Abstract— Nowadays, security plays a major role in communication. Security is the degree of resistance to, or protection from harm or viruses that corrupts the system. As there is tremendous increase in the use of internet and various communication channels, the issue of data or message security is arised. Digital signature is a technique that provides security to the data or message. In this paper we are going to survey on the digital signature. It is an electronic signature used to authenticate the identity of the sender and it assures that original content of the message or document received by the receiver is unchanged or same. The goal of the paper is to study the various digital signature methods proposed recently to secure the data transmission.

Keywords- Digital signature, Security, Public key, Private key

I. INTRODUCTION

The documents are commonly authenticated by the signature. Even when the document is signed physically one is authenticating its contents. In the same manner digital signature is a method which is used to authenticate the contents of the electronic documents, which can be used with PDF, e-mail, word processing etc. in this digital ID is required for signing documents. This ID can be obtained from various certification authorities on the web like the VeriSign and EchoSign. The documents you sign contains the digital signature which is simply a small block of data. It is generated from the digital ID that includes public key and private key. The signature is applied to the document with the help of private key while the public key is send to the file. Encrypted code is introduced in public key that verifies your identity. There are four classes of digital signature[15]:

Class 0: In this certificate is issued for demonstration.

Class 1: This certificate is issued to the private subscriber. It will confirm that the user name and e-mail address form no duplication within the certifying authorities database.

Class 2: This certificate is issued for both business as well as private use. The task of this certificate is to assure that the information provided by the subscriber will not conflict with the information in well known consumer database.

Class 3: This certificate will be issued to the individuals as well as organizations. As the class 3 certificates is high assurance certificate which is intended for e commerce applications. It should be issued to an individual only on its physical appearance before the certifying authorities.

In above figure signature generation and signature verification are carried out. For signature generation private key is used and for signature verification public key is used. For message transfer Hash function is used after that message is digested. For signature generation private key is used then signature generation is created. This signature generated is transferred for verification. After verified valid or invalid result is obtained.

There are three algorithms that are used for digital signature generation under the DSS standard.
1) DSA(Digital Signature Algorithm)
2) RSA(Rivest Shamir Adleman)
3) ECDSA(Elliptic Curve Digital Signature Algorithm)
Also hash function is used in the signature generation process, which is used to obtain message digest that is condensed version of the data. This message digest is put in to digital signature algorithm to generate the digitally signed message. In the verification process same hash function is used.

II. RECENTLY IMPLEMENTED TECHNIQUES FOR DIGITAL SIGNATURE

2.1 Method of securely transferring programmable packet using digital signature having access controlled high security verification key[1]:

Programmable network represents a new approach to its network architecture. In programmable network nodes can perform the various calculation with respect to user data. For the calculation purpose users provide their programs to their nodes. So programmable networks are useful to add and provide new services without physical action or hardware modification. Sometimes programmable network raise some security problems. To avoid this problem cryptographic technique is used. At programmable network environment, programmable packet contains programmable codes. Which should perform computations on intermediate node as well as end nodes. So proposed system provides a method of securely transferring programmable packets. By which programmable nodes are verified using digital signature having a high security signing key. This paper also provides a method by which a storage server for verification keys is provided and only authorized programmable nodes verify signature and execute codes.

2.2 New Certified Proxy Digital Signature Scheme based on Elliptic Curve Cryptosystem [3]:

This paper gives the solution to the problems such as low work efficiency and weak in delegation authority control. Which were in the existing proxy digital signature scheme. Proxy digital signature scheme means it simulates the function of seal to transfer the digital signing power to another authorized agent. It uses the public key self certified system i.e only one step is required to complete the process of verification of digital signature. It reduces the storage and computing cost. The proposed self certified proxy digital signature scheme is based on the discrete logarithmic over elliptic curve group. Elliptic curve cryptography is an approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields.

The proposed scheme is divided into three phase digital signing power delegation phase, the proxy digital signature generation phase and proxy digital signature verification phase. This covers all the operations such as verifying the warrant, verifying the proxy digital signature signed by proxy signer and verifying the certificate of original signer.

2.3 Code – Based Designated Verifier Signature Scheme [5]:

In this paper author introduced a new designated verifier signature scheme, It allows a signer to convince only. The designated verifier the sign message is authentic. Designated verifier signature scheme based on CFS signature and stern identification scheme whose security depends on syndrome decoding problem. The CFS means Courtois, Finiasz and Senderier. This scheme based on difficulty of decoding linear error correcting codes. In CFS mechanism involves sampling random syndromes. The code-based designated verifier signature scheme prove that the sign message is authenticated. The proposed scheme is first code-based designated verifier signature and it also satisfies unforgeability and distinguish ability which are require for a designated verifier.

2.4 An Improved Digital Signature Scheme with Fault Tolerance in RSA[6]:

In this paper the author proposes a scheme that can efficiently keep confidentially transfer the message and also review a digital signature scheme with fault tolerance based on RSA cryptosystem proposed by Zhang’s scheme. It used for secure data transmission. RSA stand for Ron Rivest, Adi Shamir and Leonard Adleman. In RSA cryptography two keys are used public key and private key. The public key is used for encryption and private key used for decryption purpose. Zhangis scheme has several weakness that violates the principle of secure digital signature and it has serious vulnerability. The vulnerability is the cyber security, It defines any type of weakness in computer system itself, in a set of procedures or anything that leaves information security expose to thread. The author meets all the requirements for digital signature and maintains the fault tolerance function in Zhang’s scheme.

