International Research Journal of Commerce and Law
Volume 6 Issue 05, May 2019 ISSN: 2349-705X Impact Factor: 4.616
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

RESOLUTENESS OF DIGITAL SIGNATURE: ISSUES AND CHALLENGES.

Dr.Itishree Mishra

Asst.Professor, SNIL

SOA (Deemed to be university)

Abstract

This paper tries to focus on the area of cyber law applicability in different area of intervention in life through network. The authenticity of digital document with help of different digital or electronic signature whether is admissible in the court of law to render justice to the common individual .It intends to look into the selected legal issues on digital signature and technical aspects of digital signature. What are the issues relating to this signature authenticity is at question have been tried to solve with the help of this article in order to control cyber crime committed by tampering the document as well as signature. Suggestions and recommendations are also made to improve the effectiveness of the present recognised digital signature system in protecting and solving the above issues.

Introduction:

The emergence of cyber law in India and the convergence of computer network, telecommunication facilitated by digital technologies have given birth to a common space called cyber space. This space allows a platform of human activities which converge on internet. The most happening space in the world is the cyber space .Now is the era of internet, life without internet seems to be impossible. With advancement of internet we can communicate-commerce is possible, education, banking transaction is also possible.Everthing has its own advantage and disadvantage. Lots of traditional crime is being committed through internet from hacking to indecent representation of women in internet medium and in order to control this IT Act has been framed but how far the law is being enforced is at question to control the crime rate.

The ratio of crime is increasing at a much faster rate it's the need of the hour to control crime. Therefore internet has something to perform to everybody and in the process it never increased as such.

For every transaction or business that is being conducted, the level of security is always the main concern in determining the successfulness for these activities. According to Davis and Benamati (2003) security is the quality or state of being secure which includes "freedom and danger" and "freedom from fear and anxiety". With the evolving of Information Communications Technologies(ICT), a new way of business has evolved which we refer it as E-businesses-business include the exchange of information not directly related to actual selling and buying of goods through any electronic networks such as Internet and Intranet.

For any dot com company, information is the most important of all the business. Securing information is the most complex and difficult aspects of e-business.

In old days, Security has always been about keeping people out. When considering the security of a business today, it is very much about dissolving the boundaries between customer and business, staff and the business, business and trading partner. With the high acceptance and usage of computing technologies throughout the business, security has become an increasing concern.

The challenges a company might face can be subdivided into a few areas. Privacy infringement happens where other read or copy or data or information for which they are not entitled While keeping information private, it's important to note down that sometimes it is enough for a competitor to only watch how a business manage and organise important data and reformation.

The most concerned threat is during the sending or transferring confidential data or information through an electronic network. A message or information sent by the sender might be tapped or copied by an unintended person before it reaches the intended receiver. Hence the unintended person will be able to read, alter or even delete the message .Hence privacy or secrecy has been compromise.

According to Davis and Benamati (2001) no matter how well a network is protected, some intrusion attempts will succeed.

Traditional Signature:-

Traditionally a person may sign on the document and the signature may serve various purposes. A Sign is defined u/s 3 of Interpretation Act of 1948 and 1967(Consolidated and Revised 1989) (Act 388) to include a making of a mark or affixing of a thumb print. Signing of a document serves the following purposes. Firstly it serves a proof of evidence that the document has been duly signed by a particular person and secondly the act of signing a document calls the signer attention the legal significance of signers Act and thereby helps prevent poorly considered engagements. Thirdly a signature expresses the signer's approval or authorisation of writing content or the signer's intent that it has legal effect and force.

Digital Signature:-

Digital signature is such a concept that it is used many times interchangeable with that of electronic signature. But the difference between the two terms has been clearly demarcated by the definition provided in the IT Act 2000 along with the IT rules. According to section2 (p) of the IT act digital signature means authentication of any electronic record by subscriber by means of electronic method or procedure in accordance with the provision of section 3 whereas electronic signature u/s 2(tb) means authentication of electronic record by subscriber by means of electronic technique specified in the second scheduled and includes digital signature. For this two type of signature the certificate is being issued by the certifying authority to make it authentic and approved. The authentication of electronic record is possible only when the subscriber affixes his digital signature and this can be possible by use of asymmetric cryptosystem accompanied with hash function which makes it differentiable to that of electronic signature. Looking into the technicality through the hash function a hash result is being developed by the use of alogorithm.Section 3 of the IT act states that any

person by the use of a public key of the subscriber can verify the electronic record. As the private and public key are unique to the subscriber and constitute a functioning key.

