data takes place at the sender side
- **Decipher** :(Decode) the process of converting cipher text back into plaintext using a cipher & key. A reverse process of encryption is called as Decryption. In this process Cipher text is converted into Plain text. Decryption process requires two things- a decryption algorithm and a key. Algorithm means the technique that has been used in Decryption. Generally the both algorithms are same.

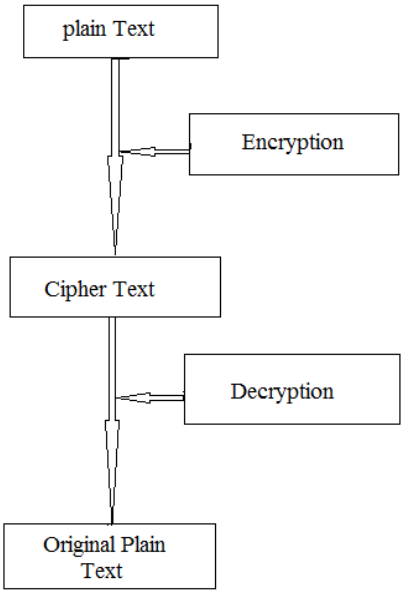

Figure 1. Cryptographic techniques

IV. CRYPTOGRAPHY IN E-GOVERNANCE SECURITY

In the present days of global economic meltdown the Government of the developing countries like INDIA are facing severe challenge in maintaining an efficient administration in its core and allied sectors like business, education, health, etc, throughout its jurisdiction within an affordable budget. This task becomes more difficult if the Indian Rupee (INR) regularly faces new highest of inflation due to recession. However, nobody will disagree that, to defend this recession,

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

the Government must use its resources in a very skilful manner, so that existing budget expenses get reduced, thereby maintaining its efficiency level.

The application of advanced Information and Communication Technology (ICT) will help to implement a Citizen centric Electronic Governance mechanism which will operate on behalf of the conventional form of Governance and will deliver services to the doorstep of the populace at reduced rate. To do so, the Citizen must possess a multivariate electronic instrument which will uniquely identify the Citizen in all respect and help to communicate with the Government.

Though our Government have launched several identity instruments which claims to uniquely identify the Citizen that respective nomenclature only, non so ever have the provision to become a complete E-Governance instrument, not even the latest Aadhaar Card. Focusing on this topic, the authors have already proposed a Citizen centric multivariate smart card based secured E-Governance mechanism which will be capable enough to perform all the governmental transactions, including the financial ones also.

Figure 2: Model Smart card

V. CERTIFICATE LESS EFFECTIVE KEY MANAGEMENT

Certificate less cryptography is a variant of ID-based cryptography intended to prevent the key escrow problem. Ordinarily, keys are generated by a certificate authority or a key generation center (KGC) who is given complete power and is implicitly trusted. To prevent a complete breakdown of the system in the case of a compromised KGC, the key generation process is split between the KGC and the user.

The KGC first generates a key pair, where the private key is now the partial private key of the system. The remainder of the key is a random value generated by the user, and is never revealed to anyone, not even the KGC. All cryptographic operations by the user are performed by using a complete private key which involves both the KGC's partial key, and the user's random secret value.

Certificateless Effective key cryptography (CL-EKM), the user's full private key is a combination of a partial private key generated by a key generation center (KGC) and the user's own secret value. The special organization of the full private/public key pair removes the need for certificates and also resolves the key escrow problem by removing the responsibility for the user's full private key. We also take the benefit of ECC keys defined on an additive group with a 160- bit length as secure as the RSA keys with 1024-bit length.

In order to dynamically provide both node authentication and establish a pair wise key between nodes, we build CL-EKM by utilizing a pairing-free certificate less hybrid sign encryption scheme (CL-HSC).In certificate less Effective key cryptography (CL-EKM), the user's full private key is the combination of a partial own secret value. The special organization of the full private/public key pair removes the need for certificates and also resolves the key escrow problem by removing the responsibility for the user's full private key

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

We also take the benefit of ECC keys defined on an additive group with a 160- bit length as secure as the RSA keys with 1024-bit length. In order to dynamically provide both node authentication and establish a pair wise key between nodes, we build CL-EKM by utilizing a pairing-free certificate less hybrid signcryption scheme (CL-HSC)

The types of key are Certificate less public/private key, Individual nodes key, Pair wise key and Cluster key.

- **Certificate less public/privatekey:** this key generates a mutually authenticated pair-wise key.
- **Individual node key:** each node will have individual key.
- **Pair wise key:** to have a secure communication and authentication of nodes each node shares a different pair wise key with the neighboring nodes.
- **Cluster key:** All the nodes in a cluster share a key and these keys are named as cluster key.

