iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6006

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

Digital Signature - The Security Tool

Md. Aquib Ali
School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh – 201306.

Abstract: ***Running towards the best technology and using technology for everything is now a trend. Usage of internet is the easiest and accessible technology we are having. The Information Technology Act 2000 (IT Act), Indian law dealing with cybercrime and electronic commerce, describes digital signatures as a means of authentication and security of electronic documents. Digital signature refers to an electronic receipt that creates link between an entity and data record, serving the purpose of verification and authentication of an electronic document. Verification of an electronic document means the process of certifying the contents of the document, while authentication means the process of certifying the sender of the document. Any handwritten signature when used in its electronic version referred as a digital signature. A valid digital signature creates believe that the message was created by a known sender, that the sender cannot deny that he sent the message and that the message was not changed in transit. This helped in increasing the use of digital technology in daily life which has increased technology dependency. Confidential messages, software distribution, cases where it is important to detect forgery or tampering are the fine examples where the digital signature has its use. It provides the services of verification, authentication and data integrity.***
Keywords: Electronic commerce, Authentication, Information technology, Verification.

I. INTRODUCTION

Presently, world is moving towards the extreme use of technology. Internet is now one of the basic elements of our day to day life. Communication, trade, banking services etc. are being done through internet. So the security while using internet becomes crucial. To achieve the Verification, authentication and security of electronic data or message digital signature is used.

Below provided with some of the security requirements that should be accounted while having communication on internet:

1) *Authentication:* Sender and recipient must be correctly identified.
2) *Integrity:* Electronic data should be verified i.e. the data should be unchanged after being sent from the sender and before the receiver get it.
3) *Confidentiality:* For example, financial data must be accessible by nobody other than the intended receiver. This is known as secrecy. The date should be out of the hands of unauthorized person.
4) *Non Repudiation:* Denial of the data cannot take place from both the side (sender or receiver).
5) *Availability:* Resource should be available to authorized person all the time.

In traditional system stamps, seal or signature creates the authentication of paper document, in the same way the digital signature plays the role of authenticating the electronic record. Subscriber can authenticate any electronic record by affixing his digital signature. A digital signature represents a handwritten signature on a paper printed document. Key pair is distinctive advanced keys used to create digital signature. The key pair consists of a private key and a public key. Both are interdependent. Separate use of these keys is also possible. Normally a key pair is specified for a key holder. The algorithm is so complicated so that a third party cannot derive it.

II. LITERATURE REVIEW

Digital Signature is an electronic signature that encrypts document with digital codes that are difficult to duplicate. Cryptographic method is used to create digital signature.

Digital signature helps to show the ownership to the electronic data. By using Key pair algorithm and hash functions digital signature can be implemented.

Digital signature helps to maintain a trust level between any two users.

Figure 1 shows the concept how digital signature is created. After the sender has written his message and is sending it for signing, the message is hashed and by the use of private key digital signature is attached to the message.

Figure 2 shows how the receiver can use public key to verify the message.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