Apart from the provisions provided under IT act still then the security of the signature and question of authenticity is at question. No doubt chapter v of IT Act along with the section 14 and 15 has been stated for securing of electronic record but its implication is yet to be verified. The certifying authority has the power to issue certificates both digital and electronic but they can do so by selecting different class of digital certificates at different level after verification starting from class0 to class 3 of certificates dealing with the purpose of demonstration and testing till high assurance certificates used for e-commerce application.

As we have covered what digital signature can do to facilitate in e-commerce application. The important thing is how it will handle the weighty issues of law. How does law view the digital signatures, electronic signatures and electronic business transaction in? There are two types of school of thoughts regarding the legality of digital signature.

One school gives emphasis to do nothing; Digital signature will come into their own through use by people. If two parties agree to conduct business and one party or even the third party contest the agreement then the issue need to be resolved by court of law. The court need to look into all the documentation associated with the agreement to find out what sort of contract is there. Did both the parties to the contract had consensus ad idem and abide by the policy and terms of contract. The usual way to indicate the intention is to pen down their signature to the bottom of contract. If both the parities have done their digital signature in electronic document then in this case the court will decide if the digital signature is legally binding. If it is determined that the parties intended digital signature to be their attestation of good faith ,then the contract will be declared to be binding and digital signature will have definition as stated under IT Act,2000.

The second school of thought said to avoid litigation process, save the overburdened court system from being bothered with the stuff and save the companies thousands of dollars in legal fees by regulating the use of digital signature

Several states has legislated the use of digital signature they range all the way from Utah's law which is quiet hefty to some other law e.g. Massachusetts law which is barely two pages long. Utah defined not only when digital signature can be used but also stated who may issue key pairs and under what circumstances. The Utah law impose severe penalties on certificate authorities and strictly controls how key are issued. The Utah law has undergone several revisions since it was first passed. There are still many who view the law as too restrictive and some view the Massachusetts law as too scanty.

Benefits of Digital Signature:-

1. Authentication of sender's identity to the receiver by an entrusted third party.

2. Verification of genuineness of the message.

3. Security of information sent (No one can tamper the message without jeopardising the verification process and the sender is unable to repudiate the effect of his signature.

The issues being of two types in relation to the digital signature:-

1. Technical issues which involve the verification of the cryptography. The signer can be any individual but if it's a valid signer then it will first apply the hash function in the signers software this function can compute the hash result of standard length which is convert into Digital signature using signer 's private key. Breaking open of this technicality is not that easy but if at all any one tries to break open this technical aspects there should be at other end the subscriber well equipped to check out who the signer is and prevent it from being tampered. Although many people know the public key of a signer and can use it to verify the signer's signature its quiet impossible to know the private key and use it to forge digital signature.

TheUNCITRAL model law adopts a technological neutral approach but it does not approve or specify any particular form for signature for authentication purpose. The Model also explains the rule of conduct to indicate the obligation of signer, the recipient and the role of certifying authorities.

Legal issues is that it's at question any one can go for signing of electronic record on behalf of anyone .The signature is at question whether it is done by the same individual or by anyone in his/her behalf .In order to have a control to this issues section 5 is concerned with the legal recognition of the electronic signature's/s 10 of IT Act states clearly the power of central government to frame rules for electronic signature and section 15 about the security of the electronic signature from being forged. Lastly section 21 which deal with the power of the controller to give license to issue Electronic signature certificates.

The other related problem of Digital Signature is as:-

1. It follows a good old fashioned authentication. If a small piece of paper is presented in court, it must be demonstrated to be authentic to make it admissible in court. The question is, is the party actually signed it or someone else. When we sign something before the notary its self authentication because the notary is a public official who is duty bound to ensure that is at question.

2. When we sign something before the witness, the witness would theoretically testify about the piece of paper by giving evidentiary support to its authenticity.

3. Its legal perspective is based on the core area.

4. Scope of its application is very limited.

5. Limitation and Restriction in recognising a sole digital signature regime.

6. Qualification and duties of the licensed identication authority and subscriber.

3. When a party sign something physically not before the witness, the paper can be shown to party familiar with handwriting as evidence in support of authentication.

All of these directly give authentication that the signature is real not forgery. But in case of Digital signature it does not incorporate any physical signature at all and thus there is always a possibility that the person on other end of the computer typing words into a box is not in fact the person on whose behalf they are signing. There are some schemes that the website operator have devised to substitute of this such as asking information not likely to be known by all other than the true signer setting up a PIN system logging IP addresses and so forth

there is no categorical rule that a digital signed paper isn't valid but our traditional rule of evidence caught up to this. The procedures being as follows:-

Plain Text- Cryptography -Cipher Text-Decrypotography-Plain text.