.

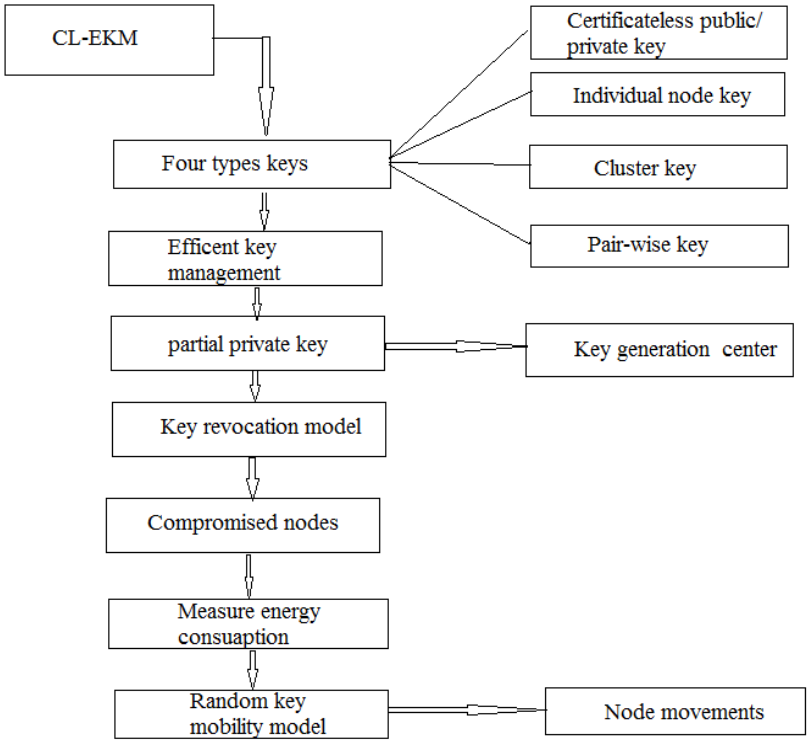

Figure 3. Types of CL-EKM

The special organization of the full private/public key pairs removes the need for certificates and also resolves the key escrows problems by eliminating the responsibility for the users full private key, the generation of CL-EKM and movement of nodes. Compared to other approach the proposed schema provides more security, decrease overhead and protect data confidentiality and integrity

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

VI. IMPLEMENTATION OF E GOVERNANCE SECURITY USING CL-EKM

We have implemented the user authentication technique in our proposed E-Governance mechanism using Object Oriented Modeling of RSA digital signature over G2C type of transactions. This application, encryption of information is done based on the call of the Government, whereas the decryption of information is done based on the call of the Citizen. For better understanding of these message passing and their corresponding replies, the Inheritance Diagram of Object Oriented Modeling (OOM) of which states that Government initiates the transactions and subsequent encryption of messages, whereas the Citizen responds for subsequent decryption of the encrypted messages.

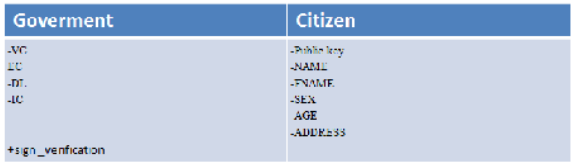

Figure 4: e-governance using CL-EKM

Acertificate less effective key management (CL-EKM) scheme for e governance. In certificate less public key cryptography (CL-PKC) [12], the user's full private key is a combination of a partial private key generated by a key generation center (KGC) and the user's own secret value. The special organization of the full private/public key pair removes the need for certificates and also resolves the key escrow problem by removing the responsibility for the user's full private key. We also take the benefit of ECC keys defined on an additive group with a 160bit length as secure as the RSA keys with 1024-bit length. In order to dynamically provide both node authentication and establish a pair wise key between nodes, we build CL-EKM by utilizing a pairing-free certificate less hybrid sign encryption scheme (CL-HSC). Due to the properties of CL-HSC, the pair wise key of CL-EKM can be efficiently shared between two nodes without requiring taxing pairing operations and the exchange of certificates.

To support node mobility, our CL-EKM also supports lightweight processes for cluster key updates executed when a node moves, and key revocation is executed when a node is detected as malicious or leaves the cluster permanently.
CL-EKM is scalable in case of additions of new nodes after network deployment. CL-EKM is secure against node compromise, cloning and impersonation, and ensures forward and backward secrecy. The security a
analysis of our schemeeffective in e governance.