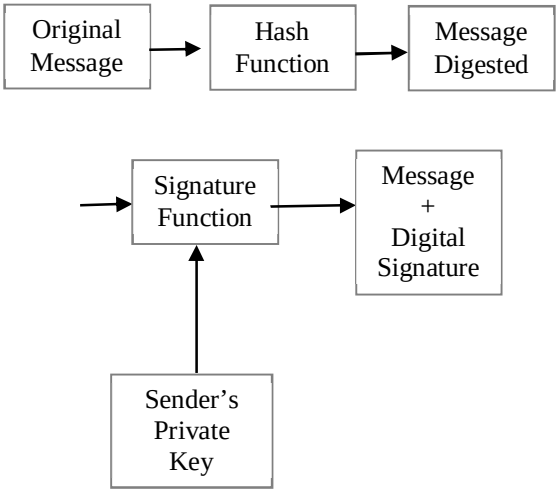


Figure 1- Steps to generate digital signature

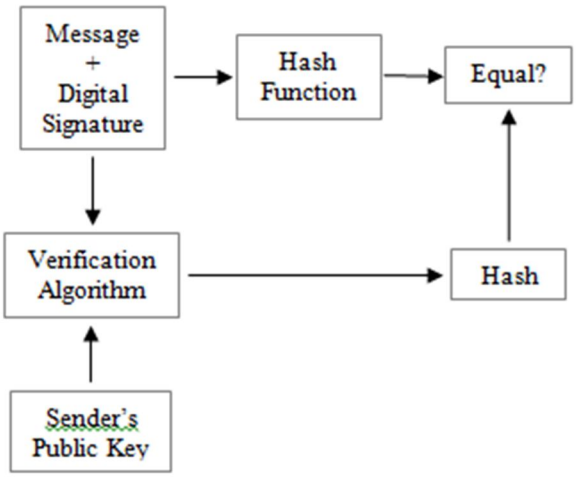


Figure 2- Steps to verify digital signature

The point to notice in this is that the original message is not being signed directly, it is first hashed then signed. Because the hash code of the message is unique representation of it. This makes the scheme efficient.

Basic requirements of appending 'Digital Signature' are:

A. Create Authenticity

To have a check on authenticity of a message we use digital signature. Digital signature empowers the receiver to verify the sender of the message. A user has a specific digital signature so a message sent by a specific user has a particular digital signature. This helps in verifying any digital material sent by the user. The authenticity of the sender makes him responsible for the message i.e. he or she knows about the content in the message and later cannot deny about it. Digital signature also keeps a check on the authenticity of the content of message. Suppose, it just verify the sender's information but there is no check on content of message and anyhow content is being altered after the signature then sender's objective is not fulfilled. If the content is altered the whole meaning of the message may get changed. Any document with valid digital signature cannot be altered without invalidating the signature. Receiver has the power to check the validity of the digital signature. This empowers the sender with capability to modify or change the document or the message.

So the authentication of sender and document both are necessary and is being fulfilled by digital signature.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

B. Non-repudiation

Any document with a digital signature can be verified by the receiver. Having a valid digital signature on the message or the document is equal to the traditional handwritten signature system. Likewise, this makes the sender fully responsible for the message or the document. Thus, denial to any digitally signed document cannot take place.

So if a valid digital signature is appended with the document the sender cannot deny that he or she sent the particular document. And as the receiver checks the validity of the digital signature he or she cannot deny being an incorrect receiver. Moreover, he or she cannot modify the content of the document makes him or her safe to be in a wrong place.

C. Key Management

This security scheme uses a key pair i.e. Public Key and Private Key. The public keys are in open domain and likely to be abused. So it is necessary to have a trustable infrastructure to manage these keys.

Key points for this management system:

1) *Secrecy of Private Key:* Private keys should remain secret their life cycle. Owner and the people who are authorized to use them should know the private keys.
2) *Assurance of Public Key:* As public keys are in an open domain, they are seen as public pieces of data. It is important to know whether the public key is correct or not, with whom it can be associated, or what it can be used for. To fulfill this purpose Public key infrastructure (PKI) is there.

Public key infrastructure compromises the following:

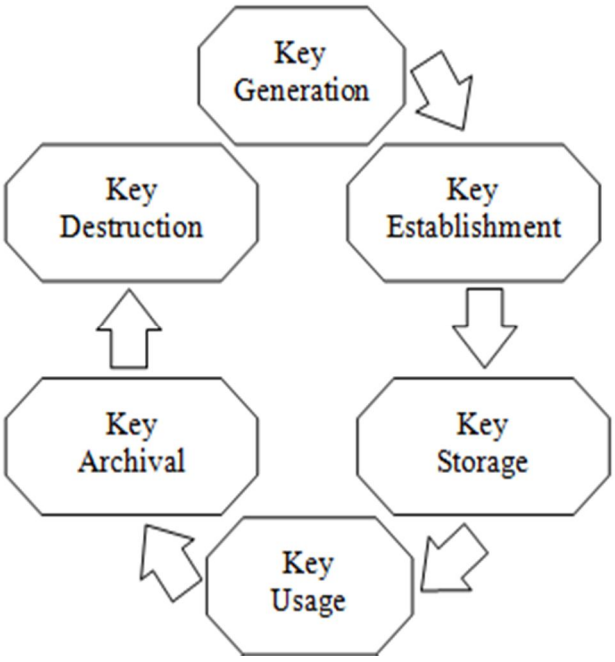


Figure 3- Lifecycle of a key

a) *Public Key Certificate / Digital Certificate:* It plays the same role as of an identity card in human world. It is not just issued to identify the identity of a person but also can be issued to computers, or anything that needs to prove its identity in electronic world. As is based on ITU standard X.509 (defines format for public key certificates and certification validation), sometimes it is also called X.509 certificates. Public keys are being attached to the certificate by certification Authority and also attach the necessary information like client information, expiration date etc.
b) *Private Key Tokens:* Hardware devices that digital certificate and private keys securely. To escape the risk of keys been stolen, everything is been done internally in a secure chip whether it be encryption, decryption or signature.
c) *Certification Authority (CA):* As name suggested, it is an authority to issue digital certificate to a client. It also helps users to verify the certificate. It is responsible to identify correctly the identity of client also has a check on the information in the certificate.

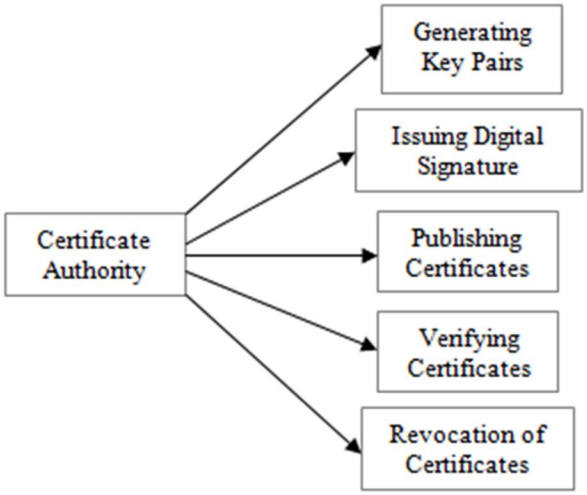


Figure 4- Functions performed by Certificate Authority

CA generates the Key pairs as an individual or sometimes with the client. It issues the digital certificate to the client after the client is able to proof his or her identity. To ensure that this digital certificate is not modified later it signs the certificate too. After the certificate is being issued that needs to be published as well and this is also been done by CA. To verify the digital certificate CA assists with its public keys. Anyhow if CA looses the trust in client for his or her identity or there might be some other reason, it revokes the certificate.

d) *Registration Authority (RA):* To have a check on the user requesting for the digital certificate CA uses RA for that purpose. It is same as we want to joint any organization and there is a registration desk which ensures the identity of the person who wants to join the organization.

e) *Certificate Management System (CMS):* This management system ensures the publication, temporarily or permanently suspension, renewal or revocation of certificate. CA and RA collectively run this system.

III. DIGITAL SIGNATURE APPROACHES

A. RSA approach

RSA, named for Ronald Rivest, Adi Shamir, and Leonard Adleman, the developers of the algorithm, is a public-key encryption algorithm. In this approach the message is first converted into Hash by applying hash function on that message. This hash code is of a fixed length. This code is then encrypted using sender's private key to form the signature. Now this message and signature both are sent to the receiver. The receiver then produces the hash of the message and decrypts the signature using sender's public key. If the hash code calculated and decrypt of signature matches then the signature is said to be valid. Because the signature is created by the sender's private key this is only known by him.

