ISSN 2277-3061
Volume15 Number 8
International journal of computer and technology

A Review of Digital Signature Using Different Elliptic Cryptography Technique

Anurag Singh Bhadoria
M.Tech Scholar, CSE
RITS,Bhopal, India
abhadoria982@gmail.com
Anurag Jain
Department of CSE
RITS,Bhopal, India
anurag.akjain@gmail.com

Abstract
Authentication and verification of digital data is important phase in internet based transaction and data access. For the authentication and verification used digital signature operation. For the operation of digital signature various cryptography techniques is used. The strength of cryptography technique measures the strength of digital signature. For the strength improvement various cryptography techniques is used such as RSA, ECC and some other bit level cryptography technique. In this paper present the review of digital signature technique basically based on elliptic curve cryptography technique. The elliptic curve cryptography technique is much stronger than other cryptography technique.

Keywords
Cryptography, Digital Signature, ECC

Introduction
The processes of authentication of digital data over internet checks and verify the content of data received by the receiver is original and not tampered. For the process of authentication used various cryptography techniques. Some cryptography technique based on symmetric key cryptography and some are based on asymmetric key cryptography. The process of digital signature authenticates the data and content of message from the both side sender and receiver. In the process of sender and receiver send the electronic document for another party. For authentication of sender and receiver used various message protocol by different user in concern of content validation. But the process of message authentication is not compete process of digital signature. Now a day's various method and algorithm are used for development of digital signature. In conventional digital signature used RSA based cryptography technique. The security strength and validation of content is big issue in digital signature. For the improvement of the strength of digital signature used various cryptography and hash function. The hash function gives the data tampering information of receiver tampered by third party and intruder. Now a day's various authors used cure based function for the authentication of digital signature. The curve cryptography technique is provide more security strength instead of normal and some other cryptography technique. The curve cryptography technique is used point and coordinate distribution function for the mapping and signature of data. The public-key cryptosystem gives rise to a new and remarkable idea, which is the concept of digital signature. The digital signature is the electronic analog of the handwritten signature. A signer can digitally sign a document with his/her secret key (Private Key), and generates a signature on that document. Then, he/she sends the generated signature, a document and his\her public key to any verifier. Therefore, a verifier can check the validity of the signature with the corresponding public key. Note that, any involved party must register his public key with a central authority, which is known as the Certificate Authority (CA). Section II discusses about cloud computing overview and description, Section III discusses about the related work. Section IV discusses problem formulation and finally, concluded in section V.

II. Digital signature
Signature is important issue in verification of document for legal process. The importance of hand writing and electronic signature is same. But the hand written signature is more secured and authenticated by electronic digital signature. But the all recognized government gives the permission of electronic data as legal document so the importance of digital signature is increase. The security and authentication process is big issue in digital signature for the verification of signature and document. For the authentication of digital signature used cryptography technique. The cryptography technique gives the algorithm for the protection of digital signature. The process of digital signature used private and public key concept given in figure 1 and figure 2.

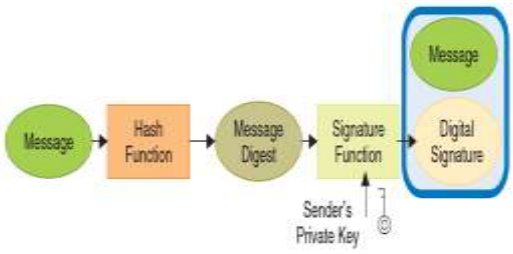

Figure 1 shows that process of digital signature

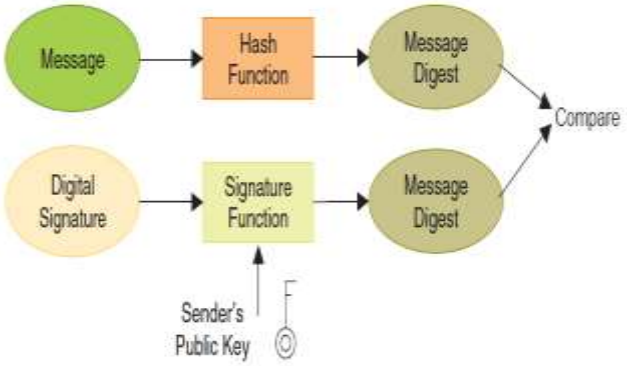

Figure 2 shows that verification process of digital signature

III Related work

In this paper [1] authors describe the concept of blind signature based on the process of anonymity of coins. Basically the property of coin is uncertain on the basis of probability. For the blind signature process used ECC cryptography technique for the distribution of key. The distribution policy of ECC cryptography technique is very robust and stronger.
In this paper [2] authors describe the process of proxy encryption based signature technique based on ECC cryptography technique. The authors proposed technique reduces the communication and computational time approx 30%. The proposed technique achieve the all other security principle and credential for the process of digital signature and authentication.
In this paper [3] authors describe the improved protocol for the application of digital signature. The proposed digital signature model based on the process of elliptic curve cryptography. The proposed algorithm design for the process of Islamic information center. The analysis report of ECC algorithm is very robust in terms of security strength. The much security strength improved the capacity of digital signature.
In this paper [4] authors describe the process of mutual authentication technique and key management for the particular process and application for the purpose for verification. The design technique and application used for the wireless sensor network application. the proposed technique used for the session based application.
In this paper [5] authors used encryption technique for the online payment system. The online payment system required the authentication process of digital signature. The digital signature used RSA based encryption technique. The RSA based encryption technique faced a problem of factorization. The estimation of factorization process is very difficult and complex for the generation of key.
[6] In this paper we show that Yang et al.'s both authenticated encryption scheme and e-payment system are vulnerable to impersonation attack. An attacker after acquiring the public key and identities of the participants can easily masquerade as legitimate user. Then, we presented improvements over both Yang et al.'s authenticated encryption and e-payment schemes. We analyze the security of proposed schemes using widespread automated tool ProVerif.
[8] In this paper, we launch a new signcryption scheme based on elliptic curve which fulfills all properties of security goal like message authentication, integrity, public verification, unforgeability and non-repudiation. If the sender discloses the private key no one can extract the original message. It also provides verification process by third party to know about the sender. This signcryption scheme saves computational cost and communication overhead than the traditional signature-then encryption scheme. The scheme is implemented using java which generate key by choosing a random point on the elliptic curve which makes more secure. The implemented scheme can be useful for e-commerce environment.
In this paper [9] authors describe the process of authentication and security technique for the digital data over the internet. The design algorithm verifies the user authentication and content of digital data. The signature based authentication technique used different cryptography method.

In this paper [10] authors describe the process of digital signature verification method based on the process of curve cryptography technique. The curve cryptography technique provides the more security strength for the digital signature. The design digital signature method used the concept of third party auditing technique. the third party auditing technique encompassed the process of mutual participation.
In this paper authors [11] describe the ID based sign verification technique for the process of identification. The proposed ID based digital signature used for proxy based server. The proxy based server precedes the authentication process of transaction data.

IV Problem Formulation

In this section discuss the problem related to digital signature. The process of digital signature basically based on the combination of different cryptography technique. in digital signature the major role is generation of key for sender and receiver.
In the process of review study various research papers related to digital signature verification and authentication technique using different cryptography technique. The security strength and integrity of data is major issue in sender and receiver side. The authentication of sender and receiver used message control protocol for the purpose of authentication. Here discuss some limitation of cryptography technique used in the process of digital signature.

1. The RSA encryption based digital signature technique is more time consuming process form other. The process of authentication of signature based on public key. Here not involved any private key technique for the purpose of authentication.
2. The ECC based digital signature technique is very much efficient instead of RSA based technique. but the process of computational time is very high. And also the distribution of key is very complex process.
3. The ID based digital signature technique is very week security strength and easily predictable for attacker and third party.
4. The proxy based digital signature technique used for the local authentication technique. the local authentication technique not provide the content validation process.
5. The combination of key technique is much stronger than some other technique used in digital signature.

