International Journal of Education and Science Research Review
E-ISSN 2348-6457
Volume-9, Issue-3 May-June- 2022
P-ISSN 2349-1817
www.ijesrr.org
Email- editor@ijesrr.org

INFORMATION SECURITY IN E GOVERNANCE USING CRYPTOGRAPHY

Unnamalai K

Assistant Professor

Department of Computer Science

Anna Adarsh College For Woman

ABSTRACT

This article offers some thoughts on how public key cryptography might be used to make e-government more secure. When it comes to e-governance, security is one of the most critical concerns. E-governance may make use of each and every security method that is traditionally employed in online commerce. However, electronic governance and online business operate in quite distinct ways. Elliptic Curve Cryptography, sometimes known as ECC, is a kind of public key cryptography that has been more popular over the past several years. The fact that it presents an exponentially greater difficulty to an intruder in terms of time is the primary selling point of exponentially stronger cryptography (ECC). ECC provides the same level of security that the more well-known RSA algorithm does when it's utilising a key with 1024 bits, but it only needs 160 bits, which results in significantly less time spent processing data, less strain on the network, and faster transactions.

Keywords: *E Governance, Security, Cryptography*

INTRODUCTION

As a result of the ongoing economic crisis on a worldwide scale, governments in developing nations are currently confronted with significant difficulties in running their organisations effectively while adhering to fiscal constraints. For the sake of the general socioeconomic growth of the state, the government may choose to take use of the many benefits offered by information and communication technology (ICT) in order to deliver excellent governance to the people of the state. Since all of the message transmission that occurs during Electronic Governance, also known as EGovernance, takes place over a public communication channel, such as the Internet, it is extremely vulnerable to being intercepted by those who wish to undermine it. Message transmission should be carried out via encryption and decryption techniques of cryptography, which is the art and science of keeping the communications hidden from the unauthorised access. This will allow for the consistency of these systems to be maintained, which is extremely important. Cryptographers are the experts who practise this particular branch of mathematics and science. Cryptographers are able to transform the plain text into the encrypted text that corresponds to it by employing these approaches in conjunction with a cryptographic algorithm. A particular algorithm may be used to decode the encrypted text in order to recover the plain text that corresponds to it. This can take place at the same time. The whole process of encrypting and decrypting the plain text is predicated on a specific parameter called the Key. The Key is a specific sequence of bits that is only known to the legitimate sender of the message and the valid receiver of the message. Utilizing this strategy, the legitimate sender can encrypt the plain text by using this key, and then send the encrypted message across the Internet. Concurrently, the person who is authorised to receive the communication will be given the encrypted

message, and then they will be able to decode it using the chosen key in order to obtain the plain text. It is exactly the same as making a public handoff of a valuable object from the sender to the recipient while maintaining the security of a lock and key system. It is referred to as Secret Key Cryptography (SKC) when the process of encrypting and decrypting a message is carried out with a single key, known as the Secret Key; however, it is referred to as Public Key Cryptography when the process is carried out with a pair of keys, known respectively as the Public Key and the Private Key (PKC). When it comes to the type of cryptography known as Secret Key Cryptography (SKC), the success of the cryptosystem is totally dependent on the key's level of secrecy. This is because the entire operation is carried out using a single key. If the Secret Key of a cryptosystem that uses Secret Key Cryptography (SKC) is revealed in any way, then it is safe to conclude that the security of the system has been breached. In the context of Public Key Cryptography (PKC), the Private Key is something that is solely known to a single participant, whereas the Public Key is something that is accessible to the whole public. The Public Key is distinguished from other keys in that it does not jeopardise the safety of the algorithms and, as a result, it may be simply disseminated across the internet. Therefore, a common secret may be created amongst the participants by simply trading their public keys with one another. Any other entity that has access just to the public information will be unable to compute the shared secret unless that entity also has access to each communication party's separate private key. The Private Key and the Public Key of a cryptosystem are connected to one another with the assistance of One-Way mathematical functions. These are functions in which the forward operation may be performed with relative ease, however the reverse action is nearly difficult. Within the confines of this particular cryptosystem, the forward operation of the one-way mathematical function is carried out by employing the Private Key in order to derive the Public Key. If the Private Key can be easily extracted from the Public Key by executing the reverse operation of the one-way functions, then it is safe to presume that the cryptosystem has been compromised. Any cryptosystem that is based on Public Key Cryptography (PKC) is subject to this assumption. Within the scope of this article, we plan to provide a summary of the research that we have carried out to ensure the confidentiality of information during e-governance transactions using cryptography.

