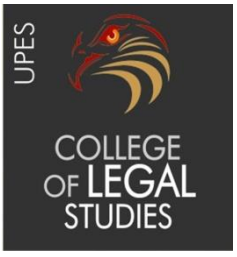
DIGITAL SIGNATURE: A LEGAL PERSPECTIVE

Author: Rishabh Jaiswal

Submitted under the guidance of: Mr. Krishna Deo Singh Chauhan, Assistant Professor, COLS

This dissertation is submitted in partial fulfilment of the degree of B.Tech., LL.B. (Hons.)



College of Legal Studies

University of Petroleum and Energy Studies

Dehradun

2017

CERTIFICATE

This is to certify that the research work entitled **"DIGITAL SIGNATURE: A LEGAL PERSPECTIVE"** is the work done by Rishabh Jaiswal under my guidance and supervision for the partial fulfilment of the requirement of B.TECH., LL.B. (Hons.) degree at College of Legal Studies, University of Petroleum and Energy Studies, Dehradun.

Mr. Krishna Deo Singh Chauhan

Assistant Professor

College of Legal Studies, University of Petroleum & Energy Studies

Dehradun

Date:

DECLARATION

I declare that the dissertation entitled **"DIGITAL SIGNATURE: A LEGAL PERSPECTIVE"** is the outcome of my own work conducted under the supervision of Prof. Krishna Deo Singh Chauhan, at College of Legal Studies, University of Petroleum and Energy Studies, Dehradun.

I declare that the dissertation comprises only of my original work and due acknowledgement has been made in the text to all other material used.

Rishabh Jaiswal

B.Tech., LL.B. (Hons)

12th Semester

2011-2017

Date:

ABSTRACT

With the rapid growth of technology, all the communications are now taking place over internet. E-commerce has provided a platform to conduct business across the territorial borders. Contracts are now being negotiated and formed between the parties through electronic communications. The need for the authentication and integrity of the electronic communications has increased. Business transactions cannot be completed unless the digital signatures are enforced.

Digital Signatures are the electronic signature which represents the consent of the person. The digital signature ensures the authentication and integrity of the information.

The paper aims at providing a detailed understanding of the concept, the mechanism of digital signature and the laws related to it. Subsequently the paper discusses the impacts of conventional and digital crimes being committed by use of digital signatures. The paper would be examining the existing laws governing the aspects of digital signature with respect to Indian and International perspective. The paper highlights various challenges faced due to digital signature. The paper ends with the discussion various propositions which need to be considered for effective IT Law to govern the aspects of digital signature or to develop a whole new legislation all together separately dealing with Digital signature.

***Keywords*:** Digital Signature, Digital Signature Certificate, Certifying Authority, Rules.

ACKNOWLEDGEMENT

I sincerely convey my deepest gratitude to my mentor Mr. Krishna Deo Singh Chauhan for his continuous support. He has actively and consistently guided me in the preparation of this Dissertation. He has been the source of motivation and encouragement.

Without his valuable insights and comments, this dissertation would not have been possible. His active words of advice and his guidance not only helped for this research work but also for my future and career.

I take this opportunity to extend my gratitude to Adv. Neeraj Arora for introducing me to this specific field and arousing my interest in the same. I am extremely thankful to him for sharing his expertise and his valuable guidance.

I would also like to acknowledge and extend my heartful gratitude to all the people whose participation has made the completion of this Dissertation possible.

Rishabh Jaiswal

B.Tech., LL.B. (Hons) with Specialization in Cyber Laws

SAP ID: 500016487

Enrolment No.: R120211013

College of Legal Studies

University of Petroleum & Energy Studies

Dehradun

TABLE OF CONTENTS

CHAPTER 1

1. INTRODUCTION

For any dealings, whether business, personal or professional, there exist an offer and an acceptance, or in other words, it would be convenient to say, for any work to be done involving two parties, there comes into picture an agreement to do the work for a given set of terms and conditions. Signatures play a significant role in affirming the will to do or to abstain for from doing a certain thing for the terms and conditions. Another very interesting and vital role that the signature plays is that of authentication, integration, authorization, and verification.

In the ancient days, signatures, thumb prints, stamps, seal etc., were put to agree by the contents of the texts, bind by them and also, in cases to keep them private communication. The seal had a name or symbol imprinted which identified the sender. The word sign became common but ambiguous as to what constitutes a sign actually. The General clause Act defined sign under section 3(56) as follows:

“"Sign” with its grammatical variations and cognate expressions, shall, with reference to a person who is unable to write his name, include, "mark", with its grammatical variation and cognate expressions”[1].

This definition is important to note while discussing digital signatures. Though digital signature is defined under Information Technology act, 2000, the definition under general clause act also legally justifies the use of digital signature in case a person is unable to write his name. Since, it is true that in electronic medium a person becomes incapable of writing his name in a way that makes it unique or binding to him and thus an electronic mode for doing the same was felt with the amount of communications and contracts being formed online. Information being shared online has increased tremendously; a secure, reliable, non-repudiated communication is the need of the hour. Gaining access to communication channel and tampering information has become easy. It is thus, required that the information is secured and encrypted.

[1] Section 3(56), The General Clauses Act, 1897, No. 10, Acts of Parliament, 1897(India).

1.1.RESEARCH METHODOLOGY

1.1.1 STATEMENT OF PROBLEM

Electronic communication and contracts are the most important area of internet today. Most of the agreed terms and conditions for performance or non-performance of any kind of task today are being dealt and discussed through communication over the internet. Due to anonymity that internet provides, digital signatures were recognized to provide authenticity, integrity, and reliability to the communication. The problem arises when these digital signature certificates are either misused in committing crime or are forged for some illegal purpose. It becomes necessary to understand such crimes, why and how are they committed and to bring out legal solutions to it.

1.1.2. OBJECTIVE

With the advent of internet and rise in the E-commerce activities, use of Digital signature has become important to ensure the authentication and integrity of the communications. Thus it has become necessary to understand the rules and regulations governing Digital signature and it legal implications. The objective of the research is to understand and highlight the probable digital signature crimes and to provide a legal remedy for such cases in the form of a proposed legislation for digital signatures for India.

1.1.3. SCOPE

The scope of the research extends to the technical and legal aspects of digital signature. It deals with what exactly is digital signature, how is a digital signature certificate generated, what are the rules and procedures prescribed by law and how to deal with situations when a crime using or against digital signature is committed.

1.1.4. METHODOLOGY

The research methodology adopted is doctrinal. Reference has been made to numerous text books, articles, research publications and online web sources. No quantitative analysis was done for the purpose this research and it is purely based on the principles of law laid down in various statutes and juristic writings.

1.1.5. LITERATURE REVIEW

The main objective of this thesis is to analyse the various aspects of Digital signature and the legal implications. And for this purpose a number of article and books have been consulted. The general text of this thesis consists of text books, articles and publications and statutes. The above mentioned materials shall be scrutinized so as to reach a conclusion. The books and articles referred are discussed below, in short:

BOOKS:

1. **Stephen Mason, Electronic signature in Law, 3rd Edition, Cambridge University Press, 2012.**

   In this book the author has traced out the history of digital signature in the context of legal terminology. The author has covered the legislations of various countries related to electronic and digital signature.

2. **Karnika Seth, Computers, Internet and New Technology Laws, 1st Edition, Lexis Nexis, 2013.**

   The author has outlined various provisions under the IT Act dealing with electronic signatures and digital Signature. The cryptographic system along with the significance of the digital signature has also been discussed in the chapter on Electronic signature. The role of certifying authority is mentioned in this chapter as well. Legal perspective of European Union and UNICITRAL Model on the digital signature has also been laid down in this book.

3. **Rohus Nagpal, Cyber Crimes & Digital Evidence – Indian Perspective, Asian School of Cyberlaws, 2008.**

   The author has discussed various types of crimes related to the digital signatures certificate with support of multiple illustrations of these crimes. The author has also discussed the provisions of IT Act, 2000 governing these categories of crimes related to digital signature along with the punishment prescribed for the cybercrimes.

ARTICLES AND PUBLICATIONS:

1. **A Brief History of Signatures, Electronic signature Blog, August 2011.**
   The author has traced out the history of signature from ancient times. The author has also thrown light on various U.S. legislations governing Digital signature

2. **Vijaykumar Chaube, Digital Signature: Nature & Scope under IT Act, 2000, SSRN Electronic Journal, (September, 2010).**
   In this article the author has made an attempt to understand the concept of digital signature. The author has tried to define effect and impact of digital signature in the cyberspace, the techno-legal effects of digital signature primarily focused upon the Indian Legal system.

3. **V. Kumar Swamy, The mystery of forged signatures, The Telegraph, (May, 2015).**
   The author discusses the crime transfer the shares of companies by forging the digital signatures of the directors.

1.1.6. RESEARCH QUESTIONS

1. Whether the existing laws are adequate to govern the uprising challenges of Digital signature and crimes related thereto?
2. Whether there is a need for separate law in India to govern Digital signatures?

1.1.7. HYPOTHESIS

Since digital signatures have not grabbed it roots well technically, the codified legislation regulating it is limited to legally recognizing it and manner of issuing it. There has been no concrete law in recognizing the probable threats of digital signatures or the kind of offences that can be committed either against such certificates or by using the said certificates. The laws are absent on the same. The existing laws are inadequate to meet the future requirements for delivering justice in case of such offences.

1.1.8. PROBABLE OUTCOME

The research shall bring out various crimes relating to digital signatures which can occur in near future or that have been taking place but people are not aware about them. The thesis shall also enlighten various deficiencies in the existing law and make some propositions by analysing laws around the world on the said subject matter. The research shall be useful in developing an effective legislation on digital signature which would deal with the upcoming computer crimes and challenges relating to digital signatures which the existing laws are deficient enough to combat.

CHAPTER – 2

OVERVIEW OF DIGITAL SIGNATURE

2.1. BACKGROUND OF SIGNATURE

In order to comprehend the significance of Digital Signature it becomes important that we understand the importance of Signature. The term 'Signature' has been derived from the Latin word '*Signare*', this means 'to sign'. The person who makes the signature by writing it down on a document is known as signor or signatory. A handwritten signature is the representation of a person's name, surname or any other kind of mark which the person writes on any document. The signature used by a person on a document or on any instrument can be used to verify the identity of that person as well as their intention.[2] One of the major facets of signature is that it indicates the consent of the person who has made it. A signature on any document or instrument holds the power to make the person bound to the obligations arising out of the signed document. The person who has signed the document becomes subject to all the legal implications which can arise from the said document.[3] Signature can be on anything like a legal document; contract, prescription, cheque or any piece of paper where by the signatory provides his assent and adhere to the commitment. In the formation of contract signature of a party plays a very vital role as it represents the consent of the party to the terms of the contract. In order for a contract to be enforceable in the court of law, the contract must have been signed by the parties. Absence of signature of the party on a contract can result in the contract to be unenforceable.

2.1.1. HISTORY OF HANDWRITTEN SIGNATURE

With time not only the meaning and scope of signature has strengthen but also its importance on daily basis as well as commercial basis has been realised. People from a typical notion of using pictures, symbols or seals to mark their identity took a step further and started mapping their identity with their names. Since this became a practice few people started adding creativity in the way of writing their names to mark

[2] Legalesign Staffwritter, *The History Of Signature*, The Legalesign Blog, (Oct. 15, 2016, 10:30 AM), https://legalesign.com/blog/history-of-signatures/
[3] S.K. Bansal, *Ecommerce Laws*, Cyber Millennium Challenges and Opportunities, pp. 223, (2001).

their identity which was unique to them and was termed as their signature. The origin of writing can be traced back to the Sumerian Era which prevailed over the period from 5th to 3rd Millennium BC. During this primeval period the people belonging to Sumerian culture developed ways for authentication of the work for the purpose of identification of the writings owner. Carving artwork in clay tablets, Creation of seal and usage of symbols were some of the ways adopted by the Sumerians in order to authenticate identity of the individual who made the writing.[4] In the 4th Century Talmud the holy book of Jews can also be found which contains the verse that specifically refers to the importance of signatures in the marriage agreement. According to Talmud the couples who are going to marry along with witnesses are required to write their names.[5] The signatures were also used during this period in order to avoid any possibility of alteration to the documents after the person had signed them. The first handwritten signature is known to be used in the period of 439 AD when Roman rule prevailed under the reign of the Emperor Valentinian III. The Romans started the practice of affixing the handwritten signatures to authenticate the instrument or the documents. The Romans started writing their names as their signature at the end of the documents for the authentication of documents. Eventually with tremendous usage of signatures by the roman people this practice of handwritten signature on the instrument or documents gained great significance in the western culture.[6] In 1677 the English Parliament passed the act State of Fraud which gave legal recognition to the signatures. This legislation provided that every contract must bear the signature of the parties as measure against fraud.[7]

With evolution of liberalisation and industrialisation, signatures became important for communications and commercial purposes. Signatures on the paper were considered to be a standard for important documents and contracts. It can be rightly interpreted from statement made by Thomas Jefferson in the Declaration of Independence - that a person's signature not only represents their name but it also represents their honor

[4] Admin, *A Brief History Of Signature*, The Electronic signature Blog, (Oct. 16, 2016, 11:25 AM), https://www.esign.com/blog/bid/108804/A-Brief-History-of-Signature
[5] Shahid Mehmood, *The Importance Of Signature*, The International News, 2 November, 2015, at A4
[6] David Fillingham, *A Comparison Of Digital And Handwritten Signature*, Ethics And Law On The Electronic Frontier, (1997)
[7] Legalesign Staffwritter, *The History Of Signature*, The Legalesign Blog, (Oct.16, 2016, 12:30 PM), https://legalesign.com/blog/history-of-signatures/

code as professionals in future.[8] Technological advancement in the field of computer science gave birth to cyber space where people came closer and transactions became easier. Soon the need to authenticate transactions and to affix the identity of an individual to the communications over cyberspace was felt by people. Signatures from traditional medium caught hold of importance in the electronic medium as well, as a result it gave birth to Digital signature.