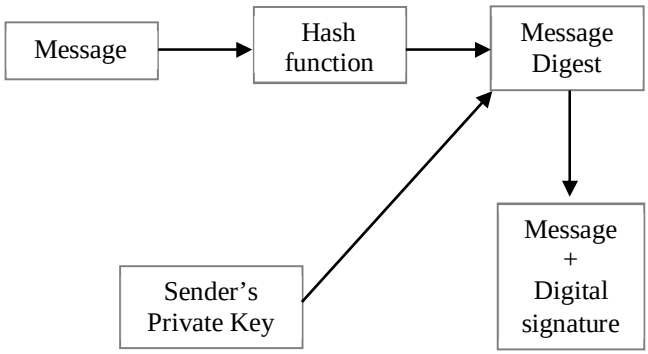


Figure 5- Generation of digital signature with RSA approach.

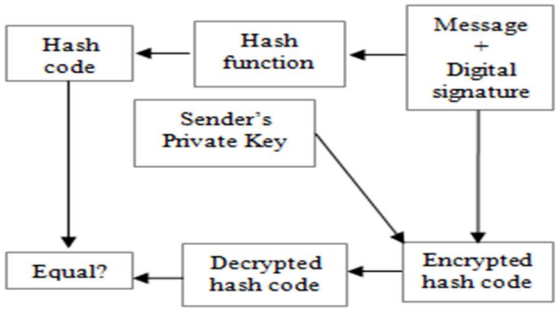


Figure 6- Verification of digital signature with RSA approach.

B. DSS Approach

Digital Signature Standard (DSS) approach is quite similar to RSA approach. In this approach the message is first converted to hash code using hash function. Now this hash code and a random number which is generated for this particular signature is being input to the signature algorithm. For signature algorithm a set of parameters known as group of communicating principals along with sender's private key is used. This generate two elements of signature 's' and 'r' along with the message. Now this is sent to the receiver. The receiver then produces the hash code of message using hash function. This hash code along with signature elements 's' and 'r' are used as the input to the verification algorithm. For verification algorithm again the group of communication principals is used along with the public key of sender. The output of this and the signature element 'r' is then compared to verify the signature.

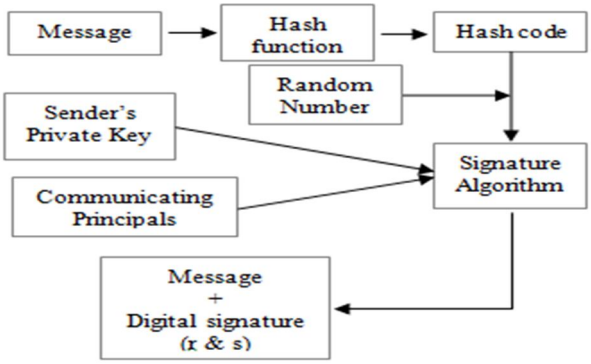


Figure 7- Generation of digital signature with DSS approach.

