ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
www.computerscijournal.org

ISSN: 0974-6471
December 2011,
Vol. 4, No. (2):
Pgs. 329-339

Risk and Remedies of E-governance Systems

ABHISHEK ROY and SUNIL KARFORMA

Department of Computer Science, The University of Burdwan, W.B. (India).
*Corresponding author: Email: dr.sunilkarforma@gmail.com

(Received: July 26, 2011; Accepted: August 29, 2011)

ABSTRACT

With the advancement of Information and Communication Technology (ICT), Information has become the most easily accessible yet very valuable commodity. Since the successful implementation of various electronic mechanisms like E-Governance, E-Commerce, E-Learning, E-Health, M-Governance, M-Insurance, etc are totally dependable on the security and authenticity of the information, it is very much susceptible to interceptions and alterations caused by the hackers. In this paper the authors have done a through study of the various risk factors of the information security and their probable remedies using various cryptographic algorithms so that the above mentioned E-mechanisms can be implemented with utmost Privacy, Integrity, Non-Repudiation and Authentication (PINA).

Key words: Authentication, Cryptography, Information Security, Interception, Integrity, Non-Repudiation, Privacy.

INTRODUCTION

Recent rapid technological advancements have made Information and Communication Technology (ICT), especially Internet as the vast storage medium of Information which is cheaply accessible to the populace. This easy accessibility feature has its advantages as well as disadvantages. As far as the advantages are counted, various electronic transaction systems such as E-Governance, E-Commerce, E-Learning, E-Health, M-Governance, M-Commerce, M-Insurance, etc have evolved nowadays. Whereas the threat perceptions established from the hackers and intruders, makes the information very much vulnerable to unauthenticated access and alterations. They are attacking directly or indirectly during transactions in E-Governance. Direct tampering of information is caused by the active attacks. Indirect tampering of information, like finding the loopholes of TCP/IP model, is caused by the passive attacks. Intruders are attacking the E-Governance system by performing alterations, modifications, stealing of vital information. Focusing on this present scenario the authors have done a through discussion of the various risk factors of information security in E-Governance system and their probable remedies using various cryptographic algorithms.

Section-2 discusses the various risk factors in E-Governance. The probable remedies are mentioned in the section-3. Conclusion drawn from the overall discussions is stated in section-4. References are cited in section-5.

Risks in e-governance systems

In this section we will be discussing various risks factors present in E-Governance [58, 59] system. Any type of digitalized information faces threat perceptions from the view point of interceptions and unauthorized alterations during transmission through Internet. It becomes mandatory for the concerned authority to impose Privacy, Integrity, Non-Repudiation and Authentication (PINA) of Information to ensure successful functioning of E-Governance. An unauthenticated user when accesses the information, then its privacy is severely infringed. This breaching leads to either active hacking or passive hacking. In passive hacking the intruder just listen the information. But in case of active hacking, the intruder listens as well as tampers it according to the requirement, which ultimately violets the integrity of the information. To achieve Non-repudiation feature, the Information must be transmitted securely in such a manner that the actual sender of the message fails to deny its origin. Authentication of the information is established only when the origin of the message passes the verification test.

Modus operandi of attackers

In E-Governance, Information is vulnerable to threats from the hackers and their corresponding attacks. As mentioned earlier these attacks can be either active or passive one. In both the cases specific algorithm is followed to breach the security of the Information. The modus operandi of the intruders can be categorized as follows –

a. Survey and assess
b. Exploit and penetrate
c. Escalate privileges
d. Maintain access
e. Prevent access.

Firstly the attacker performs the survey work to assess the characteristics of the target object. Having gathered sufficient information, the attacker tries to exploit and penetrate the application by finding the loop holes of the network host and TCP/IP models. After the application is compromised the attacker immediately attempt to escalate high level privileges. Having gained the access, the attacker takes initiative to maintain the access in future by covering the tracks. Even the attackers who cannot gain access to the system mount attack to prevent the access of other users.

The threat perceptions that persists during the E-Governance transactions can be technically categorized into followings –

Spoofing

In this technique the attacker attempts to gain the access of the 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 the privileges.

Tampering of E-Governance system

As soon as the system is compromised and privileges are raised, the classified information of the E-Governance mechanism becomes very much vulnerable to unauthorized alterations.

