ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 7 July, 2014 Page No. 7364-7374

Triple System Security in Cloud Computing

Parul Mukhi[1], Bhawna Chauhan[2]

[1] *M.Tech Scholar, B.S Anangpuria Institute of Technology & Management, Faridabad*

[2] *Assistant Professor, B.S Anangpuria Institute of Technology & Management, Faridabad*

[1]parulmukhi@ymail.com; [2]bhawna.chauhan@faculty.anangpuria.com

ABSTRACT - ***Large scale distributed systems such as Cloud Computing applications are becoming very common these days. These applications come with increasing challenges on how to transfer and where to store and compute data. The most prevalent distributed file systems to deal with these challenges are the Hadoop File System (HDFS) which is a variant of the Google File System (GFS). However HDFS has two potential problems. The first one is that it depends on a single name node to manage almost all operations of every data block in the file system. As a result, it can be a bottleneck resource and a single point of failure. The second potential problem with HDFS is that it depends on TCP to transfer data. As has been cited in many studies, TCP takes many rounds before it can send at the full capacity of the links in the cloud. These results in low link utilization and longer download times. To overcome these problems of HDFS, a new distributed file system is presented in this thesis. The scheme of this distributed file system uses a light weight front end server to connect all requests with many name nodes i.e. Triple Security.***

Keywords: DSA (Digital Signature Algorithm); DES (Data Encryption Standard); AES(Advanced Encryption Standard); RSA (Rivest Shamir AdlEman); HDFS (Hadoop File System); GFS (Google File System); TCP (Transmission Control Protocol); NFS (Network File System);AFS (Andrew File System); LAN (Local Area Network); WAP (Wireless Application Protocol);DSS (Digital Signature Standard); ECDSA (Elliptic Curve DSA); MAES (Modified AES);

I. INTRODUCTION

1.1 WHAT IS CLOUD COMPUTING

Cloud computing is an internet based technology provided us to store and deliver computing resources over the internet. There are virtual servers hosting to customers on a pay-as-you-use basis means that customers (usually organizations) can request and manage their own computing resources. Cloud computing have aimed to allow access to large amount of computing power in a fully virtualized manner.[1] In other words, it allow access to information and computer resources from anywhere that a network connection is available. The users do not have any idea of where their data is kept and who manage their data[4][5]. Cloud computing customers do not own the physical infrastructure rather the storage is provided by the third party.

1.2 CLOUD SERVICES

The cloud services are embedded with three services –

- Software as Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Software as a Service allows users to access various application software that are being hosted on the infrastructure of a service provider[8]. Platform as a Service allow developers to work on
their needed platform. Infrastructure as a Service provides administering and configuring infrastructure.

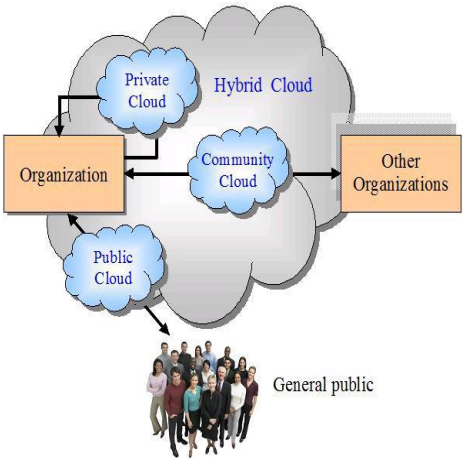
1.3 DEPLOYMENT MODEL

Cloud has a variety of deployment models such as

1.3.1 *Private Cloud:* Private Clouds are available to a specific organization and its customers. Its infrastructure is solely for a particular organization [2]. Resources present on cloud are limit to a group of people of a particular organization.

1.3.2 *Public Cloud*: This cloud infrastructure is available to the public by cloud service provider i.e. anyone can use it and pay as per need. Public clouds are less secure as compared to other cloud models because it places an additional burden that is all applications and data accessed on the public cloud are not free from malicious attacks [2].

1.3.3 *Community Cloud*: The Private Clouds are provided to a particular organization whereas community cloud is shared among the various organizations. They also shared the cloud to share and reduce the cost of computing system. This is more expensive option as compared to public cloud. It provides unlimited data storage space for storing user's data [5].



1.3.4 *Hybrid Cloud:* Hybrid cloud is a combination of private and public cloud. Its infrastructure consists of a number of clouds of any type. In other words, it is a combination of virtualized cloud server instances used together with real physical hardware.

1.4 CLOUD COMPUTING ARCHITECTURE

Its architecture consists of mainly two components (a) The Front End (b) The Back End
The front end part comprises the client's devices and some applications are needed for accessing the cloud computing system.[3] It may include the computers networks. The back end of the cloud refers to 'cloud' itself. It encompasses various computer machines, data storage, system and servers.
There is a central server who administrates the whole cloud system and monitoring clients demand and traffic ensuring smooth functioning of the system. All the computers connected to a network communicate with each other through software called 'middleware'[7]. Cloud computing also provides data redundancy i.e. copies of client's data to restore the service. This is helpful in case of any network or device breakdown.

1.5 BENEFITS OF CLOUD COMPUTING

 Flexibility : a cloud-based service can instantly meet the demand because of the vast capacity of the service's remote servers

 Disaster recovery : cloud computing take care of most issues of being data lost and provides fast recovery to them.

 Automatic Software Updates : cloud computing suppliers do the server maintenance – including security updates – themselves

 Less Expenditure Cost : Cloud computing services are typically pay as you go, so there's no need for capital expenditure at all. The starting cost of any project is minimal and increases as per the ongoing work.

 Work from Anywhere : As long as employees have internet access, they can work from anywhere.

 Document Control : When a person or employee not using the cloud then only one person can work on a file like sending and checking e-mails but in the cloud system there is a central location where all files are kept. All employees of a company can make changes to their data together. It increases the efficiency and improves a company's bottom line.