There are cases relating to digital signature:

The Hon'ble Bombay High Court, whilst granting ad-interim reliefs in a couple of Suits before it, discovered the possible manner in which a Digital Signature could be misused and scorned at the plausible impact that such misuse of Digital Signature could cause.

The Suits in reference were filed by two companies situated in Mumbai, namely *DDPL Global Infrastructure Private Limited* and *Unicorn Infra Projects & Estates Private Limited*. A group of 4 individuals are Directors on the Board of both of these companies (the "**Existing Directors**").

One fine morning, the Directors realized that the MCA portal shows the names of two unknown persons as the Directors of the Companies instead of themselves. On probing a little further, the Existing Directors fathomed the entire gamut of fraud played to oust them as the Directors of the Companies from the MCA portal.

The whole fraudulent act of removing the names of the Existing Directors from the MCA portal was initiated by fraudulently obtaining a digital signature of one of the Directors on basis of forged photo identity and address proof of the concerned Director. Using the said Digital Signature of one unknown person's name was uploaded on the MCA Portal as the Director of the Company, who then not only uploaded forms to oust the Directors and himself from the MCA portal, but also to upload requisite forms to upload the other two unknown persons as the Director of the Companies.

The Court has referred to the entire aforesaid act by the unknown persons as being "nothing short of a wholesale Corporate Hijack". The extent of threat it poses to the reputation of any corporate is unfathomable as there is room for misuse of the private key. The primary purpose behind adopting Digital Signature is to encrypt the information.

Quite contrary to serving its purpose, the present case exhibits how the digital signatures if used unwarranted, can sabotage the working of its users.

The whole case has brought to light the possible mischief that can be committed on a company by merely procuring a fraudulent Digital Signature of one of the Directors of the Company.

The other glaring issue which the Court noted was that of the access to MCA portal being permitted simply against entry of DIN numbers without any use of a now industry-standard the two-step security protocol to verify the legitimacy of the user logging in. The potential threat to any corporate, is highlighted by the present case is shuddering and requires urgent attention of the concerned authorities.

Probably nothing could conclude the whole case better than the observations of Hon'ble Mr. Justice G.S. Patel of the said case made in his Order quoted as:

"This is, to put it mildly, a most alarming state of affairs. The reasons are many. It throws into doubt the viability of using digital signature at any level that demands security, from companies to courts. It also demands a closer scrutiny of the manner in which digital signatures are issued in the first place. It appears that these are being issued willy-nilly without sufficient checks and balances and without proper verification or adherence to standard KYC norms."

Suggestions and Recommendations

The model law where many countries are signatory should be bound to follow the law and lacuna in IT act being as we are quite aware of the fraud going on in cyberspace need to be controlled at all level by improving the duties of the subscriber in verifying about the signer more closely ,by disclosure and consent by putting valid question which can prove the signer's authenticity .By having a track of the record on regular basis ,should be a computer savvy person so that the problems can be easily solved. The law should also mention sections dealing with Digital signature so the signer can be clearly identified. There should be stringent punishment for the netrespassers ,hackers etc in order to resolve this issues of digital signature and making it admissible in the court of law as a better evidentiary value.

The legislative body need to look into those issues highlighted above to safeguard the interest of parties transacted in internet (e-business).The Act shall extend its application to transaction by any person.

Instead of various governing statute there should be one comprehensive statue and should be enacted. So that it governs all aspects of electronic contracts such as formation of contracts generally and particularly the evidential proof of identity of contracting parties.

There should be an insertion of clear provision on the renewal of Digital signature certificate so that a new can be issued to the existing subscriber by providing a new key from time to time, and this may prevent the tampering activities

The Digital Signature is tried to be made more authentic and legalise by adhering certain criteria:-

a) The Signer must be authenticated.
b) There must be Disclosure and consent.
c) The signer must be aware of the fact that it's legally binding.
d) The Documents must be secure from tampering.
e) All signers must have an access to the document.
f) All actions should be documented.

References:-

1. Pavan Dug gal, Cyber law-The Indian Perspective.

2. Alfred Dudley, Investigating Cyber law and cyber Ethics-Issues, Impacts and Practices.

3. David L.Baumer, Cyber law and E-Commerce

4. Vivek Sood, Cyber Law Simplified-

5. IT Act 2000 Bare Act-Universal Publication

6. Jonathan Rosenoer; Cyber Law-The law of Internet.

7. S.R Myeni, Information Technology law and Cyber Crime-

Website references

.https://www.irjet.net/archives/V4/i6/IRJET-V4I6303.pdf
www.indialawjournal.org/technology-laws-decoded-by-n-s-nappinai.php