Critical Analysis of Digital Signature Laws in India

Deeksha Singh
Invertis University, Bareilly
Uttar Pradesh, India

ABSTRACT:

The online trading is growing broadly day by day, which makes safety the biggest concern while carrying out trading by electronic means. As many other operations can be done with digital environment and internet, operation that provides identity confirmation should also be added to the digital environment.
When data are transferred, the user should make sure that there are no alterations in the original data while transferring them from sender to receiver. And it has also become necessary to authenticate the users often to ensure safety and to avoid fraud. There are lot of divergent ways of online identification, in which digital signature is considered to be one of the powerful way of authentication. So, the online user use digital signature to authenticate the sender and to maintain the morality of the document sent.
In this paper, a study is carried out to identify the usage of digital signature and the view of people towards it in developed and developing countries and a survey is taken to support the theory.
ACRONYMS: PKC: Public Key Cryptography**, CCA:** Comptroller of Certifying Authority

I. INTORDUCTION

Digital signature is electronically generated and can be used to make sure the accuracy and legitimacy of data. The dawn of information technology transform the whole world; India is not an exception to it; as technological involvement is the social behavior in India.[1] A valid digital signature provides the guarantor to the recipient that the message was generated by a known sender, such that the sender cannot deny having sent the message. Digital signatures are mostly used for software distribution, financial transactions, and in other cases where there is a risk of forgery.[2]

The origin of information technology transforms the whole world and fortunately India led a leading role and captured global attention. India passed Information technology Act 2000 which came into force on 17-10-2000. The Act applies to the whole of India and even to persons who do offence outside India. The Act confirms "DIGITAL SIGNATURE" and provides for enabling a person to use it just like the traditional signature. The basic purpose of digital signature is not different from our traditional signature. The purpose therefore is to authenticate the document, to identify the person and to make the contents of the document binding on person putting digital signature. Let us see what digital signature is in technical terms.

A digital signature or digital signature scheme is a mathematical scheme for reveal the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not change in transit. Digital signatures are based on public key encryption. It uses prime numbers like 2,3,5,7,9,11 and so on which can be divided only by itself or by

[1] http://www.iamwire.com/2014/09/digital-signature-laws-india/100694
[2] https://www.tutorialspoint.com/information_security_cyber_law/digital_and_electronic_signatures.htm

1 and is inadequate of division by other numbers. We have unlimited prime numbers and in DS we use the multiples of prime numbers.

The functioning of DS is based on the system of public key cryptography. Public-key cryptography refers to a cryptographic system need two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key pair are mathematically connected. One key locks or encrypts the plain text, and the other unlocks or decrypts the cipher text. Neither key can perform both functions. One of these keys is published or public, while the other is kept private.

"Key encryption empowers more than just privacy. It can also satisfy the recipient of the authenticity of a document because a private key can be used to encode a message that only a public key can decode. If I have information I want to sign before sending it to you, my computer uses my private key to encipher it. Now the message can be read only if my public key-which you and everyone else know-is used to decipher it. This message is almost from me because no one else has the private key that could have encrypted it in this way".[3]

Justice Yatindra Singh in his book "Cyber laws" has stated that since public key encryption is slow and time consuming the hash function is used to alter a message into a unique shorter fixed length value called the Hash result. Hash serves the motive of an index of the original text. It is an algorithm mapping or conversion of one sequence into another. The hash function is such that the identical hash result is obtained every time that hash function is used on the identical electronic record and two electronic records cannot produce the identical hash result using the identical hash function. In other words mapping is one to one and not many to one. It is one way. One cannot recreate the original message from the hash result. The encryption of a hash result of the message with the private key of the sender is called a Digital signature.[4]

II. STATEMENT OF PROBLEM:

- In which extent India are aware of digital signature when compared to developed countries?
- What are the new challenges in improving digital signature in India?

III. RESEARCH OBJECTIVE:

To examine provisions related to Digital Signature in The Information Technology Act, 2000.

IV. RESEARCH HYPOTHESIS:

The implementation of Information Technology Act, 2000 is not much effective.

[3] http://www.certificatetiger.com/News/law-of-digital-signature.htm
[4] "Cyber laws" by Justice Yatindra Singh

V. RESEARCH METHODOLOGY:

This research paper is based on the doctrinal method in which data is collected from the secondary resources. In the secondary resource some books, e-books, websites etc. have been referred. After collecting data from these resources the materials were filtered and included in the research paper.