Repudiation

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

Disclosure of E-Governance Information

In case of the compromised E-Governance system, the unwanted information disclosure can take place very easily.

Denial of Service

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

Elevation of privilege

Once an E-Governance system is compromised; the attacker pretending to be a low profile user attempts to escalate to the high profiles so as to access its privileges to initiate further damage to the system.

Cyber Crimes

As a side effect of speedy up-gradations of science and technology, the cyber crime rates has obtained a gallop and it has figured as a menace to the transactions accomplished between the Government and its Citizenry within the E-

Governance methodology. This menace can be defined into following categories –

Threat to Citizenry

Citizens on the Internet may face the following types of threats

False or Malicious Website

These websites are build up purposefully to steal the Citizen's important information like, ID, password, credit or debit card information, spying on hard drive. Bugs such as Freiburg Bug helps to spy on a visitor's system hard drive and upload files from there.

Theft of Citizens' information from intermediary agents and ISPs

Citizens may take the help of the Internet Service Providers (ISPs) and other intermediate agents while performing online financial transactions like online tax payment, online ticket booking, etc. Hackers may break into the systems of the agents and ISPs to obtain the Citizen's information.

Violation of Citizen's Privacy through the use of Cookies

Cookies are piece of information that a website transfer on a user's system hard drive for the maintenance of the record. The use of these cookies to extract the information is also a threat to the privacy of the Citizens.

Spamming and Flaming

Spamming is the indiscriminate sending of unsolicited email messages to Internet users. Cyber criminals use this method to spread computer viruses to the systems of the Citizen.

Threat to the Governmental agencies

Alike the Citizens, the Government agencies also faces the risk from the attackers –

Citizen impersonation

In this technique the attacker pretends to be the legitimate Citizen and execute the E-Governance transactions.

Ping of Death

Ping of Death is the technique to send large number of data packets to the E-Governance server using ping command. Since the TCP/IP model will fail to handle that huge amount of data packets, the server will be left with no other options but to crash down or reboot or hang.

Teardrop

The Teardrop attack exploits the vulnerability present in the reassembling of data packets. During E-Governance transactions the data packets sent over the Internet are broken down into smaller fragments and put together at the destination system. These packets have an offset field in their TCP header part which specifies from which byte to which byte does the particular data packet is carrying the data. In the Teardrop attack, a series of data packets are sent to the target E-Governance server with overlapping offset field values. As a result, the target system fails to reassemble the packets and is forced to crash down, reboot or hang.

Intranet associated threats

An Intranet is a network inside an organization that uses the Internet technologies to facilitate Information sharing within the organization. E-Governance agencies may face threats from within the organization. Internal hackers are more troublesome because they have a potential wealth of information by using which they go ahead in designing malicious scheme.

Risks associated with data transmission during E-Governance transactions

The information transmitted in the Internet is broken into data packets which may travel over different routes to reach the destination. The most vulnerable point of interception of Information is the points of entry to and exit from the Internet.

Risks associated with stored online E-Governance Information

Many E-Governance server stores information which may be under the surveillance of intruders.

Risk associated with malicious code

Insertion of malicious code such as virus, worms and Trojan horses can result in E-Governance server down time. A Virus is a malicious

Table 1: Illustration of Brute Force Attack

Key (bits)	Permutation	Brute-force time for a device checking 2^{56} permutations per second
8	2^{8}	0 milliseconds
40	2^{40}	0.015 milliseconds
56	2^{56}	1 second
64	2^{64}	4 minutes 16 seconds
128	2^{128}	149,745,258,842,898 years
256	2^{256}	50,955,671,114,250,100,000,000,000,000,000,000,000,000,000,000,000,000,000 years

program that replicates itself in some form and performs un-requested, many a times destructive acts. A Worm differs from a virus in that it is a distinct program that can run unaided, whereas a virus program can not run without being inserted into another program. Trojan horse is another type of malicious codes that damage or destruct files. However Trojan horses are different from viruses in that they do not replicate, instead they sneak into the server by attacking a legitimate program. When the affected program is executed, the Trojan horse starts its destructive functioning.