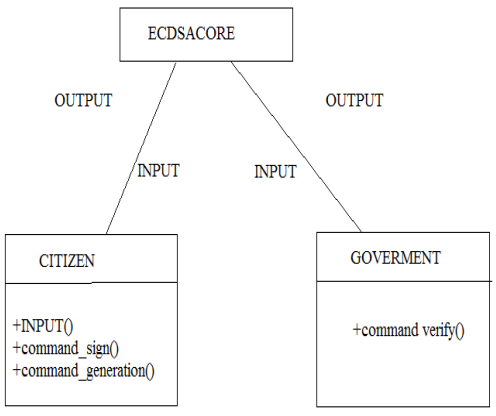

Figure 5**: Proposed e-governance Architecture on CL-EKM**

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

1. **Input Data** - Citizen Provides The Essential Information To The Government Through Multipurpose Electronic Card (MEC).
2. **User Authentication** - Citizen Authenticates Its Identity For Access Of Benefits Granted By The Government. The Entire Transaction Is Done With The Help Of Multipurpose Electronic Card (MEC).
3. **Store Service** - Government Stores The Services Provided To The Citizen In AE-Service Server.
4. **Benefits**- E-Service Server Allows The Access Of The Services To The Citizen .

VII. RESULTS AND DISCUSSION

In this research proposed the successful execution of the smart card based E-governance mechanism. The identity of the user must be verified carefully so that the intruder is not allowed to enter the E-governance mechanism and faithful its ill-intensions thereafter. The proposed research work implements the user authentication technique and secured data transfer over the proposed E-governance mechanism using cryptographic algorithm certificate less effective key management blended with the object oriented software engineering approach.

This research implemented the user authentication technique on E-governance mechanism using object oriented modeling of CLEKM. An approach using biometric signature, based on the CLEKM is implied in E-governance. The use of CLEKM in biometric signature creation improves the electronic backing security, Aadhar, and E-voting scheme, in this technique the public and private keys are created without transmitting and any private information nowhere.

The experiments result of the proposed system in fig.6 (a)

.

Figure6. (a)

Fig.6(a) show the API for the voting scheme. The implemented technique performs encryption and decryption M the e-voting data using CL-EKM with biometric signature.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Figure 6. (b)

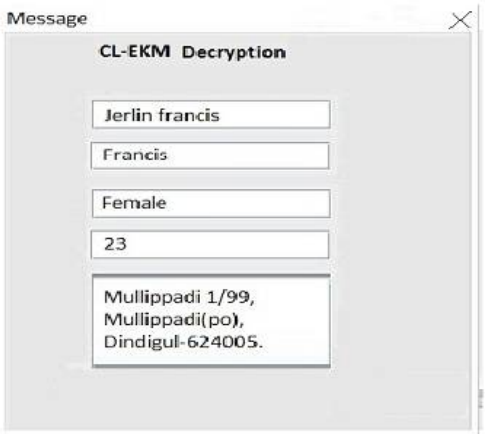

Figure 6. (c)

Fig.6 (b) shows the encrypted e-voting data by using CL-EKM with biometric signature. Fig.6 (b). Shows the encrypted E-voting data by using CL-EKM with biometric signature.Fig.6(c) shows the decrypted E-voting data by using CL-EKM with biometric security. The proposed e-governance mechanism using object oriented modeling of CL-EKM with biometric signature provides high level security over RSA and ECC.

VIII. CONCLUSION

The importance of high confidence is request for any kind of transmission of data in various department of any government sector and it is obvious in case of administrative decision and financial context. Also in many scenarios the sender government and receiver government may have a need to show their higher authority that the manage has not been altered during transmission. In this paper, the proposed CL-EKM scheme to maintain data integrity and result in more efficient. VERY SMART concept is more applicable by the proposed CL-EKM in effective manner.

REFERENCES

[1] R.kishen,KesariNikhil,P.Nithyadevi “Effective key management using CL-EKM protocol” March-April,2016,pp.250-254.
[2] D.Dayalan,S.Nandini “Certificate less effectivve key management in dynamic wireless sensor network”.
[3] RakthiV.Parthikar, “An approach for securing data in e-governance in developing countries”.
[4] D.singhKaraulia, “Information security Issues in e-governance” Dec -2011.
[5] Prokash Barman, DrBananiSaha, “Governance security using Public key cryptographic special focus on ECC”Aug-2013,pp.10-16.
[6] Mr.NikhileshBaarik, Dr.SunilKarforma, “A study on efficient digitial Signature scheme for E- governance security”.
[7] Abishek Roy, Sunil Karforma, “A study on implimentation of security in e-governance using cryptographic”,Apr-2014.
[8]. http://en.wikipedia .org.governmet to government
[9]. http://wwwshadowtech-asp.net
[10]. http://en.wikipedia.org/wiki/digitalsignature