2.1.2. HISTORY OF DIGITAL SIGNATURE

The telegraph was first used in the year 1844 which later gave rise to the problem of authenticity of the messages which were being transmitted electronically. The first relevant case related to electronic signature was reported in year 1867 in the US court. The legal dispute which aroused between the parties in this case was regarding the question of authentication of the messages that was transmitted electrically through the telegraphs.[9] The US court found out in this case that the legal requirements that were stated under the Statute of Fraud for the 'written signatures' were satisfied by the 'telegraphed signatures'. Hence the telegraph signatures would be considered valid for the purpose of authentication of messages.

In the year 1976 for the very first time the idea of the Digital signature scheme had been proposed by the researchers Martin Hellman and Whitfield Diffie. Though the research paper New Directions in cryptography written by them in 1976 talked about the scheme but it was still in its theoretical form. This was a remarkable achievement in the 19th century which laid down foundation for the development of the digital signature algorithms in the future. The research paper stated that an algorithm can be designed which would be able to generate a pair of the public and private keys. These pair of keys could be used for the encryption of information which can be transmitted over the networks.[10] Both the researchers had realised the importance of distributing the pair of cryptographic keys in the business community. According to the scheme of digital signature the private key had an associated public key and this public key could be distributed to all people.

[8] Admin, *The Value of signature*, The University of Texas Medical School at Houston, (Oct. 18, 2016, 04:24 PM), http://www.uth.tmc.edu/med/students-current/SCAIP/signature-value.htm
[9] Trevor V. Wood, 36 N.Y. 307(1867)
[10] Emily Maxie, *Infographic: The History of Digital Signature Technology*, Signix, (Oct. 20, 2016, 11:15 AM), https://www.signix.com/blog/bid/108804/Infographic-The-History-of-Digital-Signature-Technology

Later in the year 1978 the RSA algorithm was developed by Ronald Rivest, Adi Shamir and Len Adleman.[11] This algorithm could be used for the application of the digital signatures to the electronic documents. It also provided the feature of encrypting the document. This scheme provided in RSA algorithm was not very much successful in providing security to the document. Later based on the RSA Algorithm more different algorithms were developed which provided more security. Following this one of the digital signature scheme was that of ElGamal Technique which was introduced in the year 1985. In the year 1989 Lotus 1.0 became the first software that provided for the application of the digital signature to the documents.[12]

2.1.3. HISTORY OF DIGITAL SIGNATURE LAWS IN THE WORLD

2.1.3.1. Utah Digital Signature Act, 1995

Increase in the use of internet and technology led to vast growth of Ecommerce. All the transactions started taking place electronically which use the technology to digitally sign the electronic contracts. Utah became the first state to deal with the matter of electronic and digital signature by enacting the Utah Digital Signature Act in 1995.[13] The act primarily focused on the promotion of ecommerce and use of digital signature by giving legal recognition to electronic communications. The main purpose of the Utah act was to reduce the frauds being committed in Ecommerce and to curtail the forgery of digital signatures.[14] The Utah act is a regulatory scheme which has the provision for the implementation of infrastructure of public key encryption technology and certificate authorities. The legal status of digital signature has been recognised in the Utah act. The act clearly defines the liability of the certificate authorities and also addresses many of the public policy concerns.[15] The

[11] David Fillingham, *A Comparison of Digital and Handwritten signature*, (Oct. 21, 2016, 02:28 PM), http://groups.csail.mit.edu/mac/classes/6.805/studentpapers/fall97papers/fillinghamsig.html
[12] Jayakumar Thangavel, *Digital Signature Comparative Study Of Its Usage In Developed And Developing Countries*, (Oct. 21, 2016, 10:30 AM), https://www.diva-portal.org/smash/get/diva-2:695339/-FULLTEXT01.pdf
[13] R Jason Richards, *The Utah Digital Signature Act as "Model" Legislation: A critical Analysis*, John Marshall Journal of Information Technology & Privacy Law, (1999).
[14] Utah Digital Signature Act, 1995
[15] C. Bradford Biddle, *Misplaced Priorities The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, San Diego Law Review, (1996).

Utah Digital Signature act aims at facilitating the electronic commerce by encouraging reliability on electronic communications and information.

2.1.3.2. American Bar Association Digital Signature Guidelines, 1996

Digital Signature Guidelines was developed and published by the American Bar association in the year 1996. American Bar Association is associated with the information security committee in America. The Digital Signature guidelines were developed by the association with the aim to provide assistance the professionals and users in determining not only the authenticity of electronic signatures but also the quality of the electronic signatures.[16] The guidelines were developed as a result of participation of technical experts and 70 legal practitioners from different countries. It took 4 years of joint team work of these professionals to establish such guidelines for digital signature. These guidelines became the first outline as a framework and fundamental use of the digital signatures and verification of the digital signatures in Ecommerce from the legal perspective.[17] Though now these guidelines may be considered incomplete but it formed were elementary part for dealing with digital signatures during that period.

2.1.3.3. UNCITRAL Model Law on Electronic Commerce, 1996

Model Law on Electronic Commerce was adopted by the UNCITRAL: United Nations Commission on International Trade and law on 12th June, 1996. The Model Law on Ecommerce was developed as international rule that would be acceptable to all the member nations which would further enable the member nations to frame their own legislation based on the Model law with the view of facilitating commercial transactions through electronic medium.[18] The Model law aims at providing significant equivalence between the contracts and transactions based on electronic

[16] Legalesign Staffwritter, *The History Of Signature*, The Legalesign Blog, (Oct. 23, 2016, 12:30 PM), https://legalesign.com/blog/history-of-signatures/.
[17] Edward D. Kania, *The ABA's Digital Signature Guidelines: An Imperfect Solution to Digital Signatures on Internet*, Lexis Nexis, (Oct. 25, 2016, 11:39 AM), https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&srctype=smi&srcid=3B15&doctype=cite&docid=7+CommLaw+Conspectus+297&key=d710d4162d8024b3752b9f200f900999.
[18] UNCITRAL Model Law on Electronic Commerce (1996).

medium and the paper based transactions.[19] The Model Law on Electronic commerce was established to overcome the barriers which would arise from the national legislations in the commencement of ecommerce. The equal treatment to the electronic commerce with the paper based transactions is very important for stimulating effectiveness in International trade. The rules made under the Model Law on Electronic Commerce provide validity to the Electronic Contracts.

UNCITRAL Model Law on Electronic Commerce was the primitive legislative work adopted by the commission which aimed at promoting neutral technological approach, antidiscrimination principles and functional equivalence of the technology being used in electronic commerce. The provisions of Model Law on Electronic Commerce were later adopted by the Model Law on Electronic Signature. Electronic Communications convention amended few provisions of the Model Law on Electronic commerce for meeting new practices that were being implemented in electronic commerce.

2.2. Need for Digital Signature

Signatures play the most important role in the business transactions and contracts. Consent of the party is one of the essential ingredients for the formation of a valid contract. Signature of the party represents the consent of the party to the terms of the contract. Since the business transactions are now taking place over the internet, users should inculcate the habit of signing the documents digitally. Digital signature on the electronic contract would represent the consent of the party to the transactions taking place over the internet. The traditional methods of signing documents at the end cannot match with the requirement of authentication of the electronic documents on the internet. Authentication of the electronic documents is now much more complicated on the internet. Since the electronic documents are more prone to the attacks and can be easily changed or modified, it becomes necessary that the electronic records or documents should be digitally signed.[20] Internet offers anonymity and a user of internet can be located in any geographical location while entering into electronic contracts, hence digital signatures play a vital role for the purpose of proper authentication of the identity of the individual entering into the contract.

[19] UNCITRAL Model Law on Electronic Commerce (1996), UNECTE Trade Facilitation Implementation Guide.
[20] *Id.* at 8.

The business transactions and the electronic contracts are now conducted instantly by the users with the use of electronic mails and internet. Parties to the contract can now easily share their offers and acceptance to the terms of the contract by transmitting their electronic documents over the within a few minutes. Hence it becomes very important to verify the information or data which is being transmitted in the cyberspace. One party to the contract or transaction must be able to authenticate the identity of the other party by verification of the signature. Digital Signature provides the most suitable mechanism which method which provides authentication, integrity and non-repudiation to the electronic document. Digital signature uses the cryptographic algorithm to encrypt the message and then after calculating its hash value, it provides more security to the document in the electronic medium.

There also exists a great risk of alteration of the electronic documents over the internet by the cybercriminals. The criminals can easily forge, modify or change the content of any document very easily on the internet. Through correct implementation of the Digital signatures we can mitigate the risk of tampering of messages, maintain the integrity of the messages, curtail the likelihood of dealing with the imposters or defrauders who forge signatures and we can also ensure high level security.[21]

2.3. DEFNITIONS

2.3.1. TECHNICAL DEFNITION OF DIGITAL SIGNATURE

Since signature plays a vital role in authentication and legal verification, it has found its importance in the digital medium also. Increase in the communication that flows online, coupled with importance of affixing signatures, it becomes necessary not only to recognize digital signature but also to define it.

From the name itself, it is evident that digital signature is a signature for digital medium. In a little elaborative word it is a digital or mathematical code that authenticates as well as assures the integrity of an electronic message or records[22]. In other words Digital signature is a representation of signatures in the electronic medium. It is used to authenticate the communication in the electronic medium or to

[21] S.K. Bansal, *Ecommerce Laws*, Cyber Millennium Challenges and Opportunities, pp. 225, (2001).
[22] Margaret Rouse, *Digital Signature*, TechTarget, (Oct. 25, 2016, 11:26 AM), http://searchsecurity.techtarget.com/definition/digital-signature

authenticate electronic records and messages[23]. Due to invent of Digital signatures, a lot of paper work has been reduced and there has been an increase in e-contracts also.

Digital signature comprise of a pair of asymmetric keys associated to each other, one being public while the other is a private or secret key. Any data encryption with a private key can be decrypted solely by the public key corresponding to it. Like every individual has a unique signature, the uniqueness of the digital signature for each user can be derived from the said pair of asymmetric keys which are unique to the individual subscriber. After a legally recognized procedure and verification, a digital signature certificate, having details of the subscriber, public key, issuing authority etc., is issued by controller of certifying authority[24].

Digital signatures are based on the cryptographic techniques. It ensures a receiver that the message is from the intended sender and the contents are also authentic. It is a signature in the form of a code is attached to a message.

2.3.2. Definition of Digital Signature under Information Technology Act, 2000

Digital signature has been legally recognized in India under information technology (amendment) act under section 2(p) mean an electronic mode of authenticating electronic record. This in clear term means, verifying the contents of the document and identification of the sender using an electronically generated unique sign or symbol or a code. For the purpose of an elaborative explanation, section 2(P) is read with section 3 of the act which describes the working of the digital signature along with core elements of authenticating an electronic record. As per section 3, effective authentication of an electronic record shall include

1. Asymmetric cryptographic keys which are unique to the subscriber.
2. A hash function or a mapping algorithm to map hash results
3. Original text or electronic record
4. Encrypted text

[23] Jayakumar Thangavel, *Digital Signature Comparative Study Of Its Usage In Developed And Developing Countries*, (Dec 21, 2016, 10:30 AM), https://www.diva-portal.org/smash/get/diva-2:695339/-FULLTEXT01.pdf.
[24] *Id.* at 12.

The hash function should transform original electronic record in to another electronic record by enveloping it.

From a clear reading of the section, digital signature can be understood as a code, which hides the electronic record with the help of a private key and communicated in such a way that the receiver receives an electronic record different from the original record. The receiver should be able to retrieve original record and hash value by using public key. To check the authenticity of the message, the hash value of both the original as well as encrypted record should be the same. Also, it provides that the verification of the record could be done by anyone by using public key of the subscriber.