The well known attacks which has become the matter of great concern for various E-Governance schemes can be enlisted below –

Brute force attack

Brute Force Attack[1] or Exhaustive Key Search [2] being an application of Brute Force Search is a Known Plaintext Attack (KPA)[6] which requires little bit cipher text and corresponding plaintext. In case of block cipher, cryptanalyst requires a block of cipher text and the corresponding plain text. In this technique, the correct key is found by checking all possible keys systematically. The practical feasibility factor of this attack depends on the key length used for encryption purpose. The success rate of this attack depends on the number of keys to be tested and the speed of per key test. Brute Force Attack is specially made for parallel processors as these processors can separately test a subset of keyspace. Moreover these processors do not have to communicate among each other except for the success of the attack. It proves beneficial for the Brute Force Attack as it is easy to design a machine with million parallel processors which do not need to have shared memory locations. To make this attack infeasible, key with long key length must be selected. For example, the system which could brute-force a 56-bit encryption key in one second, would take 149.7 trillion years to brute-force a 128-bit encryption key[2]. The following table illustrates the example more clearly –

Two emerging technologies capable of performing successful brute force attack based on parallel processing are Graphics Processing Unit (GPU) and Field Programmable Gate Array (FPGA). GPUs benefit from their availability, FPGAs from their energy efficiency per cryptographic operation. The COPACOBANA FPGA Cluster computer which consumes the same energy as a single PC (600 W), but performs like 2,500 for certain algorithms can be cited as an efficient example of FPGA technology. Though Electronic Frontier Foundation (EFF) [2] performs customized hardware attack by developing FPGA clusters, there still remains the question of justification with respect to the feasibility factor related to cost estimation.

Boomerang attack

David Wagner introduced Boomerang Attack[8,12,57] to COCONUT98 cipher in 1999. Boomerang Attack which is further modified as Amplified Boomerang Attack and Rectangle Attack is based on Differential Cryptanalysis[9-11]. Differential Cryptanalysis is a study which depicts how the differences in input can affect the resultant difference in the output. In this method the pair of plain-text and cipher-text having constant difference is find out and then the differential behavior of the cryptosystem is investigated. In Boomerang Attack these differentials are used which cover the part of the cipher-text. In this technique two short differentials with high probabilities are used instead of one differential of more rounds with low probability.

Davies' attack

Donald Davies introduced a dedicated statistical cryptanalytic method for breaking Data Encryption Standard (DES) cryptosystems called Davies' Attack[13-14]. This Known Plaintext Attack (KPA) is based on the non-uniform distribution of the outputs of pairs of adjacent Substitution-boxes [15]. In Davies' Attack the empirical distribution of the collected pair of plain-text and their corresponding cipher-text is conducted to perform the cryptanalysis.

Birthday attack

Birthday Attack[16-17] refers to a class of brute force attack which uses the mathematical derivations of Birthday Problem in probability theory to reduce the complexity of cracking a hash function. Birthday Problem [18] states that there is a probability, that in a set of *n* randomly chosen people, some pair of them will have common birthday. According to this theory the probability reaches, 100% when the people count is 366 (excluding February 29 births), 99% when people count is 57, and 50% when people count is 23. These conclusions are driven from the assumption that each day in a year (except February 29) may be a probable birthday. For a given function *f*, the objective is to find two different inputs *a, b* such that –

$f(a) = f(b)$ where the pair *a, b* is termed as Collision.

The function *f* is evaluated over randomly chosen inputs unless same result is obtained more than once.

Meet-in-the-middle attack

Meet-in-the-Middle Attack[19-21] is an advanced type of Known Plaintext Attack (KPA) which is used to decipher the cryptosystems which are designed with more secure algorithms like 3DES. In this technique the cryptanalyst finds the a value in the domain of the composition of two functions so that the forward mapping of one through the first function is same as the inverse of the other through the second function so that the meeting is possible in the middle of the composite function. For a known pair of plain-text *P* and cipher-text *C*, the cryptanalyst can perform the following operation: $C=E_{k2}(E_{k1}(P))$, where *E* is the encryption function and *k1* and *k2* are the keys. On further calculation of $E_k(P)$ and $D_k(C)$ where *D* is the decryption function, the matches between the results obtained will reveal the correct key. Once matches are found, verification is be done by second test-set of plain-text and cipher-text.

Related-key attack[3]

In Related-Key Attack[22], the cryptanalyst performs the attack with several keys whose initial values are unknown but their mathematical relationship is known. Wired Equivalent Privacy (WEP) cryptographic protocol used in Wi-Fi wireless networks have been successfully encountered by Related-Key Attack. To defend Related-Key Attack the cryptosystems should be engineered in such a manner that the encryption keys will never have a slightest relation among themselves.

Slide attack

Slide Attack[23, 24] is a typical cryptanalytic approach first designed by David Wagner and Alex Biryukov in 1999. In cryptography, weak ciphers can become strong cipher by increasing the number of rounds during encryption process which can even defend the differential attacks In Slide Attack, the number of rounds involved in the encryption process are made irrelevant as it explores the weakness of the encryption process by analyzing the key schedule specifically those which are repeating in the cyclic manner. Since the cipher-text is broken in multiple rounds of identical functions *F* which is prone to Known Plain-text Attack. This Slide Attack has close acquaintance with Related Key Attack.

XSL attack

eXtended Sparse Linearization (XSL) Attack[25-27] designed by Nicolas Courtois and Josef Pieprzyk in 2002, is meant for the block ciphers like Advanced Encryption Standard (AES) algorithm. This technique analyses the internals of a cipher-text and derive a pattern of quadratic simultaneous equations which are typically very large in size. Then Extended Sparse Linearization algorithm is applied to solve these equations for retrieval of the key.

Rainbow table

Rainbow Table[28] is a predefined table used for cracking the cryptographic hash functions. This table recovers the plaintext password, up to a limited set of characters. It is a form of time-memory tradeoff, using less CPU at the cost of more storage. This approach fails against one-way hashes that include random bits used for creation of one of the inputs of one-way function, called salts.

Timing attack

Timing Attack[29-31] is a side-channel attack which attempts to break the cryptosystem by backward analysis of the time consumed to accomplish the cryptographic algorithm. Because of performance optimizations, computations performed by a cryptographic algorithm often take different amounts of time depending on the input and the value of the secret parameter. This approach is basically used over weak computing devices like smart cards.

Man-in-the-middle attack

Man-in-the-Middle Attack (MITM)[32-33] or Bucket Brigade Attack or Session Hijacking is a technique where the intruder listens the transmission and send the tampered message to the original recipient in behalf of the original sender. Acting on the received message when recipient replies the sender; again intruder intercepts the message and sends the tampered version to the sender on behalf of the recipient. In this way both the sender and receiver remain unaware of the attack for the entire transmission. This cryptanalytic attack is particularly applicable to the original Diffie-Hellman key exchange protocol, when used without authentication.

Replay attack

Replay Attack[34-36] is an example of typical network attack where the valid data transmission is spitefully repeated or altered. This attack is executed either by the originator or the intruder who intercepts the data and retransmits it. Transmission of pseudo-randomly generated session tokens during the encryption process can defend the Replay Attack as the intruder will fail to guess the future tokens. Apart from pseudo-random generation of session token, the synchronized time-stamping technique using secure protocol can also defend the Replay Attack.

Denial-of-service (DoS) attack

In Denial of Service (DoS) Attack[37], the attacker prevents the actual user from accessing information or services by flooding network traffic with information. When a user wants to access information from Internet, the attacker identifies the target computer and its network connection and overloads the destination server with huge amount of request so that the request send by the actual user is rejected by the destination web server. By sending spam emails the attacker can also execute Denial of Service (DoS) Attack as the specific storage capacity of the email account is consumed by the spam mails thereby preventing the actual user from receiving legitimate messages.

Distributed denial of service (DDoS) attack

Distributed Denial of Service (DDoS) Attack[38-40] is a variation of Denial of Service (DoS) Attack where the attacker remotely controls the compromised computers thereby launching Denial of Service (DoS) Attack over the victim's computer in a "distributed" fashion. Unfortunately there are no effective ways to prevent the Denial of Service (DoS) Attack and Distributed Denial of Service (DDoS) Attack. Installation of anti-virus software and firewalls to restrict the incoming, outgoing traffic and port maintenance of the computer can prevent a user from these types of attacks up to some extent.

Counter measures to minimize risks

From the above discussions it is crystal clear that security features of Information needs the maximum attention of the researchers in the field of E-Governance. And to neutralize these risk factors tough cryptographic applications must be implemented. Secret Key Cryptography (SKC)[56], Public Key Cryptography (PKC), Digital Signature (DS), Digital Certificate (DC), Digital Watermarking[44], Steganography[45], Biometric authentication[63], Elliptic Curve Cryptography (ECC)[43, 46-51], Hash Functions[52-54], Firewalls [55], Antivirus Software, Anti Spyware Software are among those few which worth mentioning in subsequent phases.

Secret Key Cryptography (SKC) is a primitive cryptographic algorithm where the encryption key can be calculated from the decryption key and vice versa. In most of the cases the encryption and decryption key are same. Key is typically hundred of bits in length which have a defined set of instructions for completion of the cryptographic operations. The strength of these Symmetric algorithms depends on the secrecy of the key, whose divulgence will lead to the easy crash down of the cryptosystem. Algorithms like IDEA, AES, etc can be implemented with further modifications to strengthen the secret key cryptosystems of E-Governance. If *M* represents plain-text, *C* represents cipher-text, *E* represents encryption function, *D* represents decryption function and *K* represents the key, the encryption and decryption process in the Symmetric Key or Secret Key Cryptography can be shown as follows –

Encryption: $E_K (M) = C$
Decryption: $D_K (C) = M$

Public Key Cryptography[41] is the art and science of encryption and decryption where each communicating devices have a pair of keys, a private key and a public key. The private key is strictly known to the particular user whereas the public key is distributed to all users taking part in the communication. As the knowledge of public key does not compromise the security of the algorithms; it can be easily exchanged online. In this way a shared secret can be established between two communicating parties by exchanging only public keys. Any third party, having access only to the exchanged public information, will be unable to calculate the shared secret unless it has access to the private key of any of the communicating parties. The private key and public key of a cryptosystem are interlinked to each other with the help of One-Way mathematical functions, where forward operation is easily possible but the reverse operation is almost impossible. In public key cryptography the forward operation of the one-way mathematical function is performed using the private key to obtain the public key. The particular cryptosystem is assumed to be compromised if the private key is obtained easily from the public key by performing the reverse operation of the one-way functions. This chance gets reduced if the key size is increased. Variations of RSA, DSA encryption algorithms like ECRSA, ECDSA, etc have eminent scope of application in the domain of E-Governance. If *M* represents plain-text, *C* represents cipher-text, *E* represents encryption function, *D* represents decryption function, *K1* represents the encryption key and *K2* represents the decryption key, the encryption and decryption process in the Public Key Cryptography can be shown as follows –

Encryption: $E_{K1} (M) = C$
Decryption: $D_{K2} (C) = M; D_{K2} (E_{K1} (M)) = M$ where $K1 \neq K2.$

Digital Signature[42] is the mechanism to authenticate a message. This technique proves that a message is effectively coming from the legitimate sender only, by signing it with the private key. Any user that has got the access to the corresponding public key can verify the signature. Thus the receiver can ensure that the message is indeed signed by the intended sender and is not modified during the transit. In case of modification of data, the signature verification test is sure to be failed.

For the successful transmission of data in a network an authority must be considered to be trusted by all devices. This trusted Certificate Authority (CA) digitally signs the public keys and the unique identifiers of all devices. These signed data (public key, IDs etc.) along with the signature arranged in a standard format is called the Digital certificate. All the devices that take part in secured and trusted communication have to obtain a certificate from the trusted authority. RCAI, NIC, TCS, MTNL, etc are among the prime certificate issuing authorities in India.

Digital Watermarking is the process of embedding information into digital multimedia content i.e still image data, audio data and video data such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. A digital watermark can be visible or invisible. A visible watermark typically consists of a conspicuously visible message or a company logo indicating the ownership of the data. On the other hand, an invisibly watermarked image appears very similar to the original. The existence of an invisible watermark can only be determined using an appropriate watermark extraction or detection algorithm which consists of encoding and decoding process. More initiatives need to be generated for protecting the Digital Rights Management (DRM)[61-62] of digitalized E-Governance information which is vulnerable to various cryptanalytic attacks.

Steganography is the art and science of secret communication

The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Steganography is often confused with cryptography as both are similar in the way that they both are used to protect confidential information. The difference between the two is in the appearance in the processed output; the output of steganography operation is not apparently visible but in cryptography the output is scrambled so that it can draw attention. Steganlysis is the process to detect the presence of steganography. Various steganographic algorithms like Jsteg, F3, F4, F5[60], etc have huge scope of application in the domain of E-Governance.