V conclusion & Future Scope

In this paper present the review digital signature based on cryptography technique. In the process of public cryptography system various public key generation algorithm are used. The generation of key for the purpose of encryption and decryption it is very crucial section. Now a day's researchers are trying to increase the performance of RSA in terms of Time and security. some such important techniques which are followed by researchers. The aim of this paper is to bring into the notice of upcoming researchers regarding various RSA implementation techniques which are already made. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security.

References:-

[1] Srikanta Pradhan and Prof. Sanjay Kumar Jena "Proxy Blind Signature using Hyperelliptic Curve Cryptography", 2013, Pp 1-37.
[2] Insaf Ullah, Inam Ul Haq, Noor Ul Amin, Arif Iqbal Umar and Hizbullah khattake "Proxy Signcrypion Scheme Based on Hyper Elliptic Curves", International Journal of Computer, 2016, Pp 157-166.
[3] Shehzad Ashraf Chaudhry, Husnain Naqvi, Taeshik Shon, Muhammad Sher and Mohammad Sabzinejad Farash "Cryptanalysis and Improvement of an Improved Two Factor Authentication Protocol for Telecare Medical Information Systems", Springer, 2014, Pp 1-11.
[4] Gaurav Indra and Renu Taneja "A time stamp-based elliptic curve cryptosystem for wireless ad-hoc sensor networks", Int. J. Space-Based and Situated Computing, 2014, Pp 39-54.
[5] Shehzad Ashraf Chaudhry, Mohammad Sabzinejad Farash, Husnain Naqvi and Muhammad Sher "A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography", Springer, 2015, Pp 1-27.
[6] Mohammad Heydari, S. Mohammad-Sajad Sadough, Mohammad Sabzinejad Farash and Mohammad Reza Aref "An Improved Authentication Scheme for Electronic Payment Systems in Global Mobility Networks", INFORMATION TECHNOLOGY AND CONTROL, 2015, Pp 387-403.
[7] Shehzad Ashraf Chaudhry, Khalid Mahmood, Husnain Naqvi andMuhammad Khurram Khan "An Improved and Secure Biometric Authentication Scheme for Telecare Medicine Information Systems Based on Elliptic Curve Cryptography", Springer, 2015, Pp1-12.
[8] Biswajit Sama, Sumanjit Das and J. Chandrakanta Badajena "A Java Implementation of Signcryption Protocol Based on Elliptic Curve", International Journal of Computer Science and Information Technologies, 2013, Pp 302-305.
[9] Sumanjit Das1 and Prasant Kumar Sahoo "Cryptanalysis of Signcryption Pr otocols Based On Elliptic Curve", International Journal of Modern Engineering Research, 2013, Pp 89-92.
[10] Sumanjit Das and Biswajit Samal "An Elliptic Curve based Signcryption Protocol using Java", International Journal of Computer Applications, 2013, Pp 44-49.
[11] Graham Enos and Yuliang Zheng "An ID-based signcryption scheme with compartmented secret sharing for unsigncryption", Information Processing Letters, 2015, Pp 128–133.
[12] Charalampos Manifavas, George Hatzivasilis, Konstantinos Fysarakis, and Konstantinos Rantos "Lightweight Cryptography for Embedded Systems - A Comparative Analysis", Springer, 2014, Pp 333-349.
[13] Sumanjit Das, Santosh Kumar Sahu and Santosh Narayan Pati "A Novel Signcryption Scheme Based on ECC with Public Verifi-cation and Encrypted Message Authentication", International Journal of Advanced Research in Computer Science & Technology, 2014, Pp 72-78.
[14] Reza R. Farashahi, Pierre-Alain Fouque, Igor E. Shparlinski, Mehdi Tibouchi, and J. Felipe Voloch "Indifferentiable Deterministic Hashing to Elliptic and Hyperelliptic Curves", Journal: Mathmatics of Computation, 2013, Pp 1-18.