1.5 ISSUES IN CLOUD COMPUTING

As all the technology has its own merits and demerits, similarly cloud computing also has some risk due to which its popularity became declined. When we work on internet we always concern about security due to cyber crime. Hacker could hack user's confidential data. Similarly in cloud computing security is the major issue.[7] Since it is available to various organization and customers, anyone can use it so it may have some criminal offences like hacking or unauthorized access. Cloud provider need to overcome security problems to increase its efficiency and popularity.

1.6 INTRODUCTION TO FILE SYSTEM OF CLOUD COMPUTING

Another popular file system for networked computers is the Network File System (NFS). It is a way to share files between machines on a network as if the files were located on the client's local hard drive. One of the disadvantages of NFS is that it tries to make a remote file system appear as a local file system, but it is dangerous to rely on that oversimplification.
There are many situations in which the use of NFS (compared to a local file system) is not appropriate or reliable. Andrew File System (AFS) is a distributed networked file system which uses a set of trusted servers to present a homogeneous, location-transparent file name space to all the client workstations.[5] AFS has several benefits over traditional networked file systems, particularly in the areas of security and scalability. It is not uncommon for enterprise AFS cells to exceed twenty five thousand clients. AFS uses Kerberos for authentication, and implements access control lists on directories for users and groups[9]. Each client caches files on the local file system for increased speed on subsequent requests for the same file. AFS may not be convenient for large scale file systems such as the once handled by GFS.

The standard notion of digital signature security is extremely vulnerable to leakage of the secret key which over the lifetime of the scheme may be quite a realistic threat.[10] Indeed if the secret key is compromised any message can be forged.
Electronic cheques are another form of Electronic tokens. They are designed to accommodate the many individuals and entities that might prefer to pay on credit or through some mechanism other than cash. Once registered, a buyer can then contact sellers of goods and services. To complete a transaction, the buyer sends a check to the seller for a certain amount of money. These checks may be sent using Email or other Transport methods. When deposited, the cheque authorizes the transfer of account balances from the account against which the cheque was drawn to the account to which the cheque was deposited. The electronic cheques

are modelled on paper checks, except that they are initiated electronically.[11] They use digital signatures for signing and endorsing and require the use of digital certificates to authenticate the payer, the payer's bank and bank account. They are delivered either by direct transmission using telephone lines or by public networks such as the Internet.
This project is basically developed for changing the current system of File System into a more secure, more reliable and more user friendly way. This application is based on giving soft copy of files to users instead of using hard copies which is not much secure.

1.7 GOALS & OBJECTIVES OF CLOUD COMPUTING

1.7.1 Goals

 Military communications system make increasing use of traffic security technique which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections.

 Support the testing of electronic check applications through pilot programs.

 Implement electronic Check applications that show the greatest potential.

 Support research to address consumer, legal, regulatory and risk issues of electronic check applications.

 Provide a forum for all stakeholders in the electronic check arena.

 Promote the development and use of electronic check applications.

 A form of payment made via the internet that is designed to perform the same function as a conventional paper check. Because the check is in an electronic format, it can be processed in fewer steps and has more security features than a standard paper check. Security features provided by electronic checks include authentication, public key cryptography, digital signatures and encryption, among others.

1.7.2 Objective

To develop a user friendly Electronic Check System to overcome the limitation of manual check system & to enhance the flexibility of the commercial as well as business transactions in an easy way.It Reduce costs, minimize risk and get faster access to your money by converting paper checks into electronic transactions right at the point of sale.

1.8 PROBLEM DEFINITION

The danger could be the possible fraud by some merchants, also hacking into the electronic records or interception of a transmission is another risk. There is also the danger of human error or equipment failure which can jeopardize the accuracy of transmissions or records. Customers should check their banking records carefully for unfamiliar or unauthorized transactions.
Some solution to be discussed is how to passing information in a manner that the very existence of the message is unknown in order to repel attention of the potential attacker. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media. In this research, we clarify what Steganography is, the definition, the importance as well as the technique used in implementing Steganography. We focus on the Least Significant Bit (LSB) technique in hiding messages in an image. The system enhanced the LSB technique by randomly dispersing the bits of the message in the image and thus making it harder for unauthorized people to extract the original message.
The main features of the proposed work are:
 It eliminates the need of issuing cheque-book from the bank.

 It eliminates cheque portability issue.

 It provides a more secure means of transaction.

 It provides a very fast and reliable means of transaction.

 It lowers the transaction processing time or the clearing cycle.

 It eliminates the need of internet banking infrastructure (for fund transfer) by the banks.

 It maintains the confidentiality and integrity of the transaction details.

 It provides an improved customer service.

 This kind of e-Cheques management is not being developed and used in any of the Banks so far.

1.9 HOW WE CAN OVERCOME THESE LIMITATIONS?

To overcome these limitations we required to add some security features:-
 DSA (Digital Signature Algorithm): Electronic Signature can prove the Authenticity of Alice as a sender of the message.

 AES (Advance Encryption Standard): AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware.

 STEGANOGRAPHY: Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. The goal of steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hiding copyright notice or serial number or even help to prevent unauthorized copying directly.

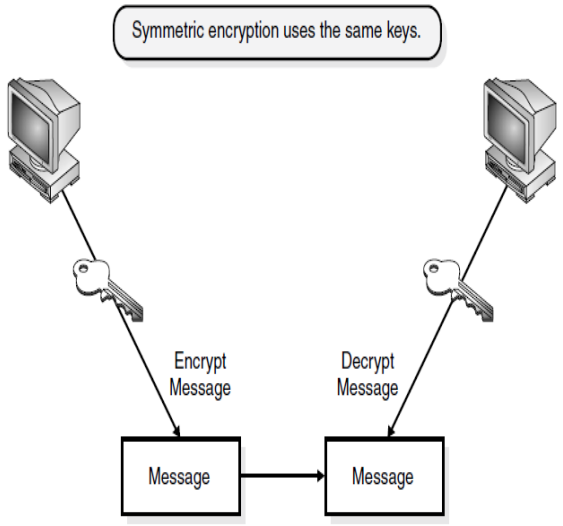
II. SYSTEM ANALYSIS AND DESIGN

2.1 CRYPTOGRAPHY

Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process. It is a science of protecting information by encoding it into an unreadable format. Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths. Although the ultimate goal of cryptography, and the mechanisms that make it up, is to hide information from unauthorized individuals, most algorithms can be broken and the information can be revealed if the attacker has enough time, desire, and resources.[6] So a more realistic goal of cryptography is to make obtaining the information too work-intensive to be worth it to the attacker. Fig-2.1 shows the process of encryption transforms plain text into cipher text and vice-versa for decryption.

2.1.1 Symmetric Systems

There are several types of symmetric algorithms used today. They have different methods of providing encryption and decryption functionality. The one thing they all have in common is that they are symmetric algorithms, meaning two identical keys are used to encrypt and decrypt the data. Fig - 2.2 shows the symmetric encryption which uses the same keys as symmetric uses the private keys for encrypt and decrypt messages



2.2 DSA (Digital Signature Algorithm)

A digital signature algorithm authenticates the integrity of the signed data and the identity of signatory. A digital signature algorithm may also be used in proving to a third party that data was actually signed by the generator of the signature and is intended for use in electronic mail, electronic data interchange, software distribution, and other applications that require data integrity assurance and data origin authentication. The wireless protocols, like Hiper LAN/2, and WAP, have specified security layers and the digital signature algorithm have been applied for the authentication purposes. Electronic Signature can prove the Authenticity of Alice as a sender of the message.

The Digital Signature Standard (DSS) uses three algorithms for digital signature generation and verification [1]. The Digital Signature Algorithm (DSA), the RSA digital signature algorithm as defined in ANSI X9.31 and Elliptic Curve digital signature algorithm (ECDSA) as defined in ANSI X9.62.

2.2.1 Algorithm of DSA

A digital signature is represented in a computer as a string of binary digits. A digital signature is computed using a set of parameters and authenticates the integrity of the signed data and the identity of the signatory. An algorithm provides the capability to generate and verify signature. Signature generation makes use of a private key to generate a digital signature. Signature 12

verification makes use of a public key, which corresponds to, but is not the same as, the private key. Each user possesses a private and public key pair. Public keys are assumed to be known to the public in general. Private keys are never shared. Anyone can verify the signature of a user by employing that user public key. Only the possessor of the user private key can perform signature generation.

Algorithm includes following steps:

Step 1: Choose an approved cryptographic hash function H. In the original DSS, H was always SHA-1, but the stronger SHA-2 hash functions are approved for use in the current DSS. The hash output may be truncated to the size of a key pair.

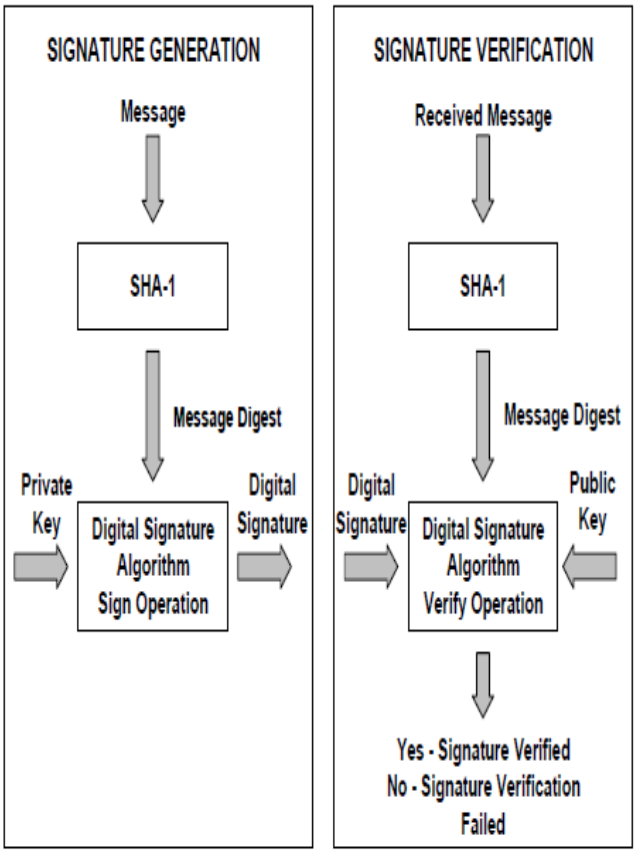
Step 2: Decide on a key length L and N. This is the primary measure of the cryptographic strength of the key. The original DSS constrained L to be a multiple of 64 between 512 and 1024 (inclusive). NIST 800-57 recommends lengths of 2048 (or 3072) for keys with security lifetimes extending beyond 2010 (or 2030), using correspondingly longer N.[10] FIPS 186-3 specifies L and N length pairs of (1024,160), (2048,224), (2048,256), and (3072,256).

Step 3: Choose an N-bit prime q. N must be less than or equal to the hash output length.

Step 4: Choose an L-bit prime modulus p such that p–1 is a multiple of q.

Step 5: Choose g, a number whose multiplicative order modulo p is q. This may be done by setting g = h(p–1)/q mod p for some arbitrary h ($1 < h < p-1$), and trying again with a different h if the result comes out as 1. Most choices of h will lead to a usable g; commonly h=2 is used.The algorithm parameters (p, q, g) can be shared between different users of the system.

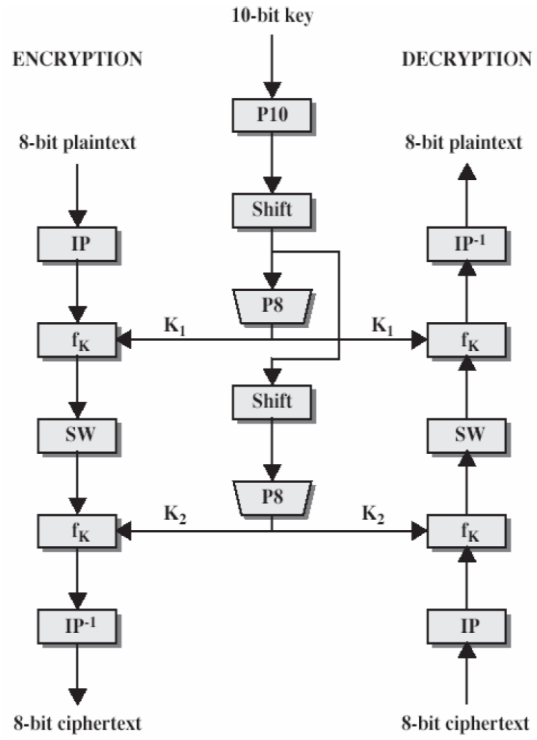
Fig – 2.3 shows the digital signature scheme that uses the signature generation and verication scheme which uses secured hash algorithm.