Biometric authentication is another tough method to protect the E-Governance cryptosystems against attacks. This is an advanced technique of human identification based on biometric identifiers like, fingerprints, iris, voice, gait, etc. The advantage with this technique is that once these biometric identifiers are collected, it can not be forgotten, which may happen in the case of computer generated passwords. Generally there are two phases in this Biometric authentication technique – Enrollment phase and Authentication phase. In the Enrollment phase, the biometric templates are collected and stored from the Citizens. In the Authentication phase, the new information is matched with the information previously stored in the database. If the match is found, the Citizen is allowed to access the E-Governance mechanism, and in case of failure, the intruder is prevented from the access. Recently in the Birbhum district of West Bengal, India, this technique has been applied as a pilot project for distribution of Job Card to the rural populace under National Rural Employment Guarantee Act (NREGA) scheme.

Elliptical Curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. An elliptic curve is not an ellipse (oval shape), but is represented as a looping line intersecting two axes (lines on a graph used to indicate the position of a point). ECC is based on properties of a particular type of equation created from the mathematical group (a set of values for which operations can be performed on any two members of the group to produce a third member) derived from points where the line intersects the axes. Multiplying a point on the curve by a number will produce another point on the curve, but it is very difficult to find what number was used, even if you know the original point and the result. Equations based on elliptic curves have a characteristic that is very valuable for cryptography purposes: they are relatively easy to perform, and extremely difficult to reverse.

Hashing, in cryptography, is a one-way operation that is performed by the Hash Functions which transforms a stream of data into a more compressed form called a Message Digest. The operation is not being invertible, meaning that recovering the original data stream from the message digest should not be possible. All the message digests or hash values generated by a given hash function have the same size no matter what the size of the input value is.

Firewalls are like locks which acts as barriers to attacks. These dedicated gateway machines filters the incoming traffic to the own network from the other network and also controls the outgoing traffic to the other network. There are two main types of firewalls: network firewalls and host-based firewalls. Network firewalls, such as the software-based Microsoft’s Internet Security and Acceleration (ISA) Server or the hardware-based Nortel Networks Alteon Switched Firewall System, protect the perimeter of a network by watching traffic that enters and leaves. Host-based firewalls, such as Internet Connection Firewall (ICF—included with Windows XP and Windows Server 2003), protect an individual computer regardless of the network it's connected to.

Antivirus and Anti-spyware software are used to prevent, detect and remove the malicious codes like virus, worms, Trojan horse, etc from the system to ensure its proper functioning. These malicious codes are generally launched by the attackers to compromise the target system and materialize their ill intensions.

Online Brute Force Attack can be handled by the system administrators by limiting the number of attempts that a password can be tried, by introducing time delays between successive attempts and locking accounts out after unsuccessful logon attempts. Even the website administrators may prevent a particular IP address from trying more than a predetermined number of password attempts against any account on the site. Alternative study of AES key schedule can be considered as the counter measure of the Boomerang Attack. The use of Hashed Message Authentication Codes (HMACs) during encryption process can be thought of as the countermeasure of Man-in-the-Middle Attack, as alterations can be identified by the recalculation of HMAC at the recipient's end. Installation and configuration of firewalls and Virtual Private Network (VPN), deployment of Network based Intrusion Detection (NID) or Network Intrusion Prevention Systems (NIPS) devices becomes mandatory for tackling Denial of Service Attack, Distributed Denial of Service Attack, Birthday Attack, Replay Attack. Implementation of proper user authentication, input validation, parameter checking, exception management, etc must be done to defend various attacks like Davies Attack, Related Key Attack, Meet-in-the-Middle Attack, Slide Attack, XSL Attack and Timing Attack.

CONCLUSION

In spite of the successful existence of present days cryptanalytic attacks, the attackers are under constant enhancement using all possible ways. Cipher-text Only Attack (COA)[4] or Known Cipher-text Attack is cryptanalysis models which presume that attacker have access only to the set of cipher-text. Frequency Analysis[5] is a statistical technique developed by the cryptographers to perform successful cipher-text attack over classical ciphers. In this technique the frequency of letters or group of letters are measured in the cipher-text. In Known Plaintext Attack (KPA) the cryptanalyst have access to a sample of cipher-text and its corresponding plain-text. In Chosen-Plaintext Attack, the cryptanalyst can choose the plain-text and its respective cipher-text. The Adaptive-Chosen-Plain-text Attack [7] is a modification of Chosen-Plaintext Attack where the cryptanalyst chooses the plain-text and then its cipher-text from the samples of plain-text selected dynamically. In Chosen-Cipher-text Attack, the cryptanalyst chooses the cipher-text and tries to decrypt it. In Adaptive-Chosen-Cipher-text Attack, the cryptanalyst chooses the cipher-text from the dynamically selected samples of cipher-text and tries to decrypt it. To encounter these future threats advanced cryptographic techniques like Elliptic Curve Cryptography (ECC) embedded with Digital Signatures like RSA Digital Signatures, El Gamal Digital Signature, etc must be engineered using object oriented approach to obtain optimum outputs from the E-Governance mechanism.

REFERENCES

1. Bruce Schneier: Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth), Publisher: John Wiley & Sons, Inc., ISBN: 0471128457.
2. http://en.wikipedia.org/wiki/Brute-force_attack Date of access: 01st August, 2011.
3. http://en.wikipedia.org/wiki/Cryptanalysis Date of access: 01st August, 2011.
4. http://en.wikipedia.org/wiki/Ciphertext-

only_attack Date of access: 01st August, 2011.

5. http://en.wikipedia.org/wiki/Frequency_analysis Date of access: 01st August, 2011.
6. http://en.wikipedia.org/wiki/Known-plaintext_attack Date of access: 01st August, 2011.
7. http://www.rsa.com/rsalabs/node.asp?id=2201 Date of access: 01st August, 2011.
8. http://en.wikipedia.org/wiki/Boomerang_attack Date of access: 01st August, 2011.
9. http://islab.oregonstate.edu/koc/ece575/notes/dc1.pdf Date of access: 01st August, 2011.
10. http://en.wikipedia.org/wiki/Differential_cryptanalysis Date of access: 01st August, 2011.
11. http://tuvalu.santafe.edu/~hag/crypto/node22.html Date of access: 01st August, 2011.
12. http://www.iacr.org/archive/fse2002/23650001/23650001.pdf Date of access: 01st August, 2011.
13. http://webcourse.cs.technion.ac.il/236612/Spring2007/ho/WCFiles/adv-crypto-slides-07-idavies.1x1.pdf Date of access: 01st August, 2011.
14. http://en.wikipedia.org/wiki/Davies%27_attack Date of access: 01st August, 2011.
15. http://en.wikipedia.org/wiki/Substitution_box Date of access: 01st August, 2011.
16. http://www.rsa.com/rsalabs/node.asp?id=2205 Date of access: 01st August, 2011.
17. http://en.wikipedia.org/wiki/Birthday_attack Date of access: 01st August, 2011.
18. http://en.wikipedia.org/wiki/Birthday_problem Date of access: 01st August, 2011.
19. http://eprint.iacr.org/2011/201.pdf Date of access: 01st August, 2011.
20. http://en.wikibooks.org/wiki/Cryptography/Meet_In_The_Middle_Attack. Date of access: 01st August, 2011.
21. http://en.wikipedia.org/wiki/Meet-in-the-middle_attack Date of access: 01st August, 2011.
22. http://www.impic.org/papers/Aes-192-256.pdf Date of access: 01st August, 2011.
23. http://www.cs.berkeley.edu/~isabelle/slideattacks.pdf Date of access: 01st August, 2011.
24. http://www.eee.metu.edu.tr/~yucel/SlideAttack.pdf Date of access: 01st August, 2011.
25. http://www.math.iastate.edu/thesisarchive/MST/KleimanMSTSS05.pdf Date of access: 01st August, 2011.
26. http://www1.spms.ntu.edu.sg/~kkhoongm/xsl_bes.pdf Date of access: 01st August, 2011.
27. http://www.quadibloc.com/crypto/co4514.htm Date of access: 01st August, 2011.
28. http://kestas.kuliukas.com/RainbowTables/ Date of access: 01st August, 2011.
29. http://crypto.stanford.edu/~dabo/papers/ssl-timing.pdf Date of access: 01st August, 2011.
30. http://www.cs.sjsu.edu/faculty/stamp/students/article.html Date of access: 01st August, 2011.
31. http://www.cryptography.com/public/pdf/TimingAttacks.pdf Date of access: 01st August, 2011.
32. http://cryptodox.com/Man-in-the-middle_attack Date of access: 01st August, 2011.
33. http://msdn.microsoft.com/en-us/library/ff648641.aspx Date of access: 01st August, 2011.
34. http://www.cs.uml.edu/~xinwenfu/paper/ICC08_Fu.pdf Date of access: 01st August, 2011.
35. http://msdn.microsoft.com/en-us/library/aa738652.aspx Date of access: 01st August, 2011.
36. http://cryptodox.com/Replay_attack Date of access: 01st August, 2011.
37. http://www.us-cert.gov/cas/tips/ST04-015.html Date of access: 01st August, 2011.
38. http://staff.washington.edu/dittrich/misc/ddos/ Date of access: 01st August, 2011.
39. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html. Date of access: 01st August, 2011.
40. http://www.jmu.edu/computing/security/info/archived/ddos.shtml Date of access:01st August, 2011
41. http://www.tataelxsi.com/whitepapers/

pub_key2.pdf?pdf_id=public_key_TEL.pdf Date of access: 01st August, 2011

42. http://www.cgi.com/files/white-papers/cgi_whpr_35_pki_e.pdf Date of access: 01st August, 2011

43. http://hosteddocs.ittoolbox.com/AN1.5.07.pdf Date of access: 01st August, 2011

44. http://citeseerx.ist.psu.edu/viewdoc/download?doi= 10.1.1.84.6722&rep=rep1&type=pdf. Date of access: 01st August, 2011.

45. http://www.tifr.res.in/~sanyal/papers/Soumyendu_Steganography_Steganalysis_ different_approaches.pdf Date of access: 01st August, 2011.

46. http://www.secg.org/collateral/sec1_final.pdf Date of access: 01st August, 2011.

47. http://www.rsa.com/rsalabs/node.asp?id=2013 Date of access: 01st August, 2011.

48. http://www.eccworkshop.org/ Date of access: 01st August, 2011.

49. http://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography. Date of access: 01st August, 2011.

50. http://www.cis.syr.edu/courses/cis428/slides/elliptic.pdf Date of access: 01st August, 2011.

51. http://citeseerx.ist.psu.edu/viewdoc/download? doi=10.1.1.174.4365& rep=rep1 &type=pdf. Date of access: 01st August, 2011.

52. https://bora.uib.no/bitstream/1956/3206/1/47401627.pdf Date of access: 01st August, 2011.

53. http://www.cs.ucdavis.edu/~rogaway/papers/relates.pdf Date of access: 01st August, 2011.

54. http://www.sans.edu/research/security-laboratory/article/hash-functions. Date of access: 01st August, 2011.

55. http://technet.microsoft.com/en-us/library/cc700820.aspx Date of access: 01st August, 2011.

56. http://www.cse.wustl.edu/~jain/cse571-07/ftp/l_05skc.pdf Date of access: 01st August, 2011.

57. http://eprint.iacr.org/2011/072.pdf Date of access: 01st August, 2011.

58. Sur C, Roy A, Banik S, *A Study of the State of E-Governance in India*, Proceedings of National Conference on Computing & Systems (NACCS) – 2010, January 29, 2010, pp: (a)-(h), Organized by: Department of Computer Science, The Univrsity of Burdwan. ISBN: 8190-77417-4

59. 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 (ICCS)- 2010, November 19-20, pp: 263-269 (2010), Organized by Department of Computer Science, The University of Burdwan, ISBN: 93-80813-01-5.

60. Westfeld A, *F5 - A Steganographic Algorithm,* Proceedings of 4th International Workshop on Information Hiding, Springer-Verlag London, UK ©2001, ISBN: 3-540-42733-3.

61. Banerjee S, Karforma S, "A Prototype Design for DRM based Credit Card Transaction in E-Commerce", ACM Ubiquity, **9**(18): 1-9 (2008).

62. http://www.aicit.org/jdcta/ppl/26_JDCTA_March_2-29.pdf Date of access: 01st August, 2011.

63. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.4.7263&rep=rep1&type=pdf Date of access: 01st August, 2011.