Objective

[1] Study on Information security in E Governance.
[2] Study on information security using Cryptography during E-Governance transactions.

What is E-governance?

E-governance is the term given to the process by which various modern information and communication technologies, such as the Internet, local area networks (LAN), mobile phones, and so on, are utilised by the government in order to enhance its effectiveness, efficiency, and service delivery, as well as to promote democracy. E-governance, also known as e-governance or e-governance, is a system that makes use of information and communication technology in order to strengthen and support effective government. "The use of information and communication technologies (ICTs) to improve the activities of public sector organisations" is what "e-government" refers to, according to [1] definition. E-governance refers to the process of providing information to users or customers in a timely and effective manner, which is to the advantage of both the customer and the government. E-governance is a tool that may be utilised to create a SMART government, where SMART refers to a government that possesses all of the required characteristics of a good government. The letter 'S' in SMART stands for 'Simple,' the letter 'M' stands for

'Moral,' the letter 'A' stands for 'Accountability,' the letter 'R' stands for 'Responsiveness,' and the letter 'T' stands for 'Transparency.'

Security of E-governance

People in a number of different nations are now living quite differently as a direct result of the implementation of e-governance. Given the current state of affairs, it is fair to assume that the majority of our operations and requirements are dependent entirely on e-governance; for this reason, ensuring the safety of e-governance is an important concern. In this article, we will attempt to describe a method for the security of e-governance that is based on specifically two concepts. These phrases are "Security of What?" and "Security against What?" In this part, we will focus on attempting to find answers to these two questions.

Security of What

What exactly are you securing? When it comes to the topic of e-governance security, this is a very important subject. Protecting an organization's investments in its information and communication technology (ICT) is the primary objective of security measures.

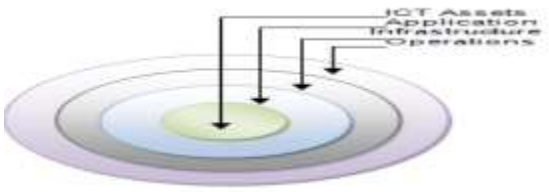

Fig.1- Security Layers

The ICT assets themselves can be of a wide variety including the following:

Data, Information, Knowledge Resources, Programs, Hardware, Networks

In the previous section, we mentioned a few different ICT assets that are highly significant from a security point of view for e-governance. Protecting these assets is a very essential job that administrators of e-governance systems are tasked with.

Security against What

There are many different dangers to the safety of our information and communications technology (ICT) system, and we are unable to precisely identify or proclaim any of them. These dangers might originate from a variety of places and take a number of different shapes. Therefore, being able to recognise these dangers is an absolute requirement for egovernance administrators. In this part, we will first discuss some potential origins of threats, and then we will discuss several categories of threats that can have an impact on e-governance.

Sources of Threat

There is a possibility that the causes of the threat lie either within the government body itself or outside of it. There are many other internal sources of danger, such as staff who work on the E-governance project or clients of the E-governance projects who may try to get access to the databases in order to make a monetary

gain for themselves. When we talk about outside sources, we may be referring to Professional hackers, Criminal Organizations, or Various Intelligence or Investigation Agencies.[2]

Types of Threat

Unauthorized access, alteration, or deletion of data might all fall under the category of threats. Because technological advances occur so often, the potential dangers can take on a variety of forms and can alter over time. Defacing of web sites, hacking, cracking, damaging important databases and programmes, network security check list, DSA, viruses and malwares, and other types of cyberattacks can all be used to compromise the safety of an e-governance system. Some of these methods include: The destruction of information and communication technology assets need not necessarily be the consequence of malevolent assaults like those described above. It might be a natural calamity, a problem with the environment, or something else entirely.

E-GOVERNANCE

E-governance refers to the most effective exploitation of information and communication technology (ICT) for the purpose of improving the efficiency with which services are delivered to citizens. E-governance refers to the process of providing information to users or customers in a timely and effective manner, which is to the advantage of both the customer and the government.

E-Governance Risk Factors

The E-governance risk factors [3] seen are as follows

Spoofing:

In this method, the attacker makes an effort to break into the E-Governance system by posing as a legitimate user with a phoney identity. This can be accomplished in stealth mode or by utilising a spoofed IP address. After gaining access to the system, the attacker will next exploit it by elevating their privileges within the E-Governance system.

Repudiation:

During the E-Governance transaction, the adversary may launch a repudiation attack, which refers to the user's capacity to contradict the results of a previously executed transaction.

Disclosure of E-Governance Information:

In the event that the integrity of the E-Governance system is breached, unwelcome exposure of information may take place with relative ease.

Denial of Service:

A denial of service assault, also known as a DoS attack, can be carried out by the attackers flooding the E-Governance server with requests in an effort to use up all of its resources and bring the system to a halt.

Elevation of Privilege

Cyber Crimes

Security measures to reduce E-Governance risk factors

The information that is sent over the internet is divided into smaller pieces known as data packets, which might take a variety of paths before arriving at their final destination. The gateways via which users connect to and disconnect from the internet are the most susceptible sites for the unauthorised collection of data. [4] In order to maintain the confidentiality and integrity of the data, it is possible to encrypt and decode the packets that are sent between these two vulnerable locations. The following is a list of the several types of cryptographic algorithms that may be used to accomplish the goals outlined above:

Symmetric or Secret Key Encryption:

Symmetric-key algorithms are a type of encryption technique that encrypts and decrypts information using the same key. These algorithms are also known as public-key algorithms. It is also known as a secret key since the one who sends the information and the person who receives it keep it a secret between the two of them. Otherwise, the secrecy of the information that has been encrypted is jeopardised. The larger the key that is utilised for symmetric key encryption, the more secure the encryption will be. Encryption with symmetric keys is significantly quicker than encryption with public keys (may be 100 to 1,000 times faster).

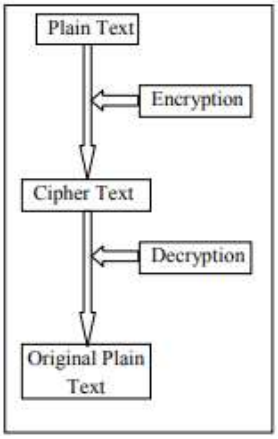

Figure 1: Encryption and Decryption

Where Encryption: EK(M)=C Decryption: DK(C)=M

M=>Original Message E=> Encryption Function D=>Decryption Function C=>Cipher Text K=>Secret Key

Symmetric/ Secret Key Encryption

Asymmetric or Public Key Encryption:

Although the term "public key algorithm" is the one that is used most frequently, the term "asymmetric key algorithm" is also used occasionally to refer to encryption algorithms that employ distinct keys for encrypting and decrypting information. When using public key encryption, it is necessary to make use of both a private key, which refers to a key that is only known to its owner, as well as a public key (a key that is available to and known to other entities on the network). It is possible for the public keys of every user to be listed in the directory, making them easily available to everyone who makes use of the organisation. Both of the keys have separate purposes, yet one of them completes the other. Information that has been encrypted with the assistance of a public key may only be decrypted with the private key that corresponds to that public key within the set.

Encryption: EK1 (M)=C

Decryption: DK2 (C)=M; DK2 (EK1 (M))

Where

M=>Original Message

E=> Encryption Function

D=>Decryption Function

C=>Cipher Text

K 1 =>Private Key

K 2 =>Public Key

K 1 ≠K

Asymmetric/ Public Key Encryption

Secret Key Exchange[6]

In the instance of symmetric key cryptography being used for online communications, the secret key needs to be kept safe from unauthorised parties while also being shared with the people involved in the conversation When exchanging secret keys over the internet, a public-key encryption technique could be necessary to ensure the safety of the transaction.

PUBLIC KEY CRYPTOGRAPHY

RSA and ECC are two of the most well-known algorithms for public key cryptography, both of which are utilised extensively in the secure transaction industry. ECC is the most up-to-date approach with a small key size, little processing overload, and provides the same level of security as the RSA algorithm, which is based on huge keys.

RSA

RSA [7] is a technique for public-key cryptography that is based on the presumptive difficulty of factoring big numbers. This difficulty is derived from the fact that large integers have a large number of digits. RSA is an acronym that stands for the first initials of the last names of the three individuals who, in 1977, were the first to explain it in public: Ron Rivest, Adi Shamir, and Leonard Adleman. Clifford Cocks, a British mathematician, invented a method that was comparable in 1973; however, it was not made public until 1997 since it was secret. The user who is participating in the RSA algorithm generates and then publishes, as an auxiliary value, the product of two big prime integers. This is done in conjunction with the user's public key. It is imperative that the primary components be kept a secret. Anyone with access to the public key can encrypt a message; but, according to the disclosed techniques now in use, if the public key is particularly big, a person with knowledge of the prime factors may be able to decrypt the entire text. The RSA issue is

an open question that seeks to answer the question of whether or not cracking RSA encryption is as difficult as factoring.

As an illustration of this take two large prime numbers (300) digits, multiply them together. As a result you will find

a) Large number (More or equals 300 digits)

b) It has two factors; both are prime (Multiplier)

It is not difficult to provide the two prime numbers, and with these, one may quickly calculate the product. But extracting the primes from the product that is supplied is a more harder task. In point of fact, if the numbers are sufficiently high, it will be extremely difficult, if not impossible, to locate them. Therefore, the straightforward function in this algorithm that involves multiplying two huge prime integers together is the one that is easiest to perform. The process of determining an inverse factor is far more challenging, and in practise, it is nearly impossible. This particular fact is utilised by the RSA system in order to produce public key and private key pairs. The functions of the product and the primes are the ones that hold the keys. This particular cryptosystem was built with the intention of performing a straightforward forward function, which is multiplication. Because the inverse operation needs to solve a complex inverse factoring problem, the operation must make it difficult to retrieve the plaintext from the cypher text using only the public key. In other words, the process must make it tough to decipher.

Elliptic Curve Cryptography (ECC)

In recent years, the key length of safe RSA has been raised, which has resulted in a larger processing strain being placed on applications that use RSA. Elliptic curve cryptography with shorter key lengths has allowed for a significant reduction in the severity of this issue (ECC). The elliptic curve serves as the foundation for the ECC.

Elliptic Curve:

Elliptic Curves are not truly ellipses. The curves got their name from the fact that they are represented by cubic equations, which are quite similar to the equations that are used to compute the circumference of an ellipse. An elliptic curve is defined as the locus of a point whose coordinates conform to a specific cubic equation along with the point at infinity O (the point at which the locus in the projective plane intersects the line at infinity). [8] An elliptic curve can also be defined as the point at which the locus in the projective plane intersects the line at infinity. The equations that define an elliptic curve in a conventional two-dimensional, x,y Cartesian coordinate system are provided below as (1) and (2). (2)

$y\,2 = x\,3 + ax + b$ (1) where $4a\,3 + 27b\,2 \neq 0$.

$y\,2 + xy = x\,3 + ax2 + b$ (2)

The mathematical foundation of ECC is based on the above equations which may be depicted as follows

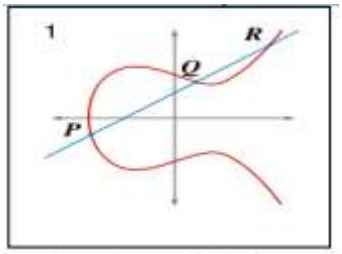

Figure 2: An Elliptic Curve

The elliptic curve is utilised in ECC as a means of defining both the members of the set over which the group is computed as well as the operations that take place between those members to determine how mathematics is conducted within the group. Imagine a graph with the numbers of a huge prime field labelled along both axes of the graph. This is how the process works. [9] Elliptic curve cryptography, sometimes known as ECC, is a method of public-key encryption that is based on the algebraic structure of elliptic curves over finite fields. [10] Elliptic curve cryptography was first developed in the 1980s. Elliptic curves were first proposed for use in cryptography in 1985 by Neal Koblitz and Victor S. Miller, both of whom did so separately. One of the three cryptosystems that are now utilised for public key cryptography (PKC) is known as the elliptic curve cryptosystem. The other two systems, known as integer factorization systems and discrete logarithm systems, round out the list. The most well-known example of the integer factorization issue is the RSA cryptosystem, whereas the Digital Signature Algorithm (DSA) cryptosystem is based on the discrete logarithm problem. The decryption of messages using public keys relies on the fact that particular mathematical puzzles can be solved simultaneously. Prior to the development of ECC, the assumption was made that public-key systems were safe on the grounds that it is impossible to factor a huge integer that is comprised of two or more large prime factors. In the case of protocols that are based on elliptic curves, it is presumed that it is not possible to compute the discrete logarithm of a random element of an elliptic curve with respect to a publicly known base point. This is due to the fact that such a calculation would be impossible. The level of difficulty of the task is directly proportional to the size of the elliptic curve. As a result, an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key, i.e. a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key. The benefit of ECC is a smaller key size, which facilitates to reduce storage and transmission requirements. Over the elliptic curve y2 = x 3 + axe + b, the mathematical operations of ECC are specified. In this context, 4a3 +27b2 0. Each possible combination of "a" and "b" results in a distinctively different elliptic curve. On the elliptic curve can be found all points (x, y) that satisfy the equation in the previous sentence in addition to a point that is infinite. The public key is represented as a point on the curve, while the private key is a random integer. The public key may be derived by taking the private key and multiplying it with the point G in the elliptic curve that serves as the generator. ECC's generating point G, the curve parameters "a" and "b," and a few other constants make up the domain parameter, which is a set of predefined constants that are known to all of the parties that are taking part in the communication. This parameter is known as the "domain parameter."

Solving security problems in E-Governance.

In order to create an effective e-governance system, its security issues need to be resolved in a manner that ensures citizens will derive the greatest possible advantage from the system. Utilizing the secure communication network as opposed to the unsecure communication network is both the most secure as well as the most expensive method for resolving this issue. Alternate strategies, on the other hand, will need to be

chosen in order to overcome this issue because it is not always possible to do so. Either a hardware component or a software component can be utilised in conjunction with the E-Governance system in order to achieve the desired result of obtaining this solution. Both of these options are viable. The incorporation of hardware security components into the E-Governance system would result in an increase in budgetary costs for the government, which is already very vulnerable to the occurrence of physical damages that are beyond of the control of individual humans. The software security component of the E-Governance system needs to be powerful enough to ward off even the most technologically sophisticated attacks on a consistent basis. Because of this, the E-Governance system has to have cryptography-based security software components integrated into it. These components, which will be discussed in the next section of this article, are essential.

Cryptography.

Cryptography is both an art and a science, and its primary purpose is to protect messages from being read by unauthorised parties. Cryptographers are the experts who practise this particular branch of mathematics and science. Cryptographers are able to transform the plain text into the encrypted text that corresponds to it by employing these approaches in conjunction with a cryptographic algorithm. A particular algorithm may be used to decode the encrypted text in order to recover the plain text that corresponds to it. This can take place at the same time. The whole process of encrypting and decrypting the plain text is predicated on a specific parameter called the Key. The Key is a specific sequence of bits that is only known to the legitimate sender of the message and the valid receiver of the message. Utilizing this strategy, the legitimate sender can encrypt the plain text by using this key, and then send the encrypted message across the Internet. Concurrently, the person who is authorised to receive the communication will be given the encrypted message, and then they will be able to decode it using the chosen key in order to obtain the plain text. It is exactly the same as making a public handoff of a valuable object from the sender to the recipient while maintaining the security of a lock and key system. Figure 1.15 illustrates both the encryption and decryption of plaintext for your convenience.[11]

Based on the characteristics of Key used by the sender and the receiver, the295

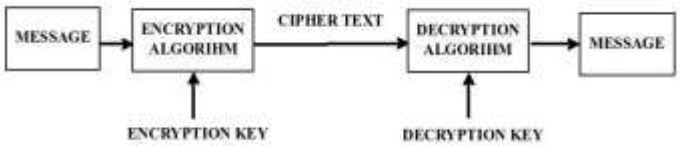

Figure 1.15: Encryption and Decryption of plain text using Cryptography.

Cryptographic techniques can be stated as below :

1. Secret Key Cryptography (SKC) - A basic kind of cryptographic method, also known as Secret Key Cryptography (SKC) or Symmetric Key Cryptography, Secret Key Cryptography (SKC) allows for the encryption key to be derived based on the decryption key, and vice versa. The key that is used for encryption and the key that is used for decryption are almost always the same. The length of a key is commonly measured in hundreds of bits, and it contains a predetermined set of instructions that must be followed in order to finish the cryptographic operations. The strength of the Symmetric algorithm is dependent on the privacy of the key, the disclosure of which will easily bring down the cryptosystem. It is possible to apply cryptographic algorithms such as the International Data Encryption Algorithm (IDEA) the Advanced Encryption Standard (AES) [12], and others with further changes in order to improve the secret

key cryptosystems of the E-Governance system. If we assume that M stands for plain text, C for cypher text, E for encryption function, D for decryption function, and K stands for the key in symmetric key or secret key cryptography, then the encryption and decryption process may be described as follows:

Encryption: EK (M) = C

Decryption: DK (C) = M

In paper - 3 we have described the application of International Data Encryption Algorithm (IDEA) [13] in our proposed E-Governance model to achieve privacy over classified information. If the intruder get the key K by some means or even by using trial and error method, the entire message communication will become highly compromised, which will ultimately destroy the sanctity of the E-Governance system. To overcome this problem, the concept of Public Key Cryptography (PKC) or Asymmetric Key Cryptography was introduced, which is discussed in the next part of this paper

Public Key Cryptography (PKC) - The art and science of encrypting and decrypting data using a system in which each participant possesses a pair of keys known as a private key and a public key is referred to as public key cryptography. [14] The private key is solely known to a single person, but the public key may be accessed by anybody in the community. The public key is distinguished in that it does not jeopardise the integrity of the algorithms and, as a result, it is not difficult to disseminate it over the internet. The only exchange that takes place between the participants is of their public keys; as a result, they have a common secret. Any other entity that has access just to the public information will be unable to compute the shared secret unless that entity also has access to each communication party's separate private key. The private key and the public key of a cryptosystem are connected to one another with the assistance of one-way mathematical functions, which allow for the forward operation to be performed with relative ease but make it nearly hard to do the reverse action. Within the confines of this particular cryptosystem, the forward operation of the one-way mathematical function is carried out by employing the private key in order to derive the public key. If the private key can be easily recovered from the public key by executing the reverse operation of the one-way functions, then it is safe to presume that the particular cryptosystem in question has been compromised. When the key size is raised, this likelihood becomes less likely to occur. In the field of electronic governance, variants of the RSA and DSA encryption algorithms have a significant amount of potential applicability. If we assume that M stands for plain text, C stands for cypher text, E stands for encryption function, D stands for decryption function, K1 stands for encryption key, and K2 stands for decryption key, then the encryption and decryption process in public-key cryptography may be described as follows:

Encryption: EK1 (M) = C

Decryption: DK2 (C) = M

That means: DK2 (EK1 (M)) = M ; where K1 6= K2.

However, in the real world it is not possible to make constant use of these cryptographic algorithms in the E-Governance system. The primary reason for this is the excessive budget expenses that are incurred for the encryption and decryption of enormous amounts of data that are transmitted between the government and its citizens. Elliptic Curve Cryptography (ECC), which will be discussed in the next sub-section, was one of the

methods that we utilised over the course of our study in an effort to cut down on costs by making the most efficient use of the resources at our disposal.