2.3 DES (Digital Encryption Standard)

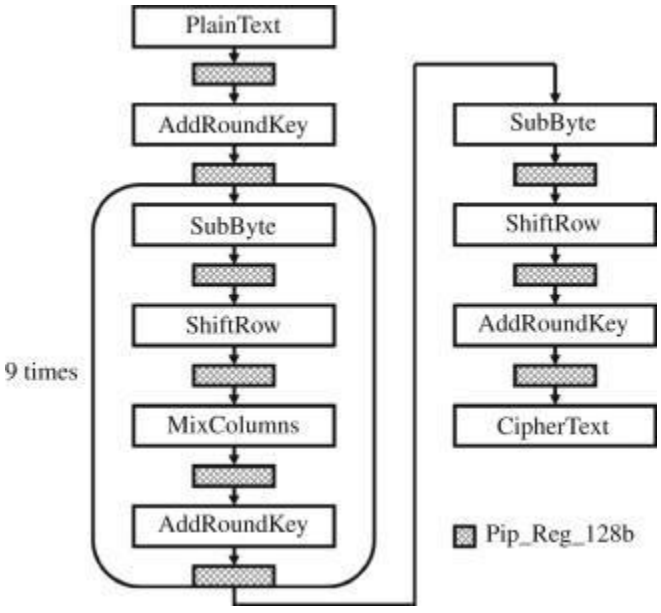
DES was designed by IBM and adopted by the U.S.govt.as the standard encryption method. The Data Encryption Standard (DES) is a block cipher that uses shared secret encryption[12] and Uses only a single key.
S-DES encryption (decryption) algorithm takes 8-bit block of plaintext (cipher text) and a 10-bitkey, and produces 8-bit cipher text (plaintext) block. Encryption algorithm involves 5 functions: an initial permutation (IP); a complex function fK, which involves both permutation and substitution and depends on a key input; a simple permutation function that switches (SW) the 2 halves of the data; the function fK again; and finally, a permutation 2 function that is the inverse of the initial permutation (IP-1). Decryption process is similar. The function fK takes 8-bit key which is obtained from the 10-bit initial one two times. The key is first subjected to a permutation P10. Then a shift operation is performed. The output of the shift operation then passes through a permutation function that produces an 8-bit output (P8) for the first sub key (K1). The output of the shift operation also feeds into another shift and another instance of P8 to produce the 2nd sub key K2. Fig – 2.4 shows the encryption algorithm as superposition in the following manner:
Mathematically,
IP-1○fk2○SW○fk1○IP
Or
Cipher text = IP-1(fk2(SW(fk1(IP(plain text)))))
Where
K1 = P8(Shift(P10(key)))
K2 = P8(Shift(Shift(P10(key))))
Decryption is the reverse of encryption :
Plain text = IP-1(fk1(SW(fk2(IP(cipher text)))))

We now examine the S-DES in more detail.
Also, fig – 2.5 below tells us the simplified form of the DES key generation which helps us understand fig – 2.4 in more detailed manner.



2.4 Advanced Encryption Standard (AES)

Earlier DES was used as an encryption standard for over 20 years and it was able to be cracked in a relative short amount of time, NIST decided a new standard, the Advanced Encryption Standard (AES), needed to be put into place. This decision was announced in January 1997, and a request for AES candidates was made.[4] The AES was to be a symmetric block cipher algorithm supporting keys sizes of 128-, 192-, and 256-bit keys.



Block diagram of AES

2.4.1 DESCRIPTION OF THE ALGORITHM

Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule [35].

Initial Round

 AddRoundKey: each byte of the state is combined with the round key using bitwise xor [35].

Rounds[35]

 SubBytes: a non-linear substitution step where each byte is replaced with another according to a lookup table.

 ShiftRows: a transposition step where each row of the state is shifted cyclically a certain number of steps.

 MixColumns: a mixing operation which operates on the columns of the state, combining the four bytes in each column.

 AddRoundKey

Final Round (no MixColumns)

 SubBytes

 ShiftRows

 AddRoundKey

2.4.2 MODIFIED AES

In modified AES changes in shift row step of AES are done. The modification in shift row step are as follow:

 Examine the value of first row and first column of state, is it even or odd.

- *If it is odd* : the shift row step operate on the rows of the state; it cyclically shift the bytes in each row by a certain offset. For MAES the first and the third rows are unchanged and the bytes in second row is shifted one to left. Similarly the bytes in fourth row are shifted three to left respectively.

- *If it is even* : the shift row step operates on the row of the state; it cyclically shift the bytes in each row by a certain offset. The first and fourth rows are unchanged and each byte in second row is shifted three to right. Similarly, the third is shifted by two on to right.

2.5 Rivest Shamir AdlEman (RSA):

The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers.

Encryption method in RSA:

 Obtains the recipient B's public key (n, e).

 Represents the plaintext message as a positive integer *m*.

 Computes the cipher text c = me mod n.

 Sends the cipher text *c* to B.

Decryption method in RSA :

 Uses his private key (n, d) to compute m = cd mod n.

 Extracts the plaintext from the message representative m.

2.6 INTRODUCTION TO STEGANOGRAPHY

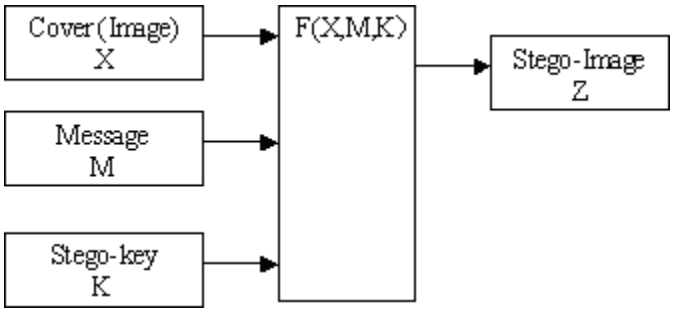
Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. Steganography is the process of hiding one medium of communication (text, sound or image) within another. The word Steganography comes from the Greek steganos (covered or secret) and graphy (writing or drawing) and so it literally means, covered writing.

Steganography is the practice of encoding secret information in a manner such that the very existence of the information is concealed under the image or picture where it is hided. Throughout history, many steganography techniques have been documented, including the use of cleverly-chosen words, invisible ink written between lines, modulation of line or word spacing, and microdots. Usually the secret information is concealed by the use of an innocuous cover so as to arouse no suspicion to anyone. As an example, the cover text: “I’m feeling really stuffy. Emily’s medicine wasn’t strong enough without another febrifuge”.[5]

2.6.1 DIGITAL STEGANOGRAPHY

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message [1]. Digital Steganography deals with developing and transmitting digital data/files under the cover of image/pictures. A typical digital steganography encoder is shown on Fig 2.16. The message is the data that the sender wishes to remain confidential and can be text, images, audio, video, or any other data that can be represented by a stream of bits. The cover or host is the medium in which the message is embedded and serves to hide the presence of the message. This is also referred to as the message wrapper. The message embedding technique is strongly dependent on the structure of the cover, and here in this thesis report covers are restricted to being digital images. It is not required that the cover and the message have homogeneous structure. For example, it is possible to embed a recording of Shakespeare’s lines (an audio stream message) inside a digital portrait of the famous playwright (an image cover).

The image with the secretly embedded message produced by the encoder is the stego-image. The stego-image should resemble the cover image under casual inspection and analysis. In addition, the encoder usually employs a stego-key which ensures that only recipients who know the corresponding decoding key will be able to extract the message from a stego-image.[5]



Steganography Encoding

Recovering the message from a stego-image requires the stego-image itself and a corresponding decoding key if a stego-key was used during the encoding process. The original cover image may or may not be required; in most applications it is desirable that the cover image is not needed to extract the message. Steganography is not the same as cryptography. In cryptography, the structure of a message is changed to render it meaningless and unintelligible unless the decryption key is available. Cryptography makes no attempt to disguise or hide the encoded message. Steganography does not alter the structure of the secret message, but hides it inside a cover. It is possible to combine the techniques by encrypting a message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged.

2.7 DIFFERENCE BETWEEN STEGANOGRAPHY AND CRYPTOGRAPHY

The art of hiding messages is an ancient one, known as steganography. Steganography is the dark cousin of cryptography, the use of codes. While cryptography provides privacy, steganography is intended to provide secrecy. Privacy is what you need when you use your credit card on the Internet, you don't want your number revealed to the public. For this, you use cryptography, and send a coded pile of gibberish that only the web site can decipher. Though your code may be unbreakable, any hacker can look and see you've sent a message. For true secrecy, you don't want anyone to know you're sending a message at all.
The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal.[1] Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

III. LITERATURE SURVEY

Yaser Esmaeili Salehani et al. [1] introduced a new dedicated 256-bit hash function:NESHA-256. The recently contest for hash functions held by NIST, motivates us to design the new hash function which has a parallel structure. Advantages of parallel structures and also using some ideas from the designing procedure of block-cipher-based hash functions strengthen our proposed hash function both in security and in efficiency. NESHA-256 is designed not only to have higher security but also to be faster thanSHA-256.
Shay Gueron , Simon Johnson , Jesse Walker[2] shows the comparison of SHA-512 and SHA-256. Hashing algorithms have long been the poor-man of the community, with their security receiving less attention than standard encryption algorithms and with little attention paid to their speed. As a result, many standards and products have started to move towards larger hash sizes. The reason why SHA-512 is faster than SHA-256 on 64-bit machines is that has 37.5% less rounds per byte (80 rounds operating on 128 byte blocks) compared to SHA-256 .

Masoud Nosrati Ronak Karimi Mehdi Harir [3] proposed about audio steganography. Basic concepts of audio steganography were mentioned and some recent approaches were investigated. They were: Modifying Quantized Spectrum Values of MPEG/Audio Layer III, Embedding data between frames in MP3 file, Quantized frequency domain embedding and reversible integer transforms, Information hiding in audio signals using Considering Parity and XORing of LSB's, Genetic-Algorithm- Based audio steganography, Increasing robustness of LSB audio steganography.
Ritu Pahal Vikas kumar [4] proposed about the AES. They presented a new AES model having bigger block size which is 200 bits rather than conventional 128 bits AES. Also, the block is made by 5 rows and 5 columns unlike the AES's 4 rows and 4 columns. As the size of the matrix has increased, all the transformations of the AES don't need to change except the mix column transformation. During mix column transformation, the diffusion takes place in form of matrix multiplication under finite field. Having a bigger block, hence, requires a new matrix of size 5*5, to enable matrix multiplication.

3.1 ADVANTAGES & DISADVANTAGES OF FILE STORAGE IN CLOUD COMPUTING

3.1.1 Advantages

The important benefits are:
 Less Processing Fees : Triple Security mechanisms are fully electronic. This means, everything from the scanning of your paper cheques to the final fund deposit your merchant's account happens electronically. Electronic methods require very less human interaction.[4] Therefore, the processing fees when using Triple Security mechanism are less compared to Physical links.
 Easy to Convert : With appropriate equipment, Triple Security mechanism is easy. The cash clerks only have to run the paper cheque over the scanning equipment and the equipment will automatically read all the required information for verification.

 *Uses Existing Networks of Direct Deposit, ACH transfers***:** Triple Security processing uses the same existing networks for ACH / direct deposit transfer. Once the Triple Security verification is done, the next step is to use the information on files.

 Governed by similar laws : A merchant using Triple Security mechanism has to inform the customer before converting his checks. According to Electronic Fund transfer Act, Triple Security mechanism is bound by the same laws of electronic security. In addition to these laws, electronic checks are also governed by same laws in which paper checks are treated.[4]

 Triple Security Mechanism reduces the costs: When you see that average paper cheque processing cost $1.5 per cheque and e-Cheque conversion requires only $0.55 per cheque, you can see lot of savings. Therefore, the cost of using e Cheque will reduce the operating costs of businesses.[4][5]

 *Reduced Environmental Impact***:** Vehicles are one of the important reasons for increase greenhouse gases. As Triple Security occur through electronic media instead of physical

transfer through transportation channels, there is a reduction in greenhouse emissions.

 Works with leading Accounting Software : Modern accounting software are designed to work with e-Cheque. Thus, for business, using such software can reduce the processing time for shipping and delivery.

3.1.2 Disadvantages

The disadvantage could be the possible fraud by some merchants, also hacking into the electronic records or interception of a transmission is another risk.[11] There is also the danger of human error or equipment failure which can jeopardize the accuracy of transmissions or records. Customers should check their banking records carefully for unfamiliar or unauthorized transactions.

 Required Special Equipment: Triple Security requires special equipment. Banks, merchant institutions and other businesses will require investing in acquiring these equipment to fully utilize the advantages of e-Cheque. According to size of the firm, the cost of investment may increase.

 Uses Computer Networks: Electronic method means computer networks are used for transferring data. This also means, the problems occurring on computer networks can affect the transactions of e-Cheque. There is also chance of fraud/phishing and other problems while using e-Cheque transfers.

IV. PROPOSED WORK

The Internet as a whole does not use secure links, thus information in transit may be vulnerable to interception as well. The important of reducing a chance of the information being detected during the transmission is being an issue now days. Another problem is that people hike the signature of the sender and use it illegally. They send data by the identification of sender. So it is very necessary to protect signatures from the attackers.

One of the reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of Steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. We proposed architecture to resolve existing fraud issues.

4.1 PROBLEM SCENARIO

Cloud Computing can handle data both in public and private domain. But this apparently undisruptive way of thinking about building applications that has its own set of issues.

The problem is that when cloud service providers provide service, that time the hacker might hack the username and the password. So, to prevent this problem we executed the concept of digital Signature. Digital signatures enable the "authentication" and non-repudiation of digital messages, assuring the recipient of the digital message - both the distinctiveness of the sender and the reliability of the message being sent.

The Rijndael algorithm has been selected as the Advance Encryption Standard (AES) to replace 3DES. AES is modified version of Rijndael algorithm. Advance Encryption Standard evaluation criteria among others was:

 Security

 Software and hardware performance

 Suitability in restricted-space environments

 Resistance to power analysis and other implementation attacks

Rijndael was submitted by Joan Daemen, and Vincent Rijmen. When considered together, Rijndael's combination of security, performance, efficiency, implement ability, and flexibility made it an appropriate selection for the AES.

By design AES is faster in software and works efficiently in hardware. It works fast even on small devices such as smart phones, smart cards etc. AES provides more security due to larger block size and longer keys. AES uses 128 bit fixed block size and works with 128, 192 and 256 bit keys. Rijndael algorithm in general is flexible enough to work with key and block size of any multiple of 32 bit with minimum of128 bits and maximum of 256 bits.

Hence AES is more appropriate than DES in the following manner:

Triple-DES **Description**	**Triple Data Encryption Standard**	**Advanced Encryption Standard**
Timeline	**Standardized 1977**	**Official standard since 2001**
Type of algorithm	**Symmetric**	**Symmetric**
Key size (in bits)	**168**	**192**
Speed	**Low**	**High**
Time to crack (assume a machine could try 255 keys per second - NIST)	**4.6 billion years**	**149 trillion years**
Resource consumption	**Medium**	**Low**

V. SIMULATION/EXPERIMENTAL RESULTS

5.1 DOT NET FRAMEWORK

The .NET Framework is an integral Windows component for building and running the next generation of software applications and Web services. The .NET Framework:

 Supports over 20 different programming languages.

 Manages much of the plumbing involved in developing software, enabling developers to focus on the core business logic code.

 Makes it easier than ever before to build, deploy, and administer secure, robust, and high-performing applications.

The .NET Framework is composed of the common language runtime and a unified set of class libraries.

5.2 The Significance of .NET and C#

In order to understand the significance of .NET, it is useful to remind ourselves of the nature of many of the Windows technologies that have appeared in the past 10 years or so. Although they may look quite different on the surface, all of the Windows operating systems from Windows 3.1 (introduced in 1992) through Windows Server 2008 have the same familiar Windows API at their core. As we have progressed through new versions of Windows, huge numbers of new functions have been added to the API, but this has been a process of evolving and extending the API rather than replacing it. The same can be said for many of the technologies and frameworks that we've used to develop software for Windows.

Part I: The C# Language

This section gives a good grounding in the C# language itself. This section doesn't presume knowledge of any particular language, although it does assume you are an experienced grammar. You start by looking at C# ' s basic syntax and data types, and then explore the object-oriented features of C# before moving on to look at more advanced C# programming topics. **Part II: Visual Studio**
This section looks at the main IDE utilized by C# developers worldwide: Visual Studio 2005. In this section look at the best way to use the tool to build applications based upon either the .NET Framework 2.0 or 3.0. In addition to this, this section also focuses on the deployment of your projects.
Part III: Base Class Libraries
In this section, you look at the principles of programming in the .NET environment. In particular, you look at security, threading localization, transactions, how to build Windows services, and how to generate your own libraries as assemblies.
Part IV: Data
Here, you look at accessing databases with ADO.NET and LINQ, and at interacting with directories and file is so extensively covers support in .NET for XML and on the Windows operating system side, and the .NET features of SQL Server 2008. Within the large space of LINQ, particular focus is put on LINQ to SQL and LINQ to XML.
Part V: Presentation
This section focuses on building classic Windows applications, which are called Windows Forms in .NET. Windows Forms are the thick - client version of applications, and using .NET to build these types of applications is a quick and easy way of accomplishing this task. In addition to looking at Windows Forms, you take a look at GDI+, which is the technology you will use for building applications that include advanced graphics. This section also covers writing components that will run on Web sites.
Language Used to create our Software:-
ADO.NET
C#.Net

5.2 SQL as Backend Language
- SQL stands for Structured Query Language
- SQL allows you to access a database
- SQL is an ANSI standard computer language
- SQL can execute queries against a database
- SQL can retrieve data from a database
- SQL can insert new records in a database
- SQL can delete records from a database
- SQL can update records in a database
- SQL is easy to learn.

The DOT NET Framework is a software framework developed by Microsoft that runs primarily on Microsoft Windows. It includes a large library and provides language interoperability across several programming languages. Programs written for the DOT NET Framework execute in a software environment known as the Common Language Runtime (CLR), an application virtual machine that provides important services such as security, memory management, and exception handling. The class library and the CLR together constitute the DOT NET Framework
The DOT NET Framework's Base Class Library provides user interface, data access, database connectivity, cryptography, web application development, numeric algorithms, and network communications. Programmers produce software by combining their own source code with the DOT NET Framework and other libraries. The DOT NET Framework is intended to be used by most new applications created for the Windows platform. Microsoft also produces a popular integrated development environment largely for DOT NET software called Visual Studio.

5.3 Design features

- **Interoperability**
  Because computer systems commonly require interaction between newer and older applications, the DOT NET Framework provides means to access functionality implemented in programs that execute outside the DOT NET environment.
- **Language Independence**
  The DOT NET Framework introduces a Common Type System, or CTS. The CTS specification defines all possible data types and programming constructs supported by the CLR and how they may or may not interact with each other conforming to the Common Language Infrastructure (CLI) specification. Because of this feature, the DOT NET Framework supports the exchange of types and object instances between libraries and applications written using any conforming DOT NET language.
- **Simplified Deployment**
  The DOT NET Framework includes design features and tools which help manage the installation of computer software to ensure it does not interfere with previously installed software, and it conforms to security requirements.
- **Security**

The design is meant to address some of the vulnerabilities, such as buffer overflows, which have been exploited by malicious software DOT NET provides a common security model for all applications.

- **Portability**
  While Microsoft has never implemented the full framework on any system except Microsoft Windows, the framework is engineered to be platform agnostic, and cross-platform implementations are available for other operating systems. Microsoft submitted the specifications for the Common Language Infrastructure, the C# language, and the C++ language making them available as official standards. This makes it possible for third parties to create compatible implementations of the framework and its languages on other platforms.

5.4 Hardware & Software Requirements

Hardware Used

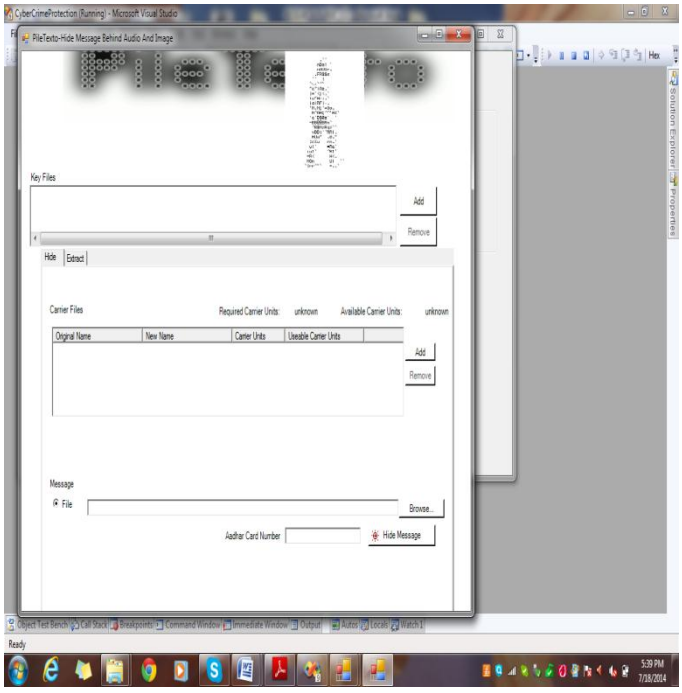
• One computer with 2 GB of memory
• 80 GB hard disk space
• An Intel Pentium Core 2 Duo based computer working at least @ 2.2 GHz speed
• 17 inch monitor

Software Used

• Microsoft Visual Studio 2008
• Windows XP operating system
• MS-office

5.6 RESULT ANALYSIS

This screen shows the message hiding technique behind an audio file using pile texto.



VI. CONCLUSION AND FUTURE SCOPE

CONCLUSION

This research work discusses a user friendly Electronic Check System to overcome the limitation of manual check system & to enhance the flexibility of the commercial as well as business transactions in an easy way. It Reduces cost, minimize risk and get faster access to your money by converting paper checks into electronic transactions right at the point of sale. It eliminates the need of issuing cheque-book from the bank. It eliminates cheque portability issue. It provides a more secure means of transaction. It provides a very fast and reliable means of transaction. It lowers the transaction processing time or the clearing cycle. It eliminates the need of internet banking infrastructure (for fund transfer) by the banks. It maintains the confidentiality and integrity of the transaction details. It provides an improved customer service. This kind of e-Cheques management is not being developed and used in any of the Banks so far. This reduces the work load on bank to clear the e-cheques. In this work the concept of high security using some security algorithms has been used. These schemes ensure security of the e-cheque (messages) and the signatures can be verified using a digital signature. It is a flexible solution for any cryptographic system and security layers of wireless protocol, such as Hiper LAN/2 and WAP. The proposed design provides high-speed performance and minimized covered area.

FUTURE SCOPE

This project can be implemented on the large scale i.e. for large no of users. Help section can be inserted which can give any particular help and information regarding the facilities about the software. Also, messenger can be used which uses secret key for information exchange.

REFERENCES

[1] Yaser Esmaeili Salehani1, S. Amir Hossein A.E. Tabatabaei,Mohammad Reza Sohizadeh Abyaneh3, Mehdi Mohammad Hassanzadeh "NESHA-256, NEw 256-bit Secure Hash Algorithm" Sharif University of Technology, Tehran.