Role of Digital signatures is the same as that of a traditional medium. It allows the receiver to rely on the received text and gives a reason to believe its genuineness and integrity if the hash value matches that of the sent message. It binds the sender to the contents which he cannot deny later only if can prove that it was not sent by him. It is a secure form of signature and allows detection of tampering of text in transit[25].

2.3.3. Definition of Electronic Signature under Information Technology Act, 2000

Information technology Act, wide its amendment in 2008 inserted a new concept of electronic signature. Section 2(ta)[26] defines electronic signature as a wider set of signatures in the electronic medium and includes digital signatures.it means authenticating electronic records by any electronic techniques specified under schedule VII of the Act[27]. These techniques may or may not provide security like a digital signature. The techniques could be signing manually on the computer screen or may be a signature b clicking a check box. There is no reliability whether or not such signatures are genuine or that if any other information has been tampered could not be found out[28].

[25] Admin, *Law of Digital Signature*, CertifcateTiger, (Oct 28, 2016, 03:40 PM), http://www.certificatetiger.com/News/law-of-digital-signature.htm
[26] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).
[27] *Id.* at 12.
[28] Emily Maxie, *The Difference Between Digital Signatures and Electronic Signatures*, Signix, (Oct. 30, 2016, 11:15 AM), https://www.signix.com/blog/bid/92791/The-Difference-Between-Digital-Signatures-and-Electronic-Signatures

Thus, electronic signature is a pool of techniques to authenticate an e-record and includes digital signatures too. Hence all digital signatures are electronic signatures but the reverse holds no true. It provides technology neutrality[29]. Introducing electronic signature as a definition in the IT Act, validation and legal recognition of future signing technologies have improved. Any new technology that will allow a user to make a signature on the electronic medium would be thus a legally recognized electronic signature[30].

UNICTRAL model on electronic signatures,2001 defines electronic signature under Article 2 clause (a) as "Electronic signature means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message;"[31]

2.4. DIFFERNCE BETWEEN – DIGITAL AND ELECTRONIC SIGNATURE

- Electronic signature is the wider term while Digital signature is the specific term which comes under the categories of Electronic signature. Still the two digital signature and electronic signature are distinct from each other. Electronic signature refers to any kind of symbol, image, sound or process which is electronically applied to any digital document while digital signature refers to the use of cryptographic method which converts the document content into a new message and digitally signs this new message with a private key.[32]
- Electronic signatures are more easy to use, they are user friendly and can seem similar to the ink signatures that can be used on electronic document while digital signatures are the mathematical schemes which are much more

[29] Yogesh Kolekar, *Electronic Signature – Legal and technical Aspect*, LegalServicesIndia, (Dec. 02, 2016, 04:45PM), http://www.legalservicesindia.com/article/article/electronic-signature-legal-and-technical-aspect-1827-1.html
[30] Abhinav, *The Role Of Digital Signatures In Digital Information Management*, International Monthly Refereed Journal of Research In Management & Technology, (2013)
[31] UNCITRAL Model Law on Electronic Signatures (2001).
[32] Melanie Attiea, *Infographic: Electronic signature Vs. Digital Signatures – Defining the differences*, eSignLive, (Dec 19, 2016, 8:10 PM), https://www.esignlive.com/blog/infographic-defining-difference-electronic-signatures-digital-signatures/

complicated, they require multiple steps – including encryption, hashing and digitally signing.

- Even if a document has been signed with an electronic signature, there still exits the chances that an outsider will be successful in forging or making a copy of the original document. This is not the case with the digital signature. If a document has been signed with a digital signature then that document cannot be forged or copied.[33]
- Digital signatures provide more security to the electronic document when compared to the electronic signatures. Electronic signatures do not provide any kind of secure coding to the electronic document. Digital signature applies the encryption technique to the document, calculates its hash value and then binds it with the digital signature. No kind of alterations can be made to the document by others; any such attempt would render the digital signature invalid.[34]
- Digital signature assures the authentication of the sender's identity, origin of the document and nonrepudiation of the document transmitted by the sender while in case of electronic signatures it is not possible to authenticate the origin and the sender of the document or the nonrepudiation service to the electronic record.

2.5. CLASSIFICATION OF DIGITAL SIGNATURE

2.5.1. Class – 0 Certificate

The digital signature certificates issued under this class are meant only for either the demonstration purpose or for conducting the tests. These digital signature certificates have no other use apart from showing the individuals how a digital signature certificate works.

[33] Emily Maxie, *The Difference Between Digital Signatures And Electronic Signatures*, Signix, (Dec 19, 2016, 8:15 PM), https://www.signix.com/blog/bid/92791/The-Difference-Between-Digital-Signatures-and-Electronic-Signatures

[34] Lloyd Gallagher, *Electronic Signature Vs. The Digital Signature: The Same Thing*,(Dec 19, 2016, 8:30 PM), http://www.adls.org.nz/dialog/emailshare.aspx?Electronicvsdigitalsignaturessamething

2.5.2. Class – I Certificate

The Digital signature certificates belonging to the Class – I category are only issued to the private subscribers or the individuals. The name of the person and the official email address of that individual who has made application for the digital signature certificate of Class – I gets stored in the database of the Certifying Authority.

2.5.3. CLASS – II Certificate

The Class - II Digital Signature Certificates can be given to both the private individuals as well as the business entities. After the verification process of the individual has been completed, the Digital certificates belonging to Class – II can be downloaded by the individuals from a verified and trusted database. The information provided by the subscriber in the application for the Class –II digital certificate is stored in the consumer database which provides the proof for the individual subscriber's information. These digital certificates are generally used by the individuals in filing of the documents electronically with the Ministry of Corporate Affairs; the electronic documents can be related to Income Tax, Value Added Tax and filing documents with the Registrar of the Companies.

2.5.4. CLASS – III Certificate

The digital signature certificates of the Class –III category can be issued to both organisations as well as to the individuals. Higher level of verification process is involved in the issuance of the Class – III digital certificates. These digital certificates will only be issued after the individual or the member from the organisation has physically appeared in front of the certifying Authority. Class –III Digital signature Certificates provide high level of assurance, hence they are predominantly used in the applications of Electronic commerce. The digital certificates of this class are used mostly for the purpose of Electronic-Tendering involved in online procurement processes or for the Electronic-Auctions.

2.6. MODEL LAW ON ELECTRONIC SIGNATURE

Model law on Electronic signature was created by UNCITRAL: United Nation commission on International Trade Law, in 2001. UNICITRAL started working on

this project in year 1997. After 4 years the completed the project on Model Law which was then adopted by the full commission.[35] United Nations Commission on International Trade Law is one of the core bodies of the General assembly of Unite Nations. UNCITRAL follows the mandate of United Nation which states for continuous unification and harmonization of the International trade law. The Model Laws developed by UNICITRAL are meant to be enforced by the member nations all over the world. This Model law made by UNCITRAL has been used as base by many nations for developing their national laws on Electronic signatures. The UNCITRAL Model Law has been successfully adopted in more than 30 jurisdictions.

2.6.1. PURPOSE

The aim of MLES: Model Law on Electronic Signature is to facilitate the usage of electronic signatures by creating more technological trustworthiness and reliability between the handwritten signature and the electronic signature.[36] The Model Law on Electronic Signature acts as a base framework in assisting the member nations to develop modern legislation which would provide fair treatment, certainty in status and legal recognition to the electronic signatures.

2.6.2. RELEVANCE

With the increase in the use of internet and telecommunication technologies the traditional handwritten signatures have been predominantly replaced with the electronic signatures. Traditional methods used for authentication of signatures cannot be used for the purpose of authenticating the electronic signatures. Hence a need arises here for development of new methodologies for the authentication of electronic signatures. There is a need for particular legislative framework that would minimize the uncertainty related to the usage of electronic signatures.[37] To meet such requirements a fundamental principle was instated in Model Law on Electronic Signature that has been derived from the article 7 of the Model law on Electronic Commerce, it states that a neutral technological approach should be adopted in an electronic environment. Hence the laws of a nation that are developed on the basis of

[35] Commentary - on the UNCITRAL Model Law on Electronic Signatures (1996).
[36] UNCITRAL Model Law on Electronic Signatures (2001).
[37] *Id.* at 16.

Model law would recognise electronic signature as well as digital signatures based on different technologies.

2.6.3. KEY PROVISIONS

The Model Law on Electronic Signature is significantly based on the very fundamental principle of the UNICITRAL Model laws which emphasises on adoption of neutral technology, facilitating Ecommerce and providing functional equivalence between the electronic signatures and handwritten signatures. The Model law on Electronic Signature also emphasis on the substantive equivalence of electronic signatures, it contains provision regarding the legal recognition of foreign certificates and digital signatures. The Model law tries to encourage the confidence in usage of electronic signatures in the legal transactions. The legal effectiveness of electronic signatures has been offered by the provisions of the UNICITRAL Model Law on Electronic signature.

The UNICITRAL Model Law on Electronic Signature states that the technologies that are at present being used are as follows:[38]

I. Passwords
II. Personal Identification Numbers (PINs)
III. Biometric Device
IV. Digital Signature with Public Key Infrastructure (PKI)
V. Scanned Handwritten Signature
VI. Signature by Digital Pen

[38] *Id.* at 18.

CHAPTER -3

3. WORKING & APPLICATION OF DIGITAL SIGNATURE

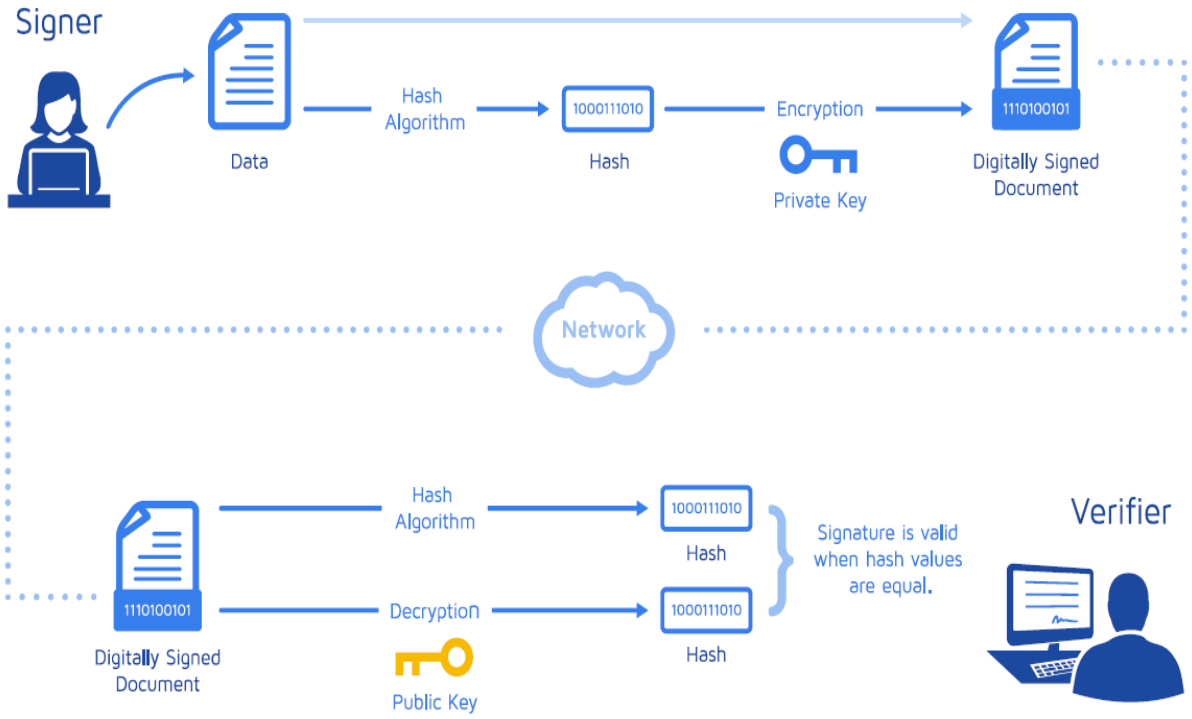
3.1 Overview of the functioning of the Digital Signature

The Digital Signature is a technique through which any information or message in the form of any contract, document can be securely transmitted over the network by using encryption algorithm coupled with the hashing algorithm. It is a mathematical scheme which can be utilised for the purpose of authenticating any electronic document. In the whole process of digital signature a new message abstract is produced by using Hash algorithm which, then this new message abstract is further encrypted and the seal or signature of the sender is affixed to the new message abstract with the help of another algorithm which performs final stage encryption. The encryption feature of digital signature performed on the new message abstract of the original message provides assurance about the integrity, authentication and non-repudiation of the message transmitted to the receiver. Digital signatures can be transmitted over the network with ease, they also contain time stamp which can be utilised for verify the accurate time when the message has been sent by the sender. This digital signature technology is thus used by the people for the purpose of authenticating the identity of the person who sends or signs the document. The Digital signatures are predominantly used for the distribution of software's, in formation and transmission of electronic contracts and in financial transactions.