VI. LITERATURE REVIEW:

For more than two decades researchers have put much attempt in developing security methodologies, models and standard definitions of security services. However, we still experience systems insecurity. The requirement for user authentication has become mandatory in e-government, e-commerce, and e-business applications. For example, there are multiple examples where two unknown parties in different branches of the public administration need to securely exchange documents. Several protocols, such as Kerberos, have been suggested to provide authentication over public networks using symmetric cryptography. Those systems are not easily expandable for large groups of users (possibly belonging to different organizations). Some researchers have put efforts to solve this problem, like Davis, Ganesan, and Schiller et al., but the resulting systems are not widely establish. On the other hand, public key cryptography, as introduced by Diffie et al., is a very strong technology and seems to be well suited to satisfy the requirements of the global Internet. In fact, it is commonly agreed that this technology is fundamental for a developing e-commerce and e-business in Internet, and has become the foundation for many such applications. The extensive use of public key cryptography requires a Public Key Infrastructure (PKI). The aim of a PKI is to make sure that a public key in use really be linked with to the claimed entity. Without a PKI, public key cryptography would not be higher to traditional private key cryptography.[5]

VII. HISTORICAL BACKGROUND:

Whitefield Diffie and Martin Hellman published a paper called New Ways in Cryptography in 1976, in which they discussed about a new method of distributing cryptographic keys. This article encourages the development of a new and effective asymmetric encryption algorithm. They gave the reason for digital signature schemes. Ronald Rivest, Adi Shamir, and Len Adleman turn up with the concept of RSA algorithm in 1977. By using both of these concepts an ancient digital signature was developed. This basic scheme was not very safe. (Shafi Goldwasser, Silvio Micali And Ronald L. Rivest, 1988). For more safe method, a cryptographic hash function was applied to the original message before following the RSA algorithm. This was proved safe in the random oracle model. Shafi Goldwasser, Silvio Micali, and Ronald Rivest were the first people to define the guaranteed requirements of digital signature, in 1984. Lamport signatures, Merkle signatures, Rabin signatures were the early digital signatures those were developed, but

[5] http://shodhganga.inflibnet.ac.in/bitstream/10603/2337/12/12_chapter%202.pdf

they were not effective. In 1989, the first well known digital signature software package Lotus 1.0 was enabled.[6]

VIII. DIGITAL SIGNATURE:

A digital signature is a mathematical technique used to recognize the authenticity and integrity of a message, software or digital document. The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent safety, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added guarantees of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer.

In many countries, including the United States, digital signatures have the same legal importance as the more traditional forms of signed documents. The United States Government Printing Office publishes electronic kinds of the budget, public and private laws, and congressional bills with digital signatures.[7]

A digital signature is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is authentic. Authentic means that you know who created the document and you know that it has not been altered in any way since that person is created it.

Digital signatures rely on certain types of encryption to safeguard authentication. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. Authentication is the process of verifying that information is coming from a reliable source. These two processes work hand in hand for digital signatures.[8]

IX. DIGITAL SIGNATURE IN SWEDEN:

- **General History:**

After the UNCITRAL model law on electronic commerce in 1996, the European Union moves the European Directives in 1999. The Sweden's EU Presidency in 2001 were discussing with different agencies to provide "24 hour service" to its citizen and to make alteration, in the law that treats the electronic signature equal to the physical signature.

Swedish bank consortium was establish, where major Swedish banks participate. The consortium was establish to come up with a standard structure of e-id, that fulfills the government requirements and also easy to use by the people. As a result of the consortium, Financial ID Teknik BID AB was establish in September 2002 to create and distribute the digital signature BankID. In 2003, the first e-id was emerging.

[6] http://www.digital-signature.com/historyof-digital-signature-law.html.
[7] https://searchsecurity.techtarget.com/definition/digital-signature
[8] https://computer.howstuffworks.com/digital-signature.htm

27000 people used BankID to file their tax return that year, the number extend across 100000 during 2004 and 500000 during May 2005. Tax and social insurance are able to adapt the usage of digital signature (Bankid, 2013).

In beginning three issuers of e-id in Sweden were BankID, Nordea and Telia. In 2007, Synovate conducted a survey on 1200 people, for Financial ID Technology, showed that 95% of the people have knowledge about BankID and e-id. In January 2008, SEB buys 18.3% of the financial identification technique's stock, became one of the largest stock holders, and started to provide the BankID to its customer.

Mobile BankID was start in the beginning of 2010. Nordea unite BankID in January 2011. There are 4.5 million active users uses the BankID for 1000 for public and private services and 7 million bank customers have the approach to digital signature certificate BankID. (Bankid, 2013).[9]

- **Law on e-signature in Sweden:**

After the European Directives in 1999, the Qualified Electronic Signatures Act (2000:832) was passed in Sweden that made the electronic signature a rational authentication id. That is, the agreements and documents signed by digital signature is legally strong as the physical signature of a traditional contract (The agreement Title deeds and Wills are not included). The laws like Consumer Credit Act, Companies Act also permit digital signature. In Money Laundry Act (2009:62) also accepts the digital signature. (Ministry of Transport and Communications 1998).