[2] Shay Gueron , Simon Johnson , Jesse Walker " SHA-512/256" Security Research Lab, Intel Labs, Intel Corporation, USA.

[3] Masoud Nosrati Ronak Karimi Mehdi Harir "Audio Steganography: A Survey on Recent Approaches" World Applied Programming, Vol (2), No (3), March 2012. 202-205.

[4] Ritu Pahal Vikas kumar " Efficient Implementation of AES" SGI Samalkha, Haryana, India Volume 3, Issue 7, July 2013.

[5] Tanmaiy G. Verma1, Zohaib Hasan2, Dr. Girish Verma3 " A Unique Approach for Data Hiding Using Audio Steganography" International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol. 3, Issue. 4, Jul - Aug. 2013 pp-2098-2101.

[6] Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay and Tai-hoon Kim, Text Steganography: A Novel Approach, Research paper , International Journal of Advanced Science and Technology, Vol. 3, February, 2009 .

[7] Arvind Kumar, Km. Pooja, Steganography- A Data Hiding Technique, Research paper , International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.
[8]Masoud Nosrati, Ronak Karimi, Mehdi Hariri, An introduction to steganography methods, World Applied Programming, Vol (1), No (3),August 2011. 191-195.
[9] Bender W, Gruhl D & Morimoto N (1996) Techniques for data hiding. IBM Systems Journal 35(3): p 313–336.
[10] Nedeljko Cvej, Algorithms for audio watermarking and steganography, Oulu 2004, ISBN: 9514273842.
[11] Sos S. Agaian, David Akopian, Sunil A. D'Souza1, Two algorithms in digital audio steganography using quantized frequency domainembedding and reversible integer transforms, USA.
[12] M. Matsui, "Linear Cryptanalysis Method for DES Cipher",EUROCRYPT, LNCS 765, pp.386-397, Springer, 1994.
[13] I. Ben-Aroya, E. Biham, "Differential Cryptanalysis of Lucifer", CRYPTO,Journal of Cryptology, pp.187-199, Springer, 1994.
[14] D. Wagner, "The Boomerang Attack, Fast Software Encryption", 6thInternational Workshop on Fast Software Encryption, LNCS 1636, Springer,1999.
[15] A. Biryukov, "The Boomerang Attack on 5 and 6-Round Reduced AES",LNCS 3373, pp.11-15, Springer, 2005.
[16] L. Knudsen, "Truncated and Higher Order Differentials", 2nd International Workshop on Fast Software Encryption, LNCS 1008, pp.196–211, Springer,1994.
[17] J. Daemen, L. Knudsen, V. Rijmen, "The Block Cipher Square", 4th International Workshop on Fast Software Encryption, LNCS 1267, pp. 149–165, Springer, 1997.
[18] T. Jakobsen, L. Knudsen "The Interpolation Attack on Block Ciphers", 4thInternational Workshop on Fast Software Encryption, LNCS 1267, pp.28–40,Springer, 1997.
[19] J. Daemen, V. Rijmen, "AES Proposal: Rijndael, Version2", http://www.esat.kuleuven .ac.be/vijmen/rijndael , 1999.
[20] Kazumaro Aoki and Yu Sasaki. Preimage attacks on one-block MD4, 63-step MD5 and more. In SelectedAreas in Cryptography'08, volume 5381 of Lecture Notes in Computer Science, pages 103–119. Springer,2008.
[21] Transferable e-cheques using Forward-Secure Multi-signature Scheme N.R.Sunitha, B.B.Amberker and Prashant Koulgi
[22]AN EFFICIENT IMPLEMENTATION OF THE DIGITAL SIGNATURE ALGORITHM P. Kitsos, N. Sklavos and O. Koufopavlou VLSI Design Laboratory Electrical and Computer Engineering Department University of Patras. Patras, GREECE E-mail: pkitsos@ee.upatras.gr
[23] An Introduction to Cryptography and Digital Signatures Author: Ian Curry March 2001 Version 2.0
[24] M.M. Amin, .M. Salleh, S. Ibrahim, M.R Katmin (2003), "Information Hiding Using Steganography", 4th National Conference on Telecommunication Technology Proceeding 2003 (NCTT2003), Concorde Hotel, Shah Alam, Selangor, 14-15 January 2003.
[25] Nameer N. EL-Emam, Hiding a Large Amount of Data with High Security Using Steganography Algorithm Applied Computer Science Department, Faculty of Information Technology, Philadelphia University, Jordan
[26] Bellare,M., Miner,S.: A Forward-Secure Digital Signature Scheme. In: Wiener, M. (eds.):National Institute of Standards and Technology (NIST), Digital Signature Standard, FIPS PUB 186-2, http://csrc.nist.gov/publications/fips/fips186-2/fips186-2.pdf
[27] Abdalla,M., Reyzin,L.: A New Forward-Secure Digital Signature Scheme. In: ASIACRYPT 2000,LNCS, Vol.1976, pp. 116-129. Springer-Verlag,(2000).
[28] Anderson,R.: Invited Lecture, Fourth Annual Conference on Computer and Communications Security,ACM, (1997).
[29] Bellare,M., Miner,S.: A Forward-Secure Digital Signature Scheme. In: Wiener, M. (eds.):Advances in Cryptology-Crypto 99 proceedings,LNCS, Vol.1666, Springer-Verlag, (1999).
[30] Advances in Cryptology-Crypto 99 proceedings,LNCS, Vol.1666, Springer-Verlag, (1999).
[31] Moerland, T., "Steganography and Steganalysis", *Leiden Institute of Advanced Computing Scienc*e,www.liacs.nl/home/tmoerl/privtech.pdf
[32] Silman, J., "Steganography and Steganalysis:An Overview", *SANS Institut*e, 2001
[33]Jamil, T., "Steganography: The art of hiding information is plain sight", *IEEE Potential*s,18:01, 1999
[34] National Institute of Standards and Technology (NIST), Digital Signature Standard, FIPS PUB 186-2, http://csrc.nist.gov/publications/fips/fips186 -2/fips186-2.pdf