2.6 Comment on a Digital Signature Scheme with Using Self Certified Public keys [4]:

In this paper the author Tseng et al proposed a digital signature scheme with using self certified public key. The self-certified public keys is one in which both public key and certificate are combined as one piece of information.
The primary of this system is that it reduce the overhead of having a separate public key. With the help of self certified public key, the verification signature and public key can be carried out in a logic step. Unfortunately, Shao et al showed that the scheme was insecure and gives an improvement scheme. In this we analyze security of Shao et.al scheme and his attack and show that the attack is not powerful and the improvement scheme can not resist man-in-middle attack. This attack is very frightful over the internet transactions

2.7 Importance of cryptography in network security [7]:

This paper gives a broad review of cryptography and digital signature. Cryptography is used to protect the information in digital form and is used to provide the network security. Digital signature provides means for an entity to bind its identity to a piece of information. Digital signature provides authentication, data integrity and non-repudiation. Cryptography protects data from theft or alteration and also used for authentication purpose. In cryptography plaintext is converted to ciphertext using key and algorithms. So no one can get plaintext from ciphertext without knowing the key for decryption easily. paper includes various attack methods like known plaintext and ciphertext attack, chosen plaintext and chosen ciphertext attack etc. cryptography was used to conceal the diplomatic and military secrets from enemy. But it is being used to secure large amount of electronic data that is stored on the corporate networks. Cryptography is means for protecting data while maintaining the privacy of confidential data like financial, personal and medical.

2.7 A secure proxy signature scheme in bilinear group [10]:

Proxy signature is one of the vital aspects of digital signature. Proxy signature scheme is a tuple (key gen, sign, verify, delegate, proxy sign, proxy verify, identify) where the algorithm runs in polynomial time. A proxy signature protocol allows an entity called original signature to delegate signing power to another entity called proxy signer to sign messages on its behalf. Proxy signature is useful to design cryptographic protocols. This paper proposes a new provable secure proxy signature scheme based on Gap Diffie Hellman (GDH) group. GDH is obtained from bilinear pairings. GDH is a group in which problem is easy but Computational Diffie Hellman (CDH) problem is hard. Though there are many other proxy signature schemes the method in this paper is easy and simple and the technique of bilinear map and traditional certificate based signature scheme is being used.

Bilinear map are the tools of pairing based cryptographic groups. The resulting scheme is based on two notations and also security analysis and definition are given. The scheme has low computational cost of signature generation. Hence suitable for low bandwidth environment. Thus the bilinear pairing is presented by using a certificate based scheme and proves its security in the random oracle model.

2.8 A new attack method on digital signature scheme [11]:

This paper describes a new attack method on digital signature scheme. There are some signature schemes which have design defects and can be broken through this method. This method will propose some signature datum (i.e. actual information derived from measurement or research) into identical base datum, and anyone can employ this way to attack and come up with or forge a valid signature. In this the author present four examples and indicates their problems of insecurity or security flaws under the attack based on identical base construction.

1. Awashti-Lal signature scheme: it is a proxy blind signature scheme.

2. Duc-Cheon-Kim signature scheme: it is a forward security blind signature scheme, which alleviate (make easy) the severe consequences brought by the secret key leak.

3. Tseng-Jan signature scheme: it is an example of group signature and has potential security flaws.

4. Xue-Cao signature scheme: it is also a proxy blind signature scheme. It consists of original signer, proxy signer and signature receiver.

So in this process of designing the signature protocols the security flaws are avoided.

2.9 New Blind Signature Schemes Based on the (Elliptic Curve) Discrete Logarithm Problem [12]:

Blind signature scheme is a kind of digital signature with significant application in anonymous electronic voting and electronic payment. In this the recently introduced blind signature scheme is analyzed and also show that without obtaining the signing key, the attacker can forge a valid signature for any arbitrary message. Damari in 2012 proposed a new blind signature scheme based on ElGamal signature claimed that their scheme is secure against forgery attack. This scheme is universally forgeable.
Then a new blind signature scheme is proposed based on hardness of discrete logarithm problem and the other which inherits the efficiency of elliptic curve cryptosystem (ECDLP) and is elliptic curved based variant of the proposed system which has lower computational overhead. These schemes are unforgeable, blind and untraceable. Hence they are appropriate candidates to be employed in protocols such as untraceable e-payment or e-voting and this scheme is more efficient one.

III. CONCLUSION

For security measures, standards has, followed, in this system which improves security. Digital signature enhances more security and guarantees efficient and powerful message security mechanism. Today digital signatures are under way and can only be seen as an amendment to traditional procedures. In the future digital signature will get more and more importance to guarantee an efficient action of public authorities. The security standard has to be followed to the computer systems that get increasingly powerful.

REFERENCES


[13] https://www.google.co.in/?gws_rd=cr&ei=2oucUoaEL4aOrQenoYGI#q=what+is+meant+classes+of+digital+signature.

AUTHORS

First Author-- Anita Gaikwad, BEIT, RSCOE, anitagaikwads25@gmail.com

Second Author-- Kajal Bhise, BEIT, RSCOE, kajal.bhise21@gmail.com

Third Author-- Prof. Dipmala Salunke, ME Comp, dipmala.salunke@gmail.com

Fourth author-- Varsha Bangar

Varshabangar94@gmail.com

Correspondence Author-- Shraddha Kalbhor, BEIT, RSCOE, shraddha.kalbhor000@gmail.com , 8378980300