- **Digital signature certificate providers in Sweden:**

1. BankID
2. Nordea bank
3. Telia
4. Danske bank
5. Handeks bank
6. Skandia bank
7. Länsförsäkringar
8. Ikano bank
9. Sparbanken öresund
10. Sparbanken Syd
11. Swedbank

[9] http://www.bankid.com/sv/om-foretaget/Historia/

12. SEB bank

13. Ica bank

E-identification emerges by banks and Telia. The name of the e-id changing depend on who is issuing it such as Bank ID, Nordea's e-authentication or Telia e-identification. (E-legitimation, 2013).

- **Requirements to obtain a digital certificate:**

The people who require digital certificate mush have a Swedish personal number that is registered in Sweden. The age limit differs from publisher and those who have e-services. For example, the Tax Board, you must have turned 18.

An organization or a company can't have a digital signature of its own, the digital signature must be connected to a person and the user must have a Swedish personal identity. If an organization likes to sign a contract, the digital signature of the CEO or the person-in-charge is used.

- **Applications of Digital Certificates in Sweden:**

The digital signature (e-legitimation) is used in login, signature for companies and government agencies that offers e-services. Most common issuers of these services are

1. Insurance: sign the care of children, apply for parental leave and plan retirement.
2. CSN: apply for a student loan.
3. Tax: tax returns check the tax account and print a birth certificate.
4. Swedish Change of Address: labels notification of removal.
5. Savings banks' internet banking: with BankID short and Mobile BankID in the mobile, you have gain to the same services with security box.
6. Direct Payment service: with Mobile BankID and BankID short, you can complete the purchase of around 500 different e-commerce sites.
7. In some agencies, you may have look to, for example, be able to represent your business. Contact each company / agency to get the proper permissions.
8. For signing documents like MS Word, MS Excel and PDFs.
9. For sending and receiving digitally signed and encrypted emails.
10. For carrying out secure web-based transactions and also to recognize other participants of web-based transactions.

- **How to Use Digital Signature:**

Digital signature is available in three divergent:

Digital signature on file: This file is saved on the computer. To authenticate, the file is used with a password. The file can be downloaded from the internet bank or bought from the provider. This file can be duplicated to another computer and can be used. The file can be used with a USB stick too.

Digital signature on card: In this type the digital signature is kept on a chip card. It is expensive than the former one. To authenticate using this type a card reader is used, that is attached to the computer through a USB cord. The card reader is given by the digital signature certificate provider. The card is also on with photo of the owner on it, which can also be used as identification card.

Digital signature on Mobile phones: The e-authentication for mobile phones and tablets are available. Mobile bank ID provides this facility. To use this facility the app is downloaded to the device and the app is linked to the internet bank.

X. DIGITAL SIGNATURE IN INDIA:

- **General History:**

E-authentication is allowed in India by passing the Information technology act 2000. The digital signatures are treated with the same legal value with the handwritten signatures and the electronic documents that have been digitally signed as same legal values as a regular paper documents. Information technology act based on asymmetric crypto system provides the required legal value to the digital signatures. The Controller of Certifying Authorities (CCA) was appointed by the central government to issue e-authentication certificates. The CCA is providing certificates since November 1, 2000 aiming to promote the growth of E-Commerce and E- Governance. (IT Act, 2000)[10]

- **Laws on e-authentication in India:**

The Information Technology act 2000 was passed in India based on Model Law for e-commerce proposed by UNCITRAL, with the major concepts like

1. Legal recognition of data messages,
2. Writing Signature,
3. Original, Admissibility and evidential weight of data message,
4. Formation and validity of contracts,
5. Recognition of parties by data message,

[10] Information Technology Act, 2000

6. Acknowledgement of receipt,
7. Time, dispatch and receipt of messages.

The central government of India assigns Controller of Certifying Authorities (CCA) under section 17 of the Act. The IT act gives the authority to CCA for issuing license to the Certifying Authorities CA. The CA issues the digital signature certificate to the public following certain criteria. 35 The digital signature of the CCA is also included in every public key of the digital signature certificate provided as established under section 18(b) of the IT act. This helps to certify the originality of the certificate. (IT Act, 2000). The legitimate signatories of company and professionals, and people who signs manual documents and returns filed with ROC are required to obtain a Digital Signature Certificate (DSC). Hence the following officials should have DSC. (Digital Signature Certificate, 2013).

1. Directors of organizations.
2. CA's/Auditors.
3. Company Secretary.
4. Bank Officials - for Registration and Satisfaction of Charges.
5. Other Authorized Signatories.

The people who have income more than a million rupees per annum can only file their tax return through e-service using digital signature.