The technology of Digital Signature is entirely based on the method of Public key Encryption which mostly makes use of the efficient algorithms such as DSA and RSA. The Digital signature utilises a pair of keys which are associated to each other based on a mathematical value generated by the algorithm. The Private Key of the owner and Public key which is available to all the people, distributed in public constitute the key pair. These pair of keys is also known as asymmetric key pair because in the encryption process the keys utilised to encryption and decryption of the message are not exactly same, these keys are different but related to each other based

on a mathematical formulae.[39] The private key belonging to the owner of the Digital signature needs to be kept secured and confidential. This key should not get into the hands of any other person else they would impersonate the actual owner and send fraudulent messages in the name of the owner of the digital signature. Anyone having the public key which is associated to the private key can verify the digital signature of the sender. In order to completely understand the process of the digital signature we must first try to understand cryptography as a technique with specific reference to Public Key Encryption.

The diagram mentioned below shows the whole process of Digital Signature:



3.2 How the digital signature works – Illustrative steps

1. Take the electronic document file into the computer system and load it into the software of Digital Signature.
2. The software converts the original electronic document into a hash value by applying the hash function.

[39] Hongjie Zhu & Daxing Li, *Research on Digital Signature in Ecommerce*, Vol. I, Proceedings of the International MultiConference of Engineers and Computer Scientists, Hong Kong, (2008).

3. Then the encryption algorithm with the help of the private key of the owner of digital signature encrypts the hash value into a cipher message.
4. The encryption algorithm then affixes the digital signature to the encrypted hash value.
5. The encrypted data is transmitted to the receiver through the open network (internet).
6. The receiver utilises the public key to decrypt the encrypted hash message and receives the original message after computing the hash value.
7. The receiver can then compare the decrypted value of the message with the original hash value, if both of them appear to be same then the message transmitted is free from any kind alteration or damage but if the values don't match then the message has been altered or damaged.[40]

3.1. WORKING

3.1.1. Components of Digital Signature

I. Cryptography

Cryptography refers to the technique of transmission and storage of the information in such a manner no other person apart from the person/receiver intended would be able to access and read the information. Cryptography can be understood as the science which deals with mathematical schemes that are utilised for the purpose of encryption and decryption of any information. Cryptography is the tool which ensures the security of the information which is being transmitted to other person. As a tool it converts the normal text message into the cipher text message that cannot be understood or read by unintended individuals. Cryptography involves two processes, namely encryption and decryption. Cryptology is the study of both the scientific techniques namely: cryptography and cryptoanalysis.[41] Cryptoanalysis refers to the technique of breaking down the encrypted secure information/message into normal text message and analysing it. Sometimes the people who attempt to attack on the encrypted message and try to decrypt it are also referred as Cryptoanalysts.

[40] Bhagyashree, Arpita, Chandana & Soujanya, *A Role Of The Digital Signature Technology Using RSA Algorithm*, (Jan 11, 2017, 12:13 PM), https://www.ijsr.in/upload/1215419297Microsoft%20Word%20-%20NCRIET-329.pdf
[41] Henk C.A. van Tilborg, *Fundamentals of Cryptology*, (Jan 10, 2017, 11:20 AM), https://www.hyperelliptic.org/tanja/teaching/cryptoI13/cryptodict.pdf.

The algorithm used in cryptography is a function which is involved in performing the encryption/decryption action on the input message. Encryption is the process of converting the message/information into encrypted message known as Cipher message. While decryption refers to the process of conversion of the cipher message which is in the encrypted form back to its normal form. The functioning of this algorithm completely relies on the usage of pair of keys known as Private Key and Public Key. The algorithm uses the private key to convert the normal text message input into the encrypted text message which is commonly referred as Cipher text message. The Cipher text cannot be easily comprehended or read unless until a software is used to convert it into a normal text message. If the private/secret key is kept safe then the encrypted data i.e. the cipher text can be kept secured from the attackers or the unintended individuals. Only the right public key would be able to decrypt the encrypted message, if wrong key is used then it would not be able to decrypt the message. The keys play a very major role in the whole encryption/decryption process. Hence Encryption forms the most important process of the cryptography which ensures that the information cannot be read by other people apart from the intended receivers.

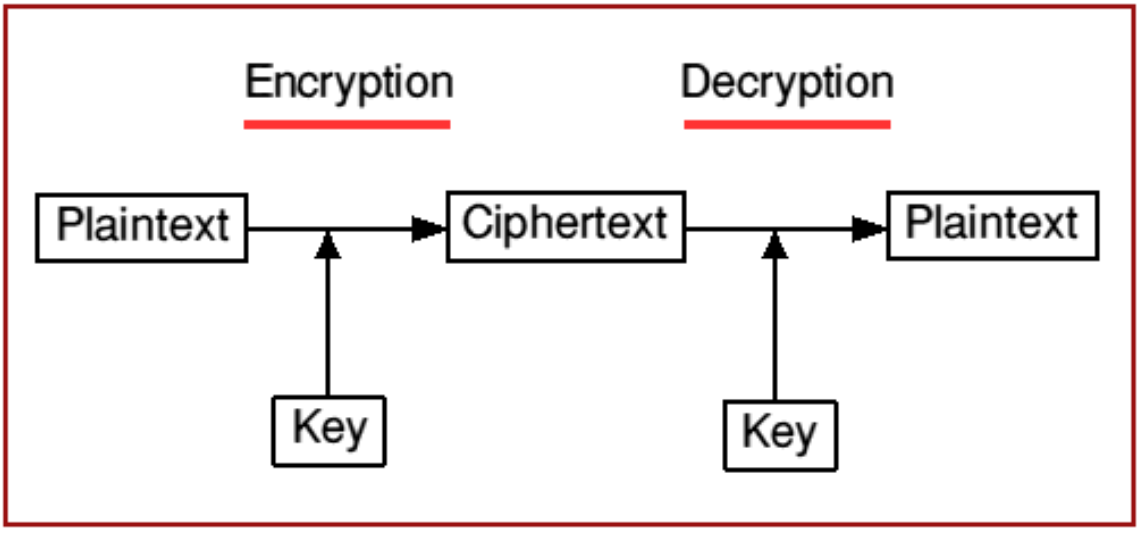
Types of Cryptographic System:

1. Symmetric Cryptography
2. Asymmetric Cryptography

The traditional system of cryptography is based on the symmetric pair of keys in which both the private as well as the public key used in the process of encryption and decryption are identical. The symmetric Cryptography system uses a single unique key is for the purpose of encryption and decryption of the information.[42] The encrypted data in the symmetric cryptography can easily be decrypted, if the person knows the secret key. This is why symmetric cryptography is not considered to be very secure.

Digital Signature is purely based on the application of the Asymmetric Key Cryptography which ensures more security to the message as both the keys are non-identical. The below stated diagram depicts the process of Cryptography.

[42] Karnika Seth, 2013, *Electronic signature*, Computers Internet and New Technology Laws, pp. 133.



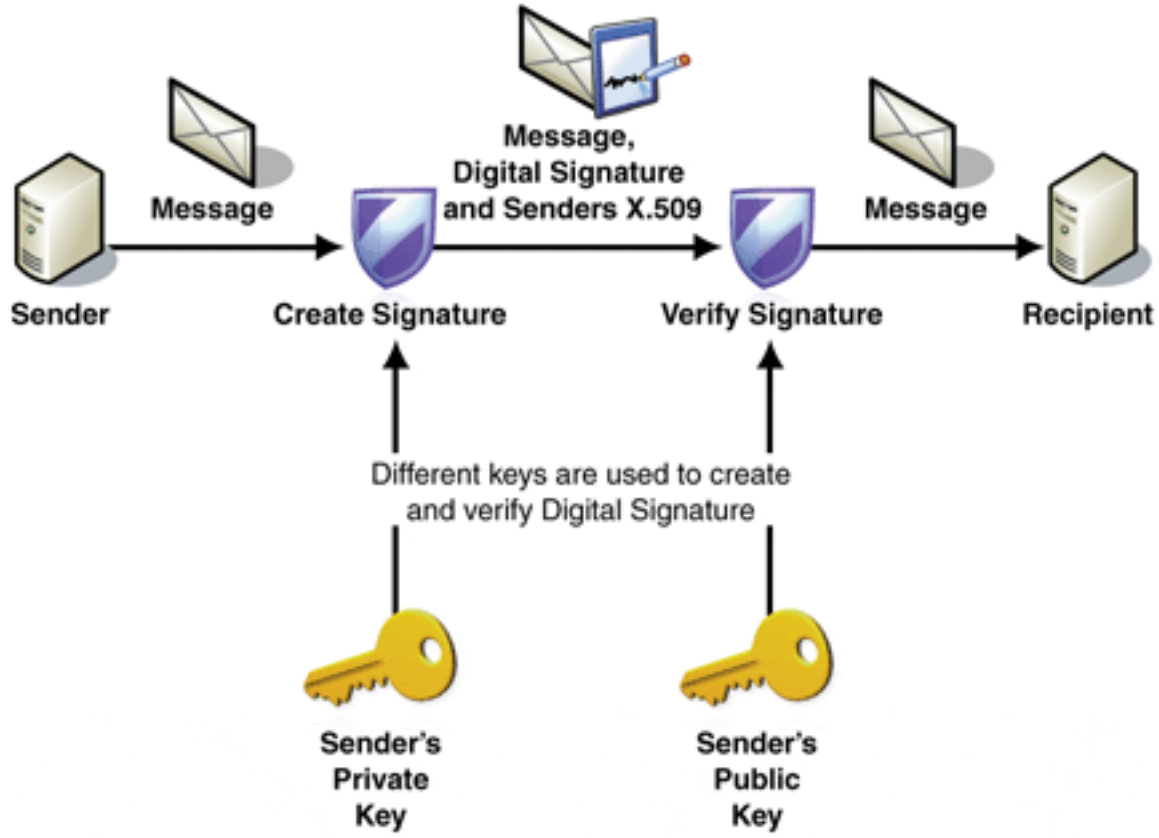
II. Public Key Encryption

It becomes important to know what exactly Public Key encryption is, as the digital signature is primarily based on this scheme. Public Key Encryption is the cryptographic system which uses a pair of unsymmetrical keys for the encryption and decryption of the information.[43] The Public Key Encryption sometimes is also referred as the Asymmetric Cryptography system. In this Cryptographic system there are two keys used by the algorithm which form the key pair, namely: Secret key and the public key. Both the keys are mathematically related to each other. The public key is available on the internet for all the people; they can download it and use it for decrypting the encrypted message. The secret or private key is only with the owner or sender. The owner of the secret/private key needs to keep it secured from other person for the encrypted message to remain confidential. Even if a person has access to the public key still it is impossible to calculate the private key mathematically. The public key Encryption technique provides more security, it also ensures the confidentially and integrity of the encrypted message.

The first Public key Encryption scheme was developed in the year 1978 by the developers: Ronald Rivest, Adi Shamir and Leonard Adleman.[44] This encryption scheme was named after them as RSA Algorithm. The RSA Algorithm provides more

[43] Hongjie Zhu & Daxing Li, Research on Digital Signature in Ecommerce, Vol. I, Proceedings of the International MultiConference of Engineers and Computer Scientists, Hong Kong, (2008).
[44] Bhagyashree, Arpita, Chandana and Soujanya, *A role of the Digital Signature Technology Using RSA Algorithm*, (Jan 11, 2017, 12:13 PM), https://www.ijsr.in/upload/1215419297Microsoft%20Word%20-%20NCRIET-329.pdf

security to the data, hence it is mostly used in Digital Signature for encrypting the hash value. There are main three algorithms for asymmetric cryptography namely: Elliptic curve, DSA and RSA.



III. Hash Algorithm

The hashing algorithm takes as input any information provided by the user, it then calculates new message abstract. The most important component of the hashing algorithm is the hash function which can take as input any file/document. The algorithm's hash function always produces new short message abstract of a fixed size. This new abstract message produced for the input messages can never be the same, the hash function produces different abstract messages for different input files. The hash value which is calculated by the hash functions forms the base for designing the keys used in the Public Key Encryption.[45] Few examples of the Hash algorithms are SHA Algorithm i.e. Secure Hash Algorithm and MD5.[46] Digital signature uses the

[45] Jeff Tyson, *How Encryption Works*, HowStuffWorks, (Jan 28, 2017, 02:35 PM), http://computer.howstuffworks.com/encryption5.htm
[46] Hongjie Zhu & Daxing Li, Research on Digital Signature in Ecommerce, Vol. I, Proceedings of the International MultiConference of Engineers and Computer Scientists, Hong Kong, (2008).

hash algorithm to provide more security to the document. When the receiver gets the encrypted hash file, he decrypts the file and calculates the hash value. If the calculated hash value is similar to the original hash value of the file, then the file is secure.

3.1.2. ALGORITHM USED IN DIGITAL SIGNATURE

Rabin signature algorithm

A method of Digital signature in cryptography is the Rabin Signature Scheme which was originally proposed by Michael O. Rabin in 1979.One of the first digital signature schemes to be proposed was The Rabin Signature Scheme. Along this, it was also the first to relate forgery hardness directly to the inter factorization problem. The Rabin Signature Scheme because of its simple and prominent role in early public key cryptography is covered in most of the introductory cryptography courses. Assuming that the integer factorization problem is intractable, in random oracle model the Rabin Signature scheme is existentially unforgeable. The Rabin cryptosystem and the Rabin Signature Scheme are also closely related.

Three steps are involved in RSA algorithm: key generation, message data encryption and message data decryption. The following simplified algorithm is used in modern presentations.

H is known as the hash function which is assumed as a random oracle. Following is the working of the algorithm:

"Key Generation

1. The primes *p,q* each of size approximately *k/2* bits are chosen by the signer *S* and the product is computed as *n= pq*
2. *n* is the public key
3. *(p,q)* is the private key

Signing

1. The signer *S* picks random padding *U* to sign a message *m* and H(mU) is calculated
2. A new pad *U* is picked up by *S* if *H(mU)* is not a square modulo *n*
3. The equation is solved by *S* as *x^2 = H(mU) mod n*
4. The pair *(U,x)* is the signature on *m*

Verification

1. A message m and a signature (U,x) is given, x^2 and H(mU) are calculated by the verifier V and also verifies that they are equal."[47]

[47] Hongjie Zhu & Daxing Li, Research on Digital Signature in Ecommerce, Vol. I, Proceedings of the International MultiConference of Engineers and Computer Scientists, Hong Kong, (2008).

First, the Message Digest Function is padded in to 512 bits and then using MD5 algorithm it is condensed.[48] Using the RSA algorithm the condensed message is then encrypted and thus a signature is created. The Message and the Signature are transmitted to receiver. The signature obtained is decrypted (using RSA algorithm) by the receiver on his end and the receiver further compares it with Message Digest.

3.1.3. MECHANISM OF DIGITAL SIGNATURE

Digital signatures as an application of public key cryptography were introduced in 1976 by Diffie and Hellman. Since then digital signatures have been predominantly used by the people. Using public key cryptography digital signing and signature verification can be done which is based on public and private key pairs. With the private key the holder of the key can sign a signal message which he intends to transmit to other recipients.

Steps involved in the mechanism of Digital Signature:

- Creation Of – Digital Signature
- Signing of - Digital Signature
- Verification of – Digital Signature

A. DIGITAL SIGNATURE CREATION

I. **Public keys:** Confirmation of the identity of the signer by using the certificate authority's services is created through the public key certificate. In associating a particular public key with an individual, a range of processes are used by a certificate authority. If anyone wants to have your signature's verification, you give your public key to them. Your public key combined with the proof of identity result in a public key certificate is known as a signer's certificate.

II. **Private keys:** You keep your private key with yourself. You use your private key to sign a document. Mathematically, the public keys are associated with the private keys. It is known that the verification of the signature is allowed by the public key but it does not allow the creation of the new signature. Hence, without your consent, your signature on a document can be created

[48] Bhagyashree, Arpita, Chandana and Soujanya, *A role of the Digital Signature Technology Using RSA Algorithm*, (Jan 11, 2017, 12:13 PM), https://www.ijsr.in/upload/1215419297Microsoft%20Word%20-%20NCRIET-329.pdf

maliciously by someone if your private key is not kept as “private”. Secrecy of your private key is thus important.

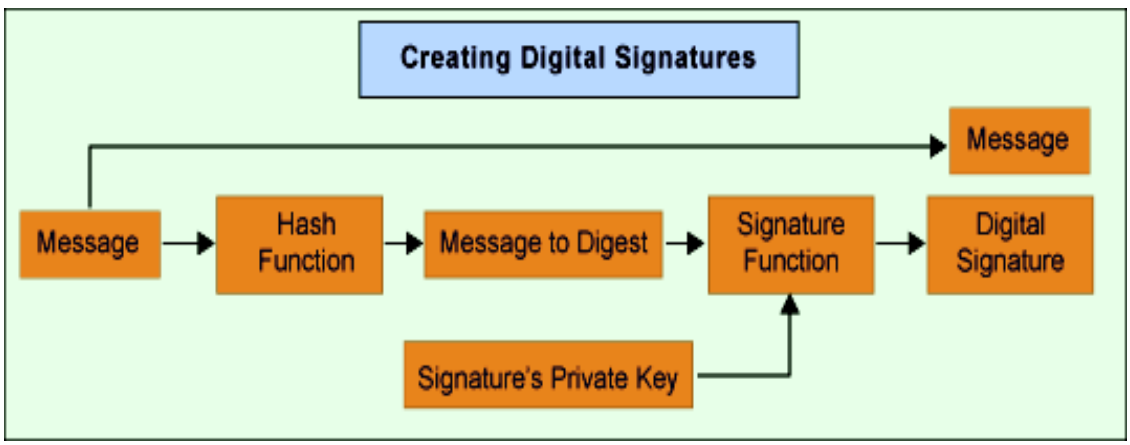
B. THE DIGITAL SIGNING PROCESS

Step 1: Calculation of the message digest:

By applying some of the cryptographic hashing algorithms example MD2, MD4, MD5 or other, the message digest (a hash value of the message) is to be calculated. The calculated hash value of a message usually has a fixed length, is a sequence of bits and is extracted from the message. When just a single bit from the input message is changed, a different digest is obtained by the application of mathematical transformation used for message digest calculation. From a given hash value of a given message, it is almost impossible to find out the message. Theoretically, it is possible that two entirely different messages have the same hash value which is calculated by some of the hashing algorithms. For this to happen, the probability is so small that it is ignored in the practice.

Step 2: Calculation of the digital signature

The information which is obtained from Step 1 is encrypted. Digital signature which is an encrypted hash value is thus obtained when the information (hash value of the message) is encrypted with the private key of the person who signs the message. Some of the mathematical cryptographic encrypting algorithms are used for this purpose. RSA (based on the number theory), ECDSA (based on the elliptic curves theory) and DSA (based on the theory of discrete logarithms) are most often used. Generally, the obtained digital signature is attached in a special format to the message that can be verified later if there is a requirement.



C. DIGITAL SIGNATURE VERIFICATION

Verification of the real origin and integrity of the recipient of given signed message is permitted by digital signature technology. The Aim of the digital signature verification process is to find out whether a given message has been signed by private key which corresponds to a given public key. Determining whether the given message has been signed by a given person is not possible with the use of the digital signature verification process. In some manner, we need to obtain the public key if we need to know whether a given message has been signed by a person or not. With the help of a digital certificate or securely getting the public key (on a floppy disk or CD) this can be possible. Checking whether the given message is signed by the person in real is impossible without the usage of a secured way in order to get the real public key of given person.

DIGITAL VERIFICATION PROCESS

Step 1: Calculation of the current hash value:

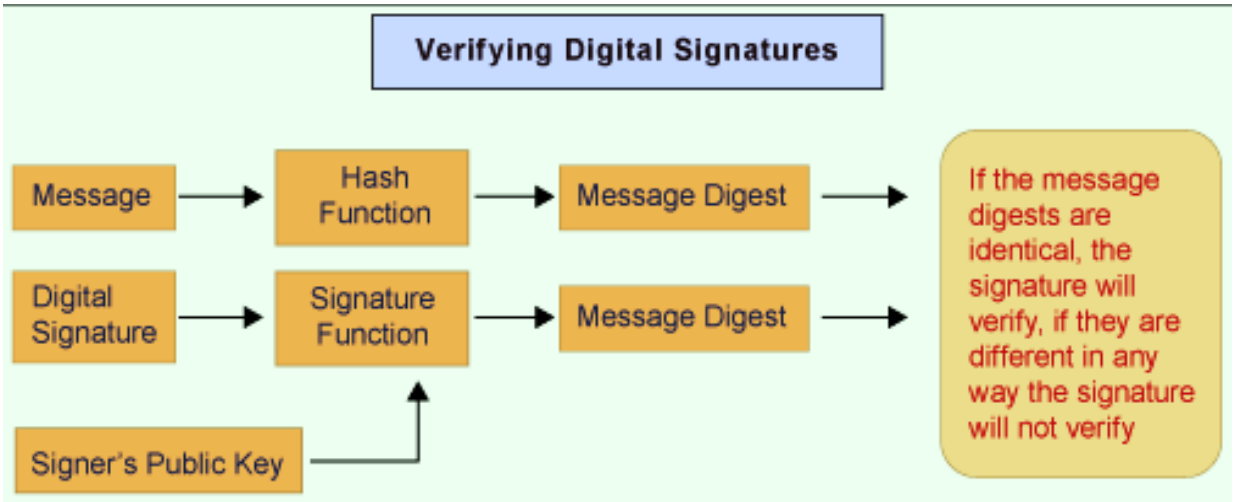
For calculation of a hash value of the signed message, the same hashing algorithm is used as it was used in the signing process. The obtained hash value is known as the current hash value since it is derived from the message's current state.

Step 2: Calculation of the original hash value:

Decryption of the digital signature is done using the same encryption algorithm as it was used in the signing process. The decryption process includes the usage of the public key that relates to the private key which was used in the signing of the message. Hence, the original hash value (the original message digests) is obtained.

Step 3: Comparison of the current and original hash values:

The current hash value obtained from Step 1 is compared with the original hash value obtained from Step 2. The verification is successful when the two values are equal and hence proves that the message has been signed with the private key that corresponds to the public key which is used in the process of verification. The digital signature is invalid and hence the verification is unsuccessful if the values are not equal.



3.1.4. TYPES OF ALGORITHMS USED IN DIGITAL SIGNATURE

1. "RSA PSS which is a variant of the RSA Signature Scheme.
2. ElGamal Mathematical Signature scheme
3. DSA Signature Scheme.
4. Rabin Signature Algorithm.
5. BLS, Pair based Scheme.
6. Undeniable Signature."[49]

3.2. APPLICATION OF DIGITAL SIGNATURE

3.2.1. AUTHENTICITY

Authentication refers to the process of establishing and verifying the identity of the individual who has sent the message to another individual. Authentication as a process has very important role in day to day activities of the individual ranging from communication of confidential message to electronic business and financial transactions. It becomes very important for the receiver to verify the origin of the document as well as the identity of the sander of the document. Since the mode have transactions has shifted from traditional medium to the electronic medium, the authentication of the electronic record also needs to be ensured. Use of Digital Signature is one of the mechanism through which a person can authenticate a message

[49] Jyotsana Mahajan, *Key Security Feature: Digital Signature*, (Jan, 11, 2017, 12:20 PM), http://www.csimumbai.org/newstrack/Oct-Dec-2013/Key%20Security%20-%20Cloud.pdf

and verify the identity of the sender of the information in the form of electronic record.[50]

Digital signature is the mathematical function that uses the cryptography to encrypt a message. The private key of the digital signature which is a unique secret key associated to the specific owner of the digital signature. It is only the owner of the digital signature who has the private key and no other person has the access to the private key. This secret key is used to secure the document by applying the cryptographic hash function to the document. The secret key binds the digital signature of the owner to the document. A valid digital signature forms sufficient proof of the fact that the information in the message has been sent by the sender who is the original owner of the digital signature.[51] The digital signature can prove to be very useful in verification of the origin of the document in question. The receiver of the document can use the associated public key which is available to all to authenticate and access the information secured by the digital signature.

3.2.2. INTEGRITY

Integrity of the information in the document is yet another very essential component which needs to be ensured and maintained through proper secure mechanism applied to the document. In electronic communication or transaction on the internet the data is transmitted through the open network.[52] Sometimes it becomes important that both the parties receiver as well as sender need to have the assurance that integrity of the information has remained intact without any tampering throughout the transmission. Integrity refers to the state of information which provides that the content of the file or document has not been altered or changed. Hash function is the best approach to ensure that the integrity of the information remains intact. This can be easily achieved through application of digital signature to the information which ensures that the information will remain in its original form. Encryption of the information alone cannot guarantee that the information would remain unaltered. Even after applying the encryption process to the information there may still exist some possibilities that the

[50] *Id.* at 30.
[51] Ralph Merkle, *A certified Digital Signature*, Vol. 435, Advances in Cryptology – Crypto'89, pp. 218
[52] C. R. Rachana, *The role of digital signature in Information Management*, Vol. II, International Monthly referred journal of research in Management & Technology, (2013).

content of the document might get tampered by the attackers.[53] This is not the case with the digital signature.

One of the key roles of Digital signature is that it helps in maintaining the essential integrity of the electronic document which is transmitted to the receiver. Digital signature applies the cryptographic hash function to the information which is secured by the use of a private key and results in production of a secure encrypted message. Digital signature ensures the protection of the integrity of the information which is intended to be sent to the other person. Once the digital signature has been applied to the information there can be no possibility of intentional or any kind of accidental alteration or change in the content of the document. If any kind of attempt is made in order to alter or change the content of the document which has already been digitally signed will lead to invalidation of the digital signature.[54] The reason behind such invalidation is that the hash function calculates a value of the entire message and the digital signature is then applied on this new message or value created.

3.2.3. NON-REPUDIATION

Non repudiation is an essential component of the traditional contract which states that a party to the contract, who has already signed it, later the party cannot deviate from its authentication in relation to the identity of the party. Nonrepudiation can be used as fact against the person who is trying to deny the origin or communication or any kind of action which has been earlier made by him. In digital communication also the nonrepudiation element plays a major role, as nonrepudiation is an essential aspect of the digital signature. Non repudiation is essentially used in the email communications, electronic contracts and financial transactions between the parties to make them legally bound by the document or communications. It provides a service for poof of the origin as well as for the integrity of the information which has been digitally signed by the sender.

Digital signature has the same legal binding effect on the person signing the document just like that of the handwritten signature. The involvement of the party cannot be denied by them at the later stage once they have bound themselves by applying the

[53] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, Chapman & Hall CRC Press, (2007).
[54] Mao Wenbo, *Modern Cryptography: Theory & Practice*, Prentice hall of technical reference, New Jersey, pp. 308, (2004).

digital signature to the document. The nonrepudiation service can only render to be a problem in a situation if the private key associated to the digital signature has already been revoked by the authorities prior to its usage on the document.[55] Non repudiation can become difficult to prove if the private key of the owner of the digital signature gets compromised and some criminal is able to fraudulently obtain it. The criminal can fraudulently use this digital signature in multiple transactions which are not originally signed by the actual owner of the digital signature and as a result the nonrepudiation service provided by the digital signature cannot be assured in this situation. Hence it becomes very important that for the nonrepudiation purpose of the information, the secret key of the digital signature owner must be secured. It should not have been compromised or stolen by any other person.

[55] Hongjie Zhu & Daxing Li, *Research on Digital Signature in Ecommerce*, Vol. I, Proceedings of the International MultiConference of Engineers and Computer Scientists, Hong Kong, pp. 22, (2008).

CHAPTER – 4

4. Legal Provisions and Authorities of Digital Signature under Indian Legislation

4.1. Digital signature and Information Technology Act, 2000

Indian IT industry plays a vital role in the economy and over all GDP of the country. The transition from IT as a department to entire enterprise being automated and run by IT is significant. Indian being a developing country has made efforts to keep par with the technology. Ever since the country has submitted to cyberspace, a progressive step has been taken not only to introduce new technologies, security ensures, but also be legally sound and vibrant country. The Indian Legal as well as commercial ideologies work hand in hand and believe, a better regulatory framework promotes influx of investment, trade, technologies, and advancement. Recognition to both Technical developments and progressive Indian Legal system has been well established. There is a huge inflow of technology and the country itself has made a huge IT base, need of strong legal backbone was well understood by the legislators. For the security and to gain trust in the working of the IT industry, digital signatures and electronic signatures have been given a legal recognition. The chapter highlights with the provisions of the IT (Amendment) Act, 2008 that deal with electronic and digital laws in India and how aforesaid recognition has been given.

Indian Laws on Information Technology has not been diverse like other countries. A single act[56] along with its one amendment of 2008[57] has broadly covered offences, digital signatures, electronic signatures, authorities, etc. The law has been comprehensive in itself to deal with the theme of the dissertation. The importance of digital signatures for the country, its IT base, enterprise IT and the economy can be predicted with the detailed law on the subject matter. The Act defines the mode of signing an electronic record by the virtue of electronic and digital signatures, the authoritative recognition of it, and functions and power of the said authority.

[56] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).
[57] The Information Technology (Amendment) Act, 2008.

Section 2(f) of the act defines the Asymmetric Cryptographic System which is used for signing the electronic record with the digital signature. It discusses the use of two different kinds of keys, private and public respectively to ensure safe and secure verification of the electronic communication. The section is simply an overview of the system used for verification of the signatures. It does not penetrate deep into the technicality of how it actually is used to verify or the working of the system. The section reads as:

> "*Asymmetric crypto system means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.*"[58]

Certificate of electronic signatures play a remarkable role in the entire system of verification and electronic communication. Even the certificate has been given a legal base to be admissible and justified. Certificate is a grant of a authority, and not a self-authorized subject matter like a traditional signature. A dedicated authority to issue the certificate and a controller has been granted a licence and appointed respectively. The following two sections elaborate on the legal definition of Certifying Authority and its Controller.

Section 2(g) of the act defines the Certifying Authority. The section reads as:

> "*Certifying Authority means a person who has been granted a licence to issue an electronic signature Certificate under section 24.*"[59]

Section 2(m) of the act defines the Controller of the Certifying authority. The section reads as:

> "*Controller means the Controller of Certifying Authorities appointed under subsection (7) of section 17.*"[60]

To proceed with the theme of the dissertation, it is important to understand how well it has been recognized or legally laid down in the Act. Digital signature, as discussed in earlier chapters is a signature in the digital medium used for ensuring the

[58] Section 2(f), The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).
[59] Section 2(g), The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).
[60] Section 2(m), The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).

authenticity and integrity of the electronic records and for the said purpose a certificate of the same is also issued which is also defined separately in the Act.

Section 2(p) of the act defines the Digital signature. The section reads as:

> "*Digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.*"[61]

Section 2(q) of the act defines the Digital signature Certificate. The Section reads as:

> *"Digital Signature Certificate means a Digital Signature Certificate issued under sub-section (4) of section 35.*"[62]

Section 2(ta) of the act defines the Electronic Signature. The Section reads as:

> "*Electronic signature means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature.*"[63]

Section 2(ta) of the act defines the Electronic Signature Certificate. The Section reads as:

> "*Electronic Signature Certificate means an Electronic Signature Certificate issued under Section 35 and includes Digital Signature Certificate.*"[64]

As discussed in the working of the asymmetric cryptographic system of verification, a pair of keys, public as well as private is used. The private belongs the subscriber whereas public is known to the intended recipients. Both the keys together make up a key pair. There can be only one subscriber to whom the private key is uniquely given whereas the public key is given for the purpose of multiple recipients. It would be right to say; a private key is private in nature and known only to one party whereas a public key can be known to more than one person and to anybody with whom the subscriber of the private key holder intends to enter into an electronic communication. Subscriber is the person who applies for a certificate for electronic certificate enlisting

[61] Section 2(p), The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).
[62] Section 2(q), The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).
[63] Section 2(ta), The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).
[64] Section 2(ta), The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).

public and private key duly assigned. For the purpose, the legal definition of key pair, public, private key and the subscriber is given below.

Section 2(x) of the act defines the Key Pair. The Section reads as:

> "*key pair in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.*"[65]

Section 2(zc) of the act defines the Private Key. The Section reads as:

> "*Private Key means the key of a key pair used to create a digital signature.*"[66]

Section 2(zd) of the act defines the Public key. The Section reads as:

> "*Public key means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.*"[67]

Section 2(zg) of the act defines the Subscriber. The Section reads as:

> "*Subscriber means a person in whose name the Electronic Signature Certificate is issued.*"[68]

Section 2(zh) of the act defines the verification in relation to the digital certificate. The section deals with the process the key pair is used to define what exactly and how verification takes place. The definition does not restrict to only authentication but also talks about integrity and non-repudiation. The use of digital signature is to ensure, that the signature is verified to an extent that by use of public key the recipient can know the corresponding private key as affixed by the intended user and also, the contents of the record is not tampered or altered with. The Section reads as:

> "*Verify in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether - the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscribe. The*

[65] Section 2(x), The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).
[66] Section 2(zc), The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).
[67] Section 2(zd), The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).
[68] Section 2(zg), The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).

initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature."[69]

The Act has taken a step further in describing how exactly authentication takes place by the use of hash function and has also defined, though in ore technical terms, but hash function also. A value, called as hash value, is used check whether the value before transmission of the message and after s receipt is same or not. In case, any change in the hash value takes take, it can be inferred that an alteration in the sent has taken place and the message received is not what was originally sent. The message sent is encased in a hash function, which generates a value called as hash value. If the value is changed it means some alteration was attempted to be done against that hash function and henceforth, access to hash function would mean access to the confidential or encrypted message. A hash function is used to change the original text into an encrypted message. The function maps the encrypted text and gives the original text to the recipient. This change of original text into encrypted text generates a value called a hash value which the receiver checks whether or not the received value is same as the sent one or not. If not, it indicates repudiation of the message, the section has in a short yet comprehensive way explained the authentication procedure.

Section 3 of the act defines what does the process of Authentication of electronic record means which is affixed by the digital signature. The Section reads as:

"*Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature. The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record. Explanation - For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible - To derive or reconstruct the original electronic record from the hash result produced by the algorithm. Two electronic records can produce the same hash result using the algorithm. Any person by the use*

[69] Section 2(zh), The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).

of a public key of the subscriber can verify the electronic record. The private key and the public key are unique to the subscriber and constitute a functioning key pair."[70]

Section 5 of the act tells us about the status of electronic signature which has been legally recognised through this provision of the act. The section clarifies that the need of affixing an electronic signature is sufficient to satisfy the need of authenticating the document. It can inferred that the electronic or to say digital signature has been given functional equivalence of that of a signature in the traditional medium. The Section reads as:

"*Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signatures affixed in such manner as may be prescribed by the Central Government. Explanation - For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.*"[71]

Section 14 of the act talks about security of an electronic record. it is to be well said that any document that has been sent after applying some security to it, or to say any procedure with an intent of making the electronic document secure, is applied, then the record is said to be secure electronic record. The Section reads as:

"*Secure electronic record - where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.*"[72]

Section 15 of the act states what secure electronic signatures are. An electronic signature can said to be secure under circumstances when it is under the control of the

[70] Section 3, The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).
[71] Section 5, The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).
[72] Section 14, The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).

signatory exclusively, without any other party having any access or mode of utilization of it. The Section reads as:

> "*An electronic signature shall be deemed to be a secure electronic signature if - the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person and the signature creation data was stored and affixed in such exclusive manner as may be prescribed."*[73]

Section 17 of the act states provision for the appointment of the controller. Since controller plays a significant role, Central government has the power to appoint a controller and other officers including Deputy Controller after a notification in the official Gazette. It also determines the power of the controller to supervise and assign the functions to its subordinate officers. The tenure, terms and conditions of the office of the controller is all under the legislative power of the central government. The Section reads as:

> "*Appointment of Controller and other officers - The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers Assistant Controllers, other officers and employees as it deems fit. The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government. The Deputy Controllers and Assistant Controllers shall perform the functions- assigned to them by the Controller under the general superintendent and control of the Controller. The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers Assistant Controllers, other officers and employees shall be such as may be prescribed by the Central Government. The head office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places*

[73] Section 15, The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).

as the Central Government may think fit. There shall be a seal of the Office of the Controller."[74]

Section 18 of the act states the functions of the controller. As discussed earlier, Controller has a significant role in the entire process of digital signatures, their authorities, supervision, etc., the section enumerate the functions of the controller to be such as a supervisor of the certifying Authority, certifying public keys, deciding the terms of employment of the Certifying Authority and lay standards for conducting business. It is an elaborative section which deals with various other functions of the Controller such as, resolving disputes between authorities, maintain databases, and other instructive and supervisory functions. The Section reads as:

"The Controller may perform all or any of the following functions, namely - exercising supervision over the activities of the Certifying Authorities. He shall certify the public keys of the certifying authorities. Lay down the standards to be maintained by the Certifying Authorities. He may specify the qualifications and experience which employees of the Certifying Authorities should possess. Specifying the conditions subject to which the Certifying Authorities shall conduct their business. Specifying the contents of written, printed or visual material and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the Public Key. Specifying the form and content of a Digital Signature Certificate and the key. Specifying the form and manner in which accounts shall be maintained by the Certifying Authorities. Specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them. Facilitate for the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems. Specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscriber. Resolve any conflict of interests between the Certifying Authorities and the subscribers. Laying down the duties of the Certifying Authorities. Maintaining a data-base containing of disclosure record of every Certifying Authority containing such particulars as may be

[74] Section 17, The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).

specified by regulations, which shall be accessible to public."[75]

Indian Laws give regards to foreign laws equally, also, because of most of the technology transfers and international business; the Indian vendors may have to maintain relations with other Nations vendor, which may have certificate from authority of their nationality. The said purpose has been equally and legally recognized under the Indian Law by recognizing foreign certifying authorities and their granted certificates.

Section 19 of the act tells about the recognition of the foreign Certifying Authority. The Section reads as:

> "*Subject to such conditions and restrictions as may be specified by regulations; the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any Foreign Certifying Authority as a Certifying Authority for the purposes of this Act. Where any Certifying Authority is recognised under sub-section (1), the Electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act. The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.*"[76]

Section 35 of the act states the procedure for the Certifying Authority to issue Electronic signature certificate. It is an illustrative section dealing with all the requirements that have to be fulfilled and the stepwise procedure to be followed by a subscriber including the process undertaken by Certifying Authority. The Section reads as:

> "*Any person may make an application to the Certifying Authority for the issue of an Electronic Signature Certificate in such form as may be prescribed by the Central Government. Every such application shall be accompanied by*

[75] Section 18, The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).
[76] Section 19, The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).

such fee not exceeding twenty- five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority. While prescribing fees, different fees may be prescribed for different classes of applicants. Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations. On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Electronic Signature Certificate or for reasons to be recorded in writing, reject the application. No application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection."[77]

Controller is the supreme authority when we talk of electronic and digital signatures, and the certificates thereof. If under any circumstances, for the purpose of obtaining a certificate, any illegal act, or wrongful act of misrepresentation, omission of doing something legal or hiding a materialist fact from the controller takes place a criminal penalty for two years or a civil penalty up to one lakh will have to be borne by the person making such presentation or for any of the acts laid above.

Section 71 of the act states the Penalty for misrepresentation. The Section reads as:

"*Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.*"[78]

It is appreciable to note that the legislation has foreseen the probable crimes that can be done using electronic signatures and for the said purpose, have laid down both criminal as well as civil compensation for making available any certificate which is either not listed, revoked, suspended or unaccepted.

[77] Section 35, The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).
[78] Section 71, The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).

Section 73 of the act states the Penalty for false Certificate. The Section reads as:

> "Penalty for publishing Electronic Signature Certificate false in certain particulars - No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that - the Certifying Authority listed in the certificate has not issued it; or the subscriber listed in the certificate has not accepted it; or the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a electronic signature created prior to such suspension or revocation. Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."[79]

Similar to traditional signatures, digital signatures also possess a threat of fraudulent use or misuse. For the said purpose, the IT act, talks for punishment up to two years or compensation up to one lakh in case of fraudulent use of the digital signature with the knowledge and for unlawful purpose.

Section 74 of the act defines the punishment for fraudulent use of the digital signature Certificate. The Section reads as:

> "*Whoever knowingly creates, publishes or otherwise makes available an Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.*"[80]

4.2. Digital Signature and Indian Evidence Act, 1872

Indian legal system is proof driven. Everything that has to be proved needs to be accompanied with evidence for the same or for the purpose of corroboration. Indian Evidence Act is a legislation much required to fulfil the said need of the legal system. It determines admissibility and relevance of the evidence. It is a very old legislation unaware of the probable technology inflow that India would have and the impact it would have in the admissibility of the evidence. Initially, the act was silent on any mode of electronic medium and corresponding evidences, blaming the absences of IT

[79] Section 73, The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).
[80] Section 74, The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).

technologies then. The act was amended to include electronic records within the ambit of the evidence. The admissibility non-admissibility is lateral stage to recognizing something as evidence. The amendment was an initiative to include records in the electronic medium within the definition of evidence and grant it equal recognition of a tradition record in the physical world.

Section 3 of the Indian Evidence Act was amended to include electronic records in meaning of the term evidence. The Section reads as:

> "*Evidence means and includes all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry such statements are called oral evidence and all document including electronic records produced for the inspection of the Court such statements are called documentary evidence.*"[81]

The Act highlight the need to give proof of a signature in the electronic medium in the manner it requires that of a traditional medium. Like a person needs to prove or disprove his signature in the court of law, the same demand has been laid down in case of digital signature. Simply because the signature is digital in nature and has certificate of the same, no presumption of the fact that it belongs to subscriber is undertaken by the court expect in case of a secure digital signature.

Section 67A of the Indian Evidence Act states proof as to digital signature. The Section reads as:

> "*Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved.*"[82]

There is a strict presumption taken in favour of the secure digital signature of its integrity unless the other party discharges its burden of proof by disproving the presumption in other words, to say, by proving the contrary. Also, presumption to affixing of the signature by the subscriber itself has also been laid down subject to proving in contrary. The section explicitly debars presumption to authenticity and

[81] Section 3, The Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872(India).
[82] Section 67A, The Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872(India).

integrity of the electronic signature or other digital signatures but restricts its presumption only to the subscriber and the secure digital signature, subject to disproving the same.

Section 85B of the Indian Evidence Act states presumptions as to electronic record and digital signature. The Section reads as:

> "*In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the point of time to which the secure status relates. In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that - the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record and except in the case of a secure electronic record or a secure digital signature, nothing in the section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.*"[83]

4.3. Digital Signature and Indian Penal Code, 1860

The Indian Penal Code of the country is substantive law that provides for what is wrong and is punishable under the law. The said code has also recognized executing an electronic record falsely by using digital signatures. Any alterations to the document or without lawful authority changing a part of a document, with an intention to mislead the recipient with fact as to who signed the document or that it was the intended document that the sender wanted to send, is a punishable offence. Misusing the mental condition a subscriber for the said purpose is also punishable under the law.

Section 464 of the Indian penal code defines making of false document as offence. The Section reads as:

> "*A person is said to make a false document - Who dishonestly or fraudulently makes, signs, seals or executes a document or part of a document, or makes any mark denoting the execution of a document, with the intention of causing it to be believed that such document or part of a document was made, signed,*

[83] Section 85B, The Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872(India).

sealed or executed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed or executed, or at a time at which he knows that it was not made, signed, sealed or executed or Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document in any material part thereof, after it has been made or executed either by himself or by any other person, whether such person be living or dead at the time of such alteration or Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document, knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practiced upon him, he does not know the contents of the document or the nature of the alteration."[84]

4.4. AUTHORITIES TO ISSUE DIGITAL SIGNATURE CERTIFICATES IN INDIA

Certifying Authority under section 24 of the IT Act 2008[85] is the licenced body which has the power to issue a digital signature certificate to the people in India. The certifying authority also has the power to renew and revoke the digital signature certificate.

The list of the 7 Certifying Authorities which are currently working in India is mentioned below in this section. These Certifying Authorities are licensed under the Controller of Certifying Authority and they are authorised to issue digital certificates in India. All these certifying authorities can be approached through their websites and online application can be made to them for obtaining the Digital Signature certificate.

4.4.1. Safescrypt

Safescrypt was the very first certifying authority India which was given license to issue digital signature. Apart from issuing digital signature certificates, it provides security services and solutions in the field of IT management.

[84] Section 464, The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860(India).
[85] Section 24, The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).

4.4.2. NIC

National Informatics Centre Certifying authority is a licensed certifying authority in India. Currently the NIC has stopped issuing and renewal of any digital certificates due to the recent security breach at its certifying authority's office. This has been notified on the official website of NIC Certifying Authority.

4.4.3. IDRBT

Institute for development and research in Banking and Technology was set up in the year 1996 by the RBI, India. IDRBT is a licensed Certifying Authority in India. IDRBT provides Digital signature certificates to 3rd Parties and it also provides Public Key Infrastructure services as well to all the applicants.

4.4.4. TCS

Tata Consultancy services Limited has also been given license by the controller of certifying authority. Not only it deals in IT Solutions and services but it also has the power to grant digital certificate to the applicants after proper verification.

4.4.5. MTNL

Mahanagr Telephone Nigam Ltd. is a licensed certifying authority in India. Since 2011 MTNL also had stopped issuing any digital signature certificate due to some operational defects faced by them.

4.4.6. Customs & Central Excise

The board of Customs & Central Excise sis also licensed to issue digital signature certificates to people in India.

4.4.7. (n)Code Solutions CA (GNFC)

(n)Code Solutions Certifying authority has been set up as a division of the Gujarat Narmada Valley fertilisers and chemical Ltd. The (n)Code Sol. Provides Public Key Infrastructure services & solutions, security services and issues digital signature certificate.

CHAPTER – 5

5. ADVANTAGES & DISADVANATGES OF THE DIGITAL SIGNATURES

5.1. Advantages of Digital Signatures

i. **SPEED:** The use of digital signatures has overcome the time taking processes and delays faced by the people in the traditional business methods. People are no longer completely dependent on the paper documents to form the contracts which used to take a long duration to transmit to the other party trough the postal or courier services. Regardless to the geographical location of the person, electronic contracts are now formed and digitally signed much faster with the help of the digital signatures. Digital signatures have made the transmission of the documents and communications over the internet much faster and with greater assurance to the authentication and integrity of the electronic documents.[86]

ii. **SECURITY:** There always exists the possibility of the paper based documents getting tampered, destroyed or altered while the document is being sent to the receiver through traditional delivery mechanisms. These risks of any kind of possible changes to the document can easily be avoided by the use of electronic documents and application of digital signatures. The use of digital signatures provides security to the electronic document.

iii. **AUTHENTICITY:** The documents signed with digital signature provide assurance for the authenticity of the document. They can authenticate the identity of the individual who sent the document as well as the origin of the document. The IT law in India has given legal recognition to the electronic record and digital signature. The electronic record is now considered to be

[86] Nahid Hassan, *Advantages and disadvantages of Digital Signatures*, (Feb. 02, 2017, 9:13 PM), http://lerablog.org/technology/datasecurity/advantagesanddisadvantagesofdigitalsignatures/

equivalent to the paper document in the court of law.[87] Hence the any electronic record which has been signed with the digital signature can be produced in the court of law as an admissible evidence to prove the authenticity of the document.

iv. **COSTS:** The amount of money spent by people on paper, documentation of contracts and the delivery services is quite expensive if compared to use of digital signature on the electronic documents. Use Digital Signature is a cost effective way. It saves the cost of transmission of the important document over the emails when compared to the charges for dispatching the paper based documents through the courier services.[88]

v. **TIME-STAMP:** The feature of time stamp is provided by the Digital signature which is attached to a document whenever it is digitally signed. This feature helps the receiver of the document to know exactly when the sender signed the document.[89] This feature is heavily utilised by the experts in forensics of cybercrime cases involving electronic record.

vi. **FACILITATE: E-COMMERCE, ONLINE BANKING:** Majority of the transactions now take place through the electronic medium. Digital signature enables the user to maintain the integrity and the trust in the use of electronic documents by providing security to it. The digital signature has facilitated the services like online banking, information exchange and electronic commerce.[90]

vii. **TRACKING:** With the help of the Digital signature the document in transmission can be tracked very easily and its location can be known by the sender within minutes. Compare to the traditional transmission modes not

[87] Anant Patel, *Advantages and Disadvantages of Digital Signature*, Digital India Insight, (Feb. 04, 2017, 9:25 PM), http://digitalindiainsight.com/advantagesanddisadvantagesofdigitalsignature/
[88] Jyotsana Mahajan, Key Security features: Digital Signature,
[89] Admin, *Essay: Advantages and Disadvantages of Digital Signature*, Super Custom Essay, (Feb. 04, 2017, 10:15 AM), http://supercustomessay.com/essayadvantagesanddisadvantagesofdigitalsignatures/
[90] Pallab Dutta, *Advantages of a Digital Signature*, Techwalla, (Feb. 04, 2017, 9:20 AM), https://www.techwalla.com/articles/advantagesofadigitalcertificate

much effort has to be made in order to track the document digitally signed by the sender.

viii. **IMPOSTER PREVENTION:** One of the major advantages of using a digital signature is that, it cannot be forged by other person. The document signed by a digital signature cannot be forged or tampered as any kind of attempt to change it will render the signature applied to the document invalid. Digital signature first creates a new message by applying the hash function and then digitally signs this new message. This helps in preventing the imposters to forge the document or the digital signature.

5.2. Disadvantages of Digital Signatures

i. **EXPIRATION:** Unlike the handwritten signatures the digital signatures do have an expiry period. The lifespan of a Digital signature is short. Though the industries and individuals are now heavily dependent on the technology and electronic communications but the digital signatures used by the people in electronic transactions and communications work only for a short period of time. After the expiration of the digital signature, person needs to obtain new digital signature from the certifying authority.

ii. **COMPATIBILITY:** The compatibility of Digital signatures is a major concern for the people sharing electronic documents in the digital environment. There exist many different kinds of digital signature schemes and standards which are likely to be not very compatible with each other. This creates some problem for the users to share the documents digitally signed in the digital environment which supports multiple incompatible digital signature standards.[91] This makes the interaction between the people a bit difficult.

iii. **WEAK LAW:** Many nations around the world still do not have any legislations governing electronic commerce. They are unable to provide legal recognition to the electronic record and digital signature. Further the

[91] Nahid Hasan, *Advantages and Disadvantages of Digital Signatures*, (Feb. 07, 2017, 1:40 PM), http://lerablog.org/technology/datasecurity/advantagesanddisadvantagesofdigitalsignatures/

legislations developed by some of the countries on technology and electronic communication are unable to properly govern the aspects of the digital signatures. In such countries the rights of the people cannot be enforced as there exists no legal remedy due to the lack of legal recognition to the electronic documents and signature. It becomes a risk for the users of the digital signatures to share information or to transact with the people belonging to such countries by using digital signatures.

iv. **SOFTWARE REQUIREMENT:** In order to work with digital signatures the users are required to purchase software's from the vendors for the verification of the documents which are signed with the digital signatures. Such software's are a bit expensive for the people but are essential for the functioning of digital signatures. Both the sender as well as the receiver needs the software for verifying the digital signature attached to the document.

CHAPTER – 6

6. Crimes related to Digital signature and their Impacts

6.1. CRIMES

6.1.1. MISREPRESENTATION

Cybercriminal often to misrepresent the identification details in order to obtain fraudulent digital certificates for committing crimes. It has been found that the Certificate Authorities do not critically examine the identification information related to the individuals or corporate organisations which seek to purchase Digital signature certificates from them. The cybercriminals are taking advantage of this fact and they have started exploiting this negligence on the part of Certificate Authorities. While validating the identity of the entity that is willing to purchase the digital signature certificate, the Certificate Authority in practice merely seek to verify the credit card details of the individual issued to them by the banks or in case of corporate organisation the Certificate Authority merely check the registration details of the company. The cybercriminals can easily misrepresent themselves and fraudulently obtain the digital signature certificates from the Certificate Authority in the name of other corporate organisation or an individual.[92]

The law recognises such acts of misrepresentation as offence which is punishable with imprisonment along with fine. In India Information Technology act, 2000 under section 71 states that if any person makes any kind of misrepresentation to the Certificate Authority for the purpose of obtaining the Digital Signature, it will be considered to be an offence under the said act and the said person committing such crime would be punished with punished with imprisonment for a period not less than 2 years or they will be charged with a fine amount of Rs 1 lakh or both imprisonment

[92] Michael Heller, *Digitally signed malware risk on the rise, Kaspersky finds*, TechTarget Blog, (Feb. 10, 2017, 05:37 PM), http://searchsecurity.techtarget.com/news/2240239598/Digitally-signed-malware-risk-on-the-rise-Kaspersky-finds.

as well as fine can be imposed on such offender on being caught committing such crime of misrepresentation for obtaining the digital signature.[93]

Even after detection of the fraudulent issue of digital certificate to the criminal, it does make much of difference to revoke the digital certificate. The cybercriminals are still able to use the revoked digital certificates due to weak security procedures followed by the web browsers. In a study conducted by United States the researchers have reported that almost 8% of the digital signature certificates have already been revoked but they are still being accepted by the Web browsers. The cybercriminals are using rogue digital signature certificates which are revoked to commit phishing scams. The researchers also found that majority of the web browsers do not examine the revocation status of the digital certificates. This fault of the web browsers is exploited by the attackers to launch fake domains on the internet which are used to steal sensitive information of the people.[94]

6.1.2. FAKE DIGITAL SIGNATURE

Fake digital signature certificate does not at any point mean forgery of digital signature, as digital signature certificate issued to individuals cannot be forged due to its complex nature.[95] Digital signature is the electronic code which is obtained by applying cryptography technique to the electronic file or information and calculating its hash value. This hash value is calculated by the cryptographic algorithms which will produce different value for different types of files. Hence the attackers can only manage to obtain unauthorised digital signature certificate by attempting the security breach at the Certificate authority's computer system or in case of any kind of human error in issuance of digital signature certificate. Forging a digital signature is not at all possible. It is also possible that the attackers can create their own versions of digital certificate to sign the malware developed by them but these fake digital certificate are not efficient as they can be easily detected by the security mechanism on the web browsers and operating systems.

---

[93] Road Broadhurst & Peter Grabosky, *Digital Signature*, Cyber-Crime: The Challenge in Asia, pp. 187, (2005).

[94] Peter Loshin, *Bad news for encryption security, PKI certificate revocation*, TechTarget Blog, (Feb. 12, 2017, 10:30 AM), http://searchsecurity.techtarget.com/news/4500257008/Bad-news-for-encryption-security-PKI-certificate-revocation

[95] Lee Shafrir, *Digital Signature: The Cyber security certification*, ComsignTrust, (Feb. 14, 2017, 12:45 PM), https://www.comsigntrust.com/digital-signatures-cyber-security-certification/.

The cybercriminals can utilise a fake root digital certificate for operating the fake domains to bypass the certificate validation mechanism on the web browsers. The attackers breach the security on the certificate authorities computer system and obtained the above mentioned fake root digital certificates.[96] Such incident of security breach at certificate authority was reported in India when a cybercriminal hacked into the computer system of NIC certificate authority and was able to obtain fake digital signature certificates.[97] There also have been incidents where the criminals produce fake identification documents to the certificate authorities and get successful in obtaining fake digital certificates. Cybercriminals also sell these fake or unauthorised digital certificates to other hackers who can use it to sign their malicious program. The price for selling these fake digital certificates in the market varies based on the Certificate issuing company.[98]

McAfee has stated in its report of 2015 that they were able to identify existence of more than 20 million malicious software's digitally signed in cyberspace, all these malwares were bearing fake digital signature. Developers have started listing practices and developing tools to prevent the use of fake digital signatures but this would take long time to be adopted by the authorities. This is another opportunity which is being used by the attackers to commit phishing crimes.[99]

6.1.3. STEALING DIGITAL CERTIFICATE

Nowadays the attackers can easily trick people into installing malwares on their computer systems through emails or software files on websites. The users of computers receive emails from anonymous sources which contain malicious attachments. Once the person installs this malicious code on the computer system, the system gets infected with malwares such as Trojan or other malicious codes. The hackers can take complete control of the users system by using the malware. The

[96] Lenny Zeltser, *How Digital Certificates are Used and Misused*, The Zeltser Blog, (Feb 16, 2017, 06:08 PM), https://zeltser.com/how-digital-certificates-are-used-and-misused/.
[97] Livemint Staffwritter, *NIC gets rap for issuing fake digital certificates*, LiveMint, (Feb 16, 2017, 08:38 PM), http://www.livemint.com/Politics/raFfYM4JbSoNxw22LyYpHM/NIC-gets-rap-for-issuing-fake-digital-certificates.html.
[98] Security Expert, *Cyber Crooks Selling Fake Digital Certificates*, Information security buzz news, (Feb 16, 2017, 10:50 PM), http://www.informationsecuritybuzz.com/expert-comments/cybercrooks-selling-fake-digital-certificates/.
[99] Barry Collins, *Fake signatures letting malware sneak onto your PC*, Expertreviews Blog, (Feb 17, 2017, 10:20 AM), http://www.expertreviews.co.uk/software/internet-security/1403867/fake-signatures-letting-malware-sneak-onto-your-pc.

attackers can further gain unauthorised access to all the files that are stored on the computer system and they can also misappropriate any information which is available on the computer.[100] If the attacker is able to gain access to the Windows certificate store on the computers operating system then they can successfully steal the digital certificate as well as the associated private key. Though chances of attackers to check each file and certificate store on the infected system is very tough but still if they manage to obtain the private key from the compromised system, the attackers can use this private key to digitally sign any malicious code.[101] Once the digital signature certificate has been stolen, a person cannot find who in actual signed the software or file. In addition to this after the digital certificate has been stolen by the cybercriminal and even if this theft of digital certificate gets discovered by the authorities, it is still very difficult to revoke this stolen certificate. Reason behind this is that revocation of this stolen certificate would result in all the software's which have been digitally signed through the certificate would automatically get revoked and would not be trusted as legitimate software.[102] By using the stolen digital certificate to sign the malicious code the cybercriminals can make the malware appear as a trustworthy code.[103]

To install software on the operating system it is required that the software must be signed with the digital certificate of trusted vendor. Hence the attackers steal the digital signature certificates of the trusted vendors in order to avoid the risk of detection of their malicious code or software. The windows operating system does not display any kind of warning if the file is signed with a valid digital signature certificate. There have been cases reported where the cybercriminals were successful in compromising the computer networks of trusted software vendors, thus by obtaining the private keys of these trusted vendors the hackers sign their malicious code and send these files to other people impersonating as original manufacturers of

[100] Hiroshi Shinotsuka, *How Attackers Steal Private Keys from Digital Certificates*, Symantec Official Blog, (Feb. 19, 2017, 11:20 AM), https://www.symantec.com/connect/blogs/how-attackers-steal-private-keys-digital-certificates.
[101] Andrew Ladikov, *Why you shouldn't Completely trust files signed with Digital Certificates* , SecureList, (Feb. 20, 2017, 07:10 PM), https://securelist.com/blog/security-policies/68593/why-you-shouldnt-completely-trust-files-signed-with-digital-certificates/.
[102] Roger A. Grimes, *Digital Certificates are helping deliver malware*, Infosec Blog, (Feb. 21, 2017, 09:20 PM), http://www.infoworld.com/article/3051755/security/digital-certificates-are-helping-deliver-malware.html
[103] Barry Collins, *Fake signatures letting malware sneak on to your PC*, ExpertReviews, (Feb. 21, 2017, 10:30 PM), http://www.expertreviews.co.uk/software/internet-security/1403867/fake-signatures-letting-malware-sneak-onto-your-pc.

software. It was also reported by security professionals that often legitimate digital signatures were stolen from the Certificate authorities or organisations and these theft incidents never came to their knowledge. Often these malicious codes were found to be signed with multiple digital signature certificates in order to avoid detection at the target computer systems.[104]

To obtain the digital certificate or private key the attackers design a special kind of malware which infects the system and specifically searches the files containing certificates on the computer in order to steal them.[105] The cybercriminals use these stolen private keys either for selling it to other people or using it for signing the malicious code developed by them. Signing a malware is not very difficult as Microsoft issues a number of signing tools accompanied with software's such as visual studio and Windows DDK. The attackers after obtaining the stolen private keys can use these signing tools to easily sign their malicious code or software. The cybercriminals are mostly able to obtain the private keys of either private individual or the small scale software manufactures who do not have strong security infrastructure. The cybercriminals are not able to infiltrate the computer networks of large scale software manufacturers because these big companies deploy strong protection of hardware's from external threats and they also ensure to store the private keys in secure hardware storage which is kept separate from the corporate network.

6.1.4. DIGITALLY SIGNED MALWARE PRODUCTION

Malware is a malicious code or computer program that infects the computer system, gains access to all the files stored and takes control of the system; the malicious software also gathers information residing on the system. Malware infusion with the Digital signature certificate of the Certificate authorities or trusted vendors is the new approach adopted by the criminals in their cyberattacks. Different operating system platforms such as Apple, Windows etc. use digital certificates for the purpose of

[104] Val S, *Malware is being signed with multiple digital signature certificates to evade detection*, Symantec connect Blog, (Feb. 23, 2017, 11:20 AM), https://www.symantec.com/connect/blogs/malware-being-signed-multiple-digital-certificates-evade-detection.
[105] Randy Abrams, *Why steal Digital Certificates?* , Welivesecurity Blog, (Feb. 23, 2017, 02:40 PM), http://www.welivesecurity.com/2010/07/22/why-steal-digital-certificates/.

installing software's on the computer system.[106] It has now become a major problem for these platforms that the malicious code can now bear a valid digital certificate, making it appear as a legit application. A digital signature certificate does not give any assurance that the file is free from any kind of virus. Digital signature certificate is only to authenticate the identity of the sender and to maintain integrity of the content of the original file.

The aim of the perpetrators behind signing a malware with Digital signature certificate is to avoid any kind of detection of the malware by the system. If the malicious code is digitally signed with a digital certificate of a trusted vendor the system would not show any kind of warning to the users while installing the malicious code on the computer system. The information of Digital signature certificate which is applied to a file does not form the part of original file. When the attacker signs the malicious file then this information regarding the signature gets stored in the header of the file which is not included while calculating the hash value of the file.[107]

Cybercriminals are targeting their attacks on the computer network of Certificate Authorities or Software manufacturing companies to infiltrate their servers and computer systems. After gaining access to the servers attackers can easily compile their malicious software with the valid digital signature certificate of the authorities.[108] The attackers can install spywares on the computer system of targeted victims and monitor all their activities, retrieve sensitive information of the victims to other computer systems. The cybercriminals have recognised the benefits of signing their malicious software's with not just one digital certificate but with multiple digital signature certificates. By signing the malicious software or malware with multiple digital certificates the attackers ensure that even if one of the digital certificates gets revoked, the malicious software would still be in signed state because of the other

[106] Nick Lewis, *Malware defence: Mitigating malware hiding as digitally signed software*, TechTarget Blog, (Feb. 25, 2017, 10:40 AM), http://searchsecurity.techtarget.com/tip/Malware-defense-Mitigating-malware-hiding-as-digitally-signed-software.
[107] Lucian Constantin, *Researcher hides stealthy malware inside legitimate digitally signed files*, IDG News Service, (Feb. 25, 2017, 11:40 AM), http://www.pcworld.idg.com.au/article/604698/researcher-hides-stealthy-malware-inside-legitimate-digitally-signed-files/.
[108] Andrew Ladikov, *Why you shouldn't Completely trust files signed with Digital Certificates* , SecureList, (Feb. 25, 2017, 09:37 AM), https://securelist.com/blog/security-policies/68593/why-you-shouldnt-completely-trust