CONCLUSION

In order to safeguard both secret and unclassified components of the nation's security infrastructure, the National Security Agency (NSA) uses elliptic curve cryptography in its Suite B. It may be used for both the exchange of keys and the creation of digital signatures. This demonstrates that the elliptic curve cryptosystem is ready for usage in the real world and is to be chosen in many situations over other cryptosystems. [Cryptosystems] Although there is no real mathematical proof that elliptic curve cryptosystem is more secure than cryptosystems based on discrete logs over finite fields or integer factorisation, elliptic curve cryptosystem appears to be the most efficient and secure public key cryptosystem that is currently available. This is despite the fact that there is no real mathematical proof that elliptic curve cryptosystem is more secure. In light of the fact that it is possible to assess the kind of assaults launched against the E-Governance system, the most powerful and cutting-edge cryptographic mechanism, known as ECC, needs to be developed in order to provide the greatest possible degree of security for the E-Governance system.

REFERENCES

[1] Abhishek Roy and Sunil Karforma, "Risk and Remedies of E-Governance System", in Oriental Journal of Computer Science &Technology, Vol. V, No.(2), pp. 329-339, December 2011
[2] Wikipedia.org, http://en.wikipedia.org/wiki/RSA_%28algorithm%29, -Accessed on 17-10-2012
[3] Bruce Schneier., "Applied Cryptography: Protocols, Algorithms, and Source Code in C", -Second Edition.
[4] Wikipedia.org, http://en.wikipedia.org/wiki/Elliptic_curve_cryptography -accessed on 17-10-2012
[5] Microsoft Technet, http://technet.microsoft.com/en-us/library/cc962035.aspx -, accessed on 17-10-2012
[6] Vivek Katiyar, Kamlesh Dutta & Syona Gupta,"A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment", in International Journal of Computer Applications (0975 – 8887) , Volume 11– No.10, December 2010, pp. 41- 46 .
[7] Arun Kumar, Dr. S.S. Tyagi, Manisha Rana, Neha Aggarwal, Pawan Bhadana - "A Comparative Study of Public Key Cryptosystem based on ECC and RSA" - International Journal on Computer Science and Engineering (IJCSE), Vol 3, No. 5, May-2011, pp. 1904-1905. [8]. William Stallings, Cryptography and Network SecurityFifth Edition, Pearson. pp. 344.
[8] Sumita Sarkar, Abhishek Roy, A Study on Biometric based Authentication, Proceedings of Second National Conference on Computing and Systems - 2012 (NaCCS - 2012) organized by the Department of Computer Science, The University of Burdwan, March 15 - 16, 2012, 1st Edition - 2012, Pp: 263-268, ISBN 978-93-80813- 18-9.
[9] Abhishek Roy, Sumita Sarkar, Joydeep Mukherjee, Arindom 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" organized by the Department of Computer Science, Sammilani Mahavidyalaya in collaboration with Department of Computer Science and Engineering, University of Calcutta, February 21 – 22, 2012, Vol: 1, Pp:153-160, ISBN 978-81- 923820-0-5.

[10] Abhishek Roy, Sunil 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.

[11] Abhishek Roy, Subhadeep Banik, Sunil Karforma, Object Oriented Modelling of RSA Digital Signature in EGovernance Security, International Journal of Computer Engineering and Information Technology (IJCEIT), Summer Edition 2011, Vol 26 Issue No. 01, Pp: 24-33, ISSN 0974-2034.

[12] Abhishek Roy, Sunil 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.

[13] Abhishek Roy, Subhadeep Banik, Sunil Karforma, Jayanta Pattanayak, Object Oriented Modeling of IDEA for EGovernance Security, Proceedings of International Conference on Computing and Systems 2010 (ICCS 2010), November 19-20, 2010, Pp: 263-269, Organized by: Department of Computer Science, The University of Burdwan, West Bengal, INDIA. ISBN 93-80813-01-5.

[14] Chayan Sur, Abhishek Roy, Subhadeep 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, Pp: a-h, Organized by : Department of Computer Science, The University of Burdwan, West Bengal, INDIA. ISBN 8190-77417-4.