- **Types Of Digital Signatures Certificates:**

There are 4 different types of digital signatures certificates in India. They are

1. Class 0 Certificates
2. Class 1 Certificates
3. Class 2 Certificates
4. Class 3 Certificates

Class 0 Certificate:

This certificate is used only for demonstration purposes to test the certificate and get familiar with the various usage of the digital signature certificates over the different fields of applications.

Class 1 Certificate:

This certificate is used to individuals or private subscribers. These certificates will confirm that users name or E-mail address form a clear subject within the Certifying Authorities database.

Class 2 Certificate:

This certificate is used by both business personnel and private individuals. These certificates will confirm that the information in the application is given by the subscriber does not conflict with the information in well-recognized consumer databases.

Class 3 Certificate:

This certificate is used by individuals as well as organizations. This is high affirmation certificate, primarily intended for e-commerce applications. This certificate is given to individuals only on their personal (physical) appearance before the Certifying Authorities. (Classes of Digital Signature Certificates, 2013).

- **Components of a Digital Signature Certificate:**

Public key: It is the reference for the digital certificate; this is provided to certify the document sent.

User name and e-mail address: This provides information about the person, to whom the signature relates.

Expiration date of the public key: The digital signature certificate is authentic until this date.

Name of the company: This is used for identifying the company to which the signature belongs.

Serial number of the Digital ID: This is a unique number that is included in the signature helps us for tracking.

Digital signature of the Certification Authority: This is the signature of the CA, used to certify the originality of the certificates.

- **Certifying Authorities:**

Certification Agencies are appointed by the office of the Controller of Certification Agencies (CCA) under the provisions of IT Act 2000 in India. There are a total of seven Certification Agencies authorized by the CCA to issue the Digital Signature Certificates.[11]

- **Applications of Digital Certificates in India:**
- For sending and receiving digitally signed and encrypted emails.
- For carrying out secure web-based transactions and also to know other participants of web-based transactions.
- eTendering – Tendering for the various government projects.
- eProcurement – Procuring various kinds of commodities in the ecommerce applications.
- Ministry of Corporate Affairs for registering the corporate companies.

[11] www.cca.gov.in

- eFiling - Income tax returns filing for the government.
- For signing documents like MS Word, MS Excel and PDFs.

XI. COMPARISON BETWEEN INDIA AND SWEDEN:

The idea of digital signature was introduced to both the countries around the same time. But the awareness and the usage change, this is because of the following reasons.

In Sweden, almost everyone is an internet user (International Telecommunications Union (Geneva), June 2013.). And the students use digital signature to get their scholarship money and their loan from the Government and the tax filling is submitted using digital signature, thus placing the digital signature for regular use for the people in Sweden. There are 4.5 million digital signature users that is around 48% of the population of Sweden uses it.

In India, the digital signature is used mostly for filing tax return. And not everyone uses digital signature to file the tax return, it is only mandatory to use digital signature for tax filing, if the turnover of the company is more than 10 million rupees per annum or the turnover of an individual is more than 2.5 million rupees per annum. Since 2000 till June 2013 only around 5.2 million digital signatures has be given by the Controller of Certifying Authorities, India, which is large number but its only 0.43% of Indian population uses digital signature.

In Sweden the digital signature certificate is given by the banks and whereas in India it is distributed by government appointed firms. This makes a huge difference in the awareness.

Digital signature is easily available to the Swedish people because digital signature certificate is given by the banks and it has the authenticated information of its customer upfront, thus process of issuing DS is simple. And it can also be downloaded from the bank websites using internet banking.

Whereas in India the digital signature is given only by the few certifying authorities, the listed firms that has been given by the CCA. And to get the digital signature (Class 3 certificate), the person has to be physically present with an identification card. And thus the digital signature is not easily accessible for the Indians, which make the usage and awareness of the product less.[12]

XII. CONCLUSION:

The thesis provided an unambiguous view on the historical development of the digital signature and its laws. And provided detail information about digital signature, its work and what makes it more safe and trustable.

[12] https://www.diva-portal.org/smash/get/diva2:695339/FULLTEXT01.pdf

The thesis is done by examining through theoretical study and practical study. The practical study was done to carry the theoretical study and done by interviews and survey. It provides an unambiguous view on the awareness of digital signature in developing and developed countries.

The legal part of the thesis has stated more information about the laws on e-authentication in both countries and the history of it. Sweden and India had introduced DS in the year 2000 by following the Model Law for e-commerce proposed by UNCITRAL by passing the Qualified Electronic Signatures Act (2000:832) and Information Technology Act 2000 respectively but the usability of the product changes, the reason for the different were also discussed.

XIII. SUGGESTION:

- The developing country can follow the developed countries in implementing the digital signature in different fields; thus increasing the use of the product, which in return increases the number of users.
- In India the use of digital signature can be improved by making it available in places that are easily reachable to public like banks, post office etc. The easy approach to digital signature will also increase the awareness of the people towards digital signature.