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 5, May 2017

Anti Cyber Crime Technologies For E-Governance

D.Infanta Michael Jenifer[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 outgrowth of the efforts made by the governments to improve relations with their citizens. To protect e-governance projects there is a need for information security best practices. Cyber-crime against government is a major threat to citizen, government properties, government -plans and society. Some cybercrime risk factors on e-governance are spoofing, reproduction, disclosure of e-governance information, denial of service and elevation of privilege. This paper deals with the efficient security, cryptography, biometrics authentication, and steganography to reduce cybercrime on e-governance.

KEYWORDS: E-government, Cryptography, Cybercrime, Biometrics, Steganography.

I. INTRODUCTION

Electronic Governance is the application of information and communication technology (ICT) for delivering government services, exchange of information, communication transactions, integration of various stand-alone between government-to-systems and services between government-to-customer(G2C),governmentto business(G2B),government to government(G2G).

II.RELATED WORK

In the present day world, India has witnessed an unprecedented index of Cybercrimes whether they pertain to Trojan attacks, salami attacks, e-mail bombing, DOS attacks, information theft, or the most common offence of hacking is explained by Er. Harpreet Singh Dalla et al[2]. In this paper, they have discussed various categories of cybercrime and cybercrime as a threat to person, property, government and society. In this paper they have suggested various preventive measures to be taken to snub the cybercrime.

This paper gives an idea on E-Governance Security using public key cryptography. The public key cryptography technique called Elliptic Curve Cryptography (ECC) become popular in the last few years is explained by Prokash Barman et al[2]. In this paper, they have represent ECC using 160 bits key, provides the same security as offered by the well-known RSA using 1024 bits key, thus leading to lower processing time, minimal bandwidth use and speedy transactions. E-Governance is the application of information &communication technologies to transform the effectiveness, transparency and accountability of informational& transactional exchanges with in government, between government & government agencies of National, State, Municipal & Local levels, citizen & businesses, and to empower citizens through access & use of information is explained by MadhaviGudavalli et al[2]. In this paper they discusses the role of biometric authentication in e-governance environment to provide services efficientlyand securely over the internet.

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 5, May 2017

III. E-GOVERNANCE IN CYBER CRIME POSSIBILITIES

A. Cybercrime

Cybercrime, or **computer crime**, is crime that involvesa computer and a network. Issues surroundings these types of crimes have become high-profile, particularly those surrounding hacking , copyright infringement, child pornography, and child grooming.

B. Cyber Security

Computer security, also known as **cyber security** or **IT security**, is the protection of computer systems from the theft or damage tohardware, software or the information on them, as wellas from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware.

C. Crime on E-governance

Cyber security of e-governance projects of India is still not contemplated by Indian government. For instance, Indian government is adamant on wasting public money on illegal and unconstitutional projects like Aadhaar. After wasting many crores Indian money, it is only now that the Supreme Court of India has declared that Aadhaar card is not mandatory for availing public services in India. This paper discusses the Implementation of efficient cyber security in e-governance and Implementation of efficient cyber security. This paper also discusses about email and SMS spoofing using cryptography, smart card using biometric security, cheating and fraud avoidance using biometric authentication and prevention of misusing photograph with steganography.

IV.E-GOVERNANCE RISK FACTORS

A. Spoofing:

In this technique the attacker attempts to gain access of E-Governance system by using fallacious identity either by stealth or by using false IP address.

B. Repudiation:

The attacker can mount repudiation attack during the E–Governance transaction, which is the ability of the user to deny its performed transaction.

C. Disclosure of E-Governance Information:

Unwanted information disclosure can take place easily, in case of the compromised E-Governance system.

D. Denial of Service:

Attackers can perform Denial of Service (DoS) attack by flooding the E-Governance server with request to consume all of its resources so as crash down the system.

V. ANALYSIS ON CYBER CRIME

A. Categories on Cyber Crime

Cyber-crimes committed against persons include various crimes like transmission of child-pornography, cyber porn, harassment of a person using a computer such as through e-mail, fake escrow scams. **E-Mail Spoofing**A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates. **SMS Spoofing** is a blocking through spam which means the unwanted uninvited messages. Here an offender steals identity of another person in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cybercrime against any individual.

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 5, May 2017

VI. IMPLEMENTATION OF EFFICIENT CYBER SECURITY

A. Protection from Email and SMS Spoofing using Cryptography

Email spoofing may occur in different forms, but all have a similar result: a user receives email that appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

Prevention (Deterrence)

Use cryptographic signatures (e.g., PGP "Pretty Good Privacy" or other encryption technologies) to exchange authenticated email messages. Authenticated email provides a mechanism for ensuring that messages are from whom they appear to be, as well as ensuring that the message has not been altered in transit. Similarly, sites may wish to consider enabling SSL/TLS in their mail transfer software. Using certificates in this manner increases the amount of authentication performed when sending mail.

B. Smart Card using Biometric Security

Traditionally, ATM security the world over has relied on two-factor authentication that includes something the user has (a card or token) and something the user knows (a PIN). Biometrics solves the problem while providing the only true means of linking digital identities to "you" and determining "who" is actually using the system. While several biometric modalities have been tried at ATMs and other self-service kiosks, fingerprintand iris based biometrics has become the most widely used because of its ease of use, performance, interoperability, ability to thwart imposters, and lower cost.

C. Avoidance of Cheating and Fraud using Biometric Authentication

Cheating & Fraud means the person who is doing the act of cybercrime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.

Many of the attempts at fraud in biometric identification can be seen in films, although some of these definitely belong to world of science fiction. fingerprints using silicone or other plastics, while cutting off a person's finger or hand in order to use his/her fingerprint or hand geometry for identification purposes would only work with systems that are in the lowest range.

D. Prevention of Misusing Photograph using Steganography

Steganography

Steganography is the art of concealing messages into something innocuous in such a way that it is extremely difficult for someone to suspect, let alone find, a hidden message. Steganography masks the sensitive data in any cover media like images, audio, video over the internet. Steganography involves four steps: 1. Selection of the cover media in which the data will be hidden. 2. The secret message or information that is to be masked in the cover media. 3. A function that will be used to hide data in the cover media and its inverse to retrieve the hidden data. 4. An optional key or the password to authenticate or to hide and unhide the data [2]. The cover chosen should be done very carefully. The cover chosen should contain sufficient redundant information which can be used to hide the data, because steganography works by replacing the redundant data with the secret message.

VII. RESULTS AND DISCUSSION

In spoofing the attacker attempts to gain access of E-Governance system by using fallacious identity either by stealth or by using false IP address. Once the access is gained the attacker abuses the E-Governance system by elevation of privileges. Furthermore the attacker can mount repudiation attack during the E-Governance transaction, which is the ability of the user to deny to performed transactions. Some unwanted information disclosure can take place easily, in case of the compromised E-Governance system. Attackers can perform Denail of Service (DOS) attack by flooding the E-Governance server with request to consume all of its resources so as crash down the system.This research work implements an approach using biometric signatures, based on the ECC is implied in E-Governance. A

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 5, May 2017

multimodal Biometric security system using Elliptic key Cryptography is proposed in this research work to prevent cybercrime on E-Governance.This research also proposes to design smart card for E-Governance applications to avoid database attacks. The QR Code for the biometrics Finger Vein and Iris can be stored in the smart card itself to perform multimodal biometric security using Elliptic Key Cryptography.

Figure 1 shows the smart voter ID for Dynamic voting scheme, this dynamic voting scheme is one of the E-Governance applications, which implements conducting polling on online or web based voting.

Figure 1. A Model Biometric Secured Voter ID

Figure 2 shows the new model Debit card, which consists of the QR Code itself to perform multimodal biometric security using ECC.

Figure 2. A Model Biometric Secured Debit Card

Figure 3 shows the proposed multimodal biometric security system for E-Governance using elliptic key cryptography.

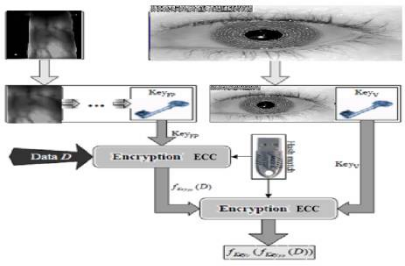

Figure 3. Architecture of Proposed Multimodal Biometric Security Scheme

In this research work, first capture the biometrics finger vein and Iris, then perform preprocessing operations to enhance the images. Figure 3 shows the input and enhanced finger print Iris images.Finger vein images are captured by using ECC imaging techniques. A promising biometric pattern for personal identification in terms of its security and convenience.Takes only about 0.8 seconds to identify one input finger vein sample. In image preprocessing the part of an image which is captured by the camera is cropped and the rest of the part is deleted. The cropped portion of that image is enhanced to achieve more clarity of the veins.

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 5, May 2017

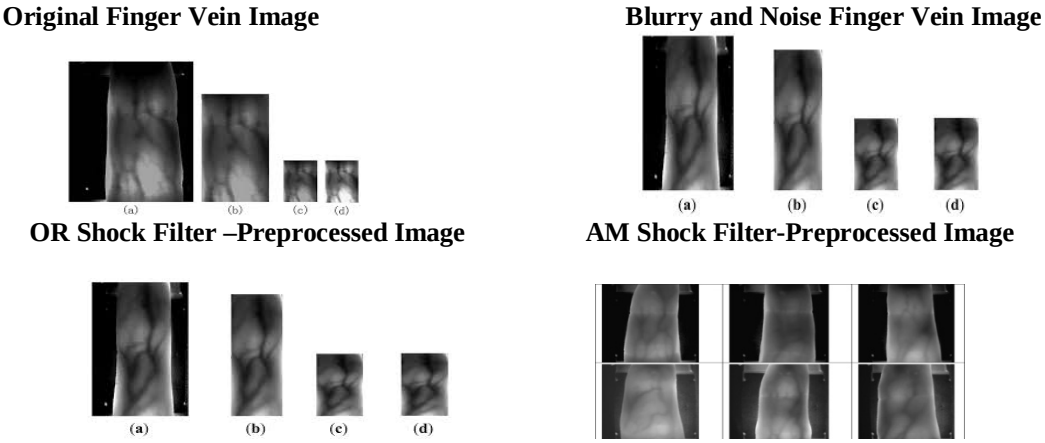

Figure 4. Preprocessing On Finger Vein Images

Image denoising an enhancement is done by OR or AM shock filter and the denoised finger vein is used for further recognition process.Figure 4 shows the preprocessed finger vein image.

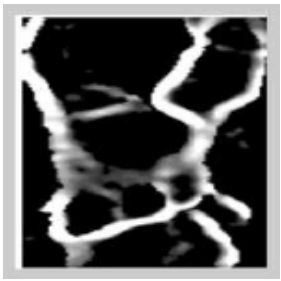

Figure5.Extracted Finger Vein Vector

After preprocessing, the features are captured from finger vein, iris and face to perform authentication. Feature vectors are extracted from finger vein for authentication.The feature vector is obtained by taking mean, standarddeviation and co-occurrence parameters.The extracted finger vein vector is shown in figure 5. Iris is thin membrane on the interior of the eyeball. Iris pattern remains unchanged after the age of two and does not degrade overtime or with the environment. Iris patterns are extremely complex than other biometric patterns.

The iris-scan process begins with a photograph. A specialized camera, typically very close to the subject, not more than three feet, uses an infrared imager to illuminate the eye and capture a very high-resolution photograph. This process takes 1 to 2 seconds. An iris recognition camera takes a black and white picture from 5 to 24 inches away. Iris recognition cannot take place without the person permission. The picture of eye first is processed by software that localizes the inner and outer boundaries of the iris. And it is encoded by image-processing technologies. Preprocessing on Iris is done by Iris Localization, Iris Normalization, Image Enhancement. In Iris Localization both the inner boundary and the outer boundary of a typical iris can be taken as circles. But the two circles are usually not co-centric. Compared with the other part of the eye, the pupil is much darker. The localization process detects the inner boundary between the pupil and the iris. The outer boundary of the iris is more difficult to detect because of the low contrast between the two sides of the boundary. And also the localization process detects the outer boundary by maximizing changes of the perimeter- normalized along the circle. The technique is found to be efficient and effective. The size of the pupil may change due to the variation of the illumination and the associated elastic deformations in the iris texture may interface with the results of pattern matching. For the purpose of accurate texture analysis, it is necessary to

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 5, May 2017

compensate this deformation. Since both the inner and outer boundaries of the iris have been detected, it is easy to map the iris ring to a rectangular block of texture of a fixed size. This is done by Iris Normalization process. The image enhancement process enhances the iris image reduce the effect of non-uniform illumination.

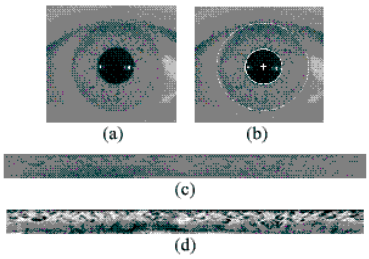

Figure 6.Iris preprocessing: (a) original eye (b) iris localization (c) iris normalization (d) image enhancement

The image enhancement process enhances the iris image reduce the effect of non-uniform illumination. The Preprocessing on Iris image is shown in figure 13.Features of iris textures are extracted using Local Binary Patterns (LBP). LBP operator forms labels for the image pixels by thresholding the neighborhood of each pixel and considering the result as a binary number. LBP provides fast feature extraction and texture classification. Due to its discriminative power and computational simplicity, the LBP texture operator has become a popular approach in various applications like image retrieval, remote sensing, biomedical image analysis, motion analysis etc…. to extract the entire iris template features. Here, LBP is used to extract the features of the normalized iris image.

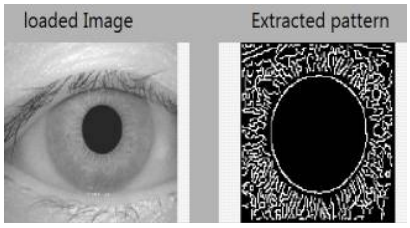

Figure 7. Texture Feature of Iris

Features of iris textures are extracted using Local Binary Patterns (LBP). LBP is used to extract the features of the normalized iris image. And so, the output of LBP is feature vectors with n dimension. The Figure 7 shows the texture feature extracted from the iris image.

Figure 8.Pattern Matching on Iris Recognition

Figure 8 is the simulated output for matching, which compares the extracted pattern of the input loaded image with patterns existing in the database. If any of the pattern is matched then it displays “Match occurred” else “No Match”.The proposed model smart cards hold the extracted biometric features in the form of QR code. Instead of using traditional PIN, the recognition process is done by using biometric features available with the smart cards. This

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 5, May 2017

proposed smart card based biometric authentication scheme for e-governance application can reduce the cyber crimes on e-governance.

A. *Steganography based Security Scheme*

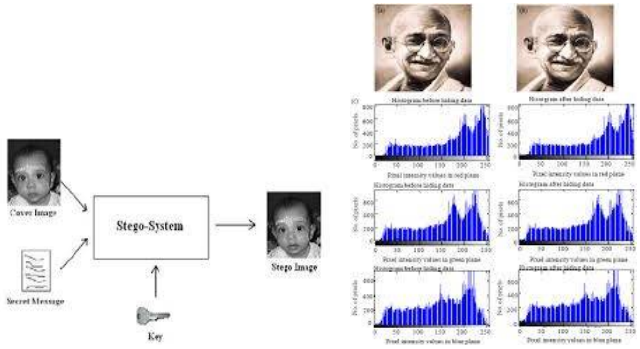

Figure 9.Architecture ofSteganography based security scheme

The main goal of steganography is to hide a message in some audio or video data, to obtain new data practically indistinguishable from data, by people, in such a way that an eavesdropper cannot detect the presence of mind. The Figure 9 shows the Architecture of Steganography based security scheme.The main goal of watermarking is to hide a message in some audio cover data, to obtain new data practically indistinguishable from, by people in such a way that an eavesdropper cannot remove or replace message in data.

VIII. CONCLUSION

E-Governance has already occupied a significant place in the global economy. Essentially actions for securing information and information systems are required to be done at different levels in the e-governance. As cyber crime is the major threat to the e-governance, certain steps should be taken at the different levels in e-governance activities. This research paper provides better solutions for cyber crime threats on e-governance. An important form of cyber crime on e-governance is identity theft, in which criminals or terrorist use the internet to steal personal information from other citizen, this type of cyber terrorism can be overcome by the proposed biometric secured smart card system. Avoidance of message spoofing and secure electronic transaction and secure electronic banking can be done by the proposed public key cryptographic algorithm using biometric signature in e-governance. This paper discusses various categories of cyber crime on e-governance and suggests various preventive measures based on biometric security, cryptography, steganography to be taken to snub the cybercrime on e-governance.

REFERENCES

[1]. Er. Harpreet Singh Dalla and Ms. Gaeta, “Cyber Crime – A Threat to Persons, Property, Government and Societies”, Volume 3, May 2013.
[2]. Kumar D and Dr. N. Panchanatham, “Case study on Cyber Security in E-Governance”, Volume 2, Nov 2015.
[3]. Abhishek Roy and Sunil Karforma, “A Study on Implementation of Security in E-Governance using Cryptography”, Volume 4, April 2014.
[4]. Prokash Barman and Dr.BananiSaha, "E-Governance Security using Public Key Cryptography special focus on ECC”, Volume 2, August 2013.
[5]. MadhaviGudavalli and Dr. D. Srinivasa Kumar, “Securing E-Governance Services through Biometrics”, Volume 8 June 2014.
[6]. Communications Fraud Control Association. 2011 global fraud loss survey. Available: http://www.cfca.org/fraudlosssurvey/,2011.
[7]. Steel. C. (2006), Windows Forensics: The Field Guide for Corporate Computer Investigations, Wiley.
[8]. Bruce Scheier., “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, Second Edition.
[9]. Wikipedia.org, http://en.wikipedia.org/wiki/RSA, Accessed on 17-10-2012.
[10]. Microsoft Technet, http://technet.microsoft.com/en-us/library/cc962035.aspx- accessed on 17-10-2012.