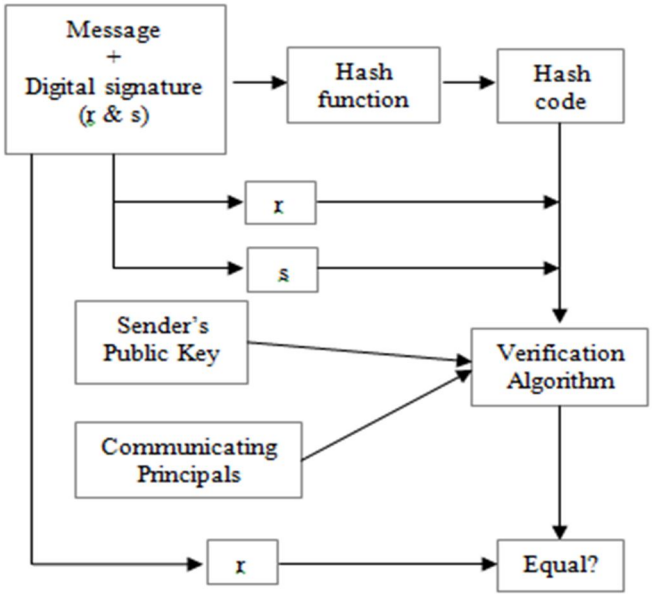


Figure 8- Verification of digital signature with DSS approach

IV. ADVANTAGES OF DIGITAL SIGNATURE

1) *Security:* Use of digital signature made electronic documentations more secure. Reduce the risk of document being altered while in transit.
2) *Costs:* digital documentation is less costly than physical documentation.
3) *Speed:* 'Time is money'. The time to send a physical document by any means is much higher than electronic means.
4) *Authenticity:* As the physical signature is being replaced by digital signature in an electronic document, the validity of the electronic document stands the same as of physical document even in courts.
5) *Tracking:* Tracking the location of the digital document is easier.
6) *Non-Repudiation:* Producing a digital signature by use of private key that is just being known to the sender cannot deny about the document later.
7) *Imposter Prevention:* As the private key is just known to the sender, no other person can forge the document.
8) *Time-stamp:* By time stamping your digital signature, you clearly know when the document was signed.
9) *Legal:* Government authorities have certified the authority which issues the certificate.

A. *Disadvantages of Digital Signature*

1) *Expiry:* Now days, technology advancement is one of the basic step towards development. So the tech products have short shelf life. Same is with the technology on which digital signature is based on.
2) *Certificates:* For the effective use of digital signature, both sender and receiver have to buy certificates at some cost.
3) *Software:* Verification software needed to be bought to work with digital signature.
4) *Law:* If the laws regarding cyber-crime and technology based issues are weak or not existing, the use of digitally signed electronic document is very risky.
5) *Compatibility:* Having many different digital signature standards, out of those most are incompatible with each other creating complication in sharing digitally signed documents.

V. CONCLUSION

The traditions ways are now rapidly converted to the digital ways as they are much faster and easy to access. Even the documentations are also heading towards electronic means rather than physical. However some documentation is still valid in its physical forms. The excessive use of digitalization is making it compulsory to have a check on security. Digital signature is one of the technologies that help to maintain a trust level. This trust level should keep increasing as the use of digital signature is also using rapidly. New mechanism to enhance the security levels of digital signature is a need of present era. Strict laws regarding cyber-crime will help in increase in digitalization. Use of digital signature is described in this paper. How the digital signature works and what are the basic approaches on which it works is also shown in this paper.

A. *Future scope of Digital Signature*

Under below are mentioned some future scopes:

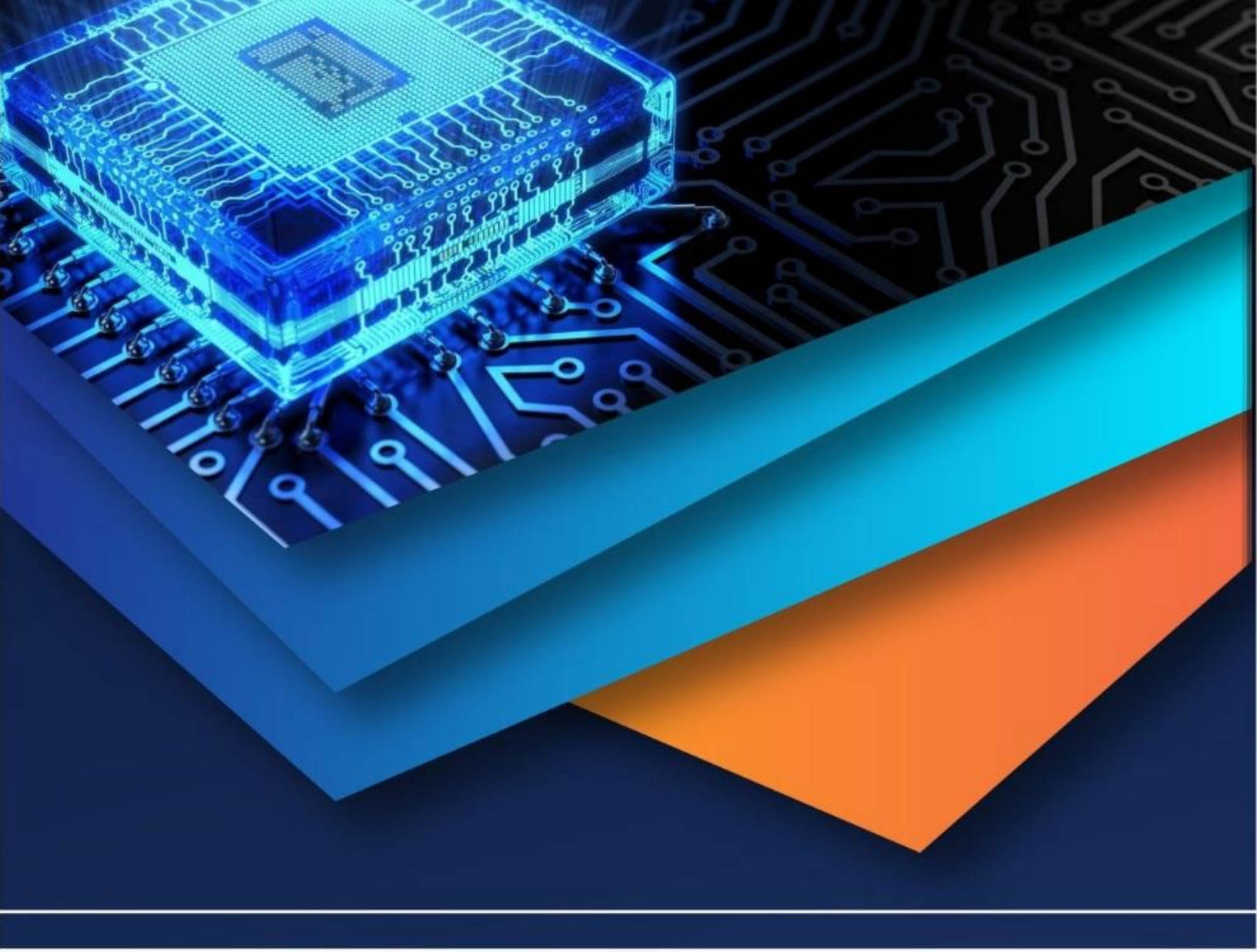
1) Quantum digital signature, established from the laws of quantum physics, is an area of ongoing significant researches. The advancement in this area will provide protection against tampering, even from the parties in possession of quantum computers.
2) To faster the operations related to produce digital signature, RNS digit exponent will be used.
3) The pool proof method during an electronic transaction will exist by display of a unique code. This code will be in the screen of a digital video to validate that the sender is alive.
4) Factoring and discrete logarithm will be used in the novel digital signature scheme that will prove the security of digital signature.

VI. ACKNOWLEDGEMENT

I would like to thank Dr. Vajenti Mala for her valuable suggestions and comments that helped me in this work.

REFERENCES

[1] Saha (2016). A comprehensive study on digital signature for internet security. ACCENTS Transactions on Information Security. https://www.accentsjournals.org/PaperDirectory/Journal/TIS/2016/1/1.pdf
[2] Yadav, Srivastava, Trehan (2012). Digital signature. International Journal of Engineering and Management Science. http://scienceandnature.org/IJEMS-Vol3(2)-Apr2012/IJEMS_V3(2)6.pdf
[3] https://digitalsignaturescertificates.wordpress.com/2015/01/21/merits-and-demerits-of-digital-signature-certificate/
[4] https://www.tutorialspoint.com/cryptography/public_key_infrastructure.htm
[5] http://docshare.tips/advantages-and-disadvantages-of-digital-signature_58898e27b6d87f3e478b4b25.html
[6] https://www.dqindia.com/digital-signatures-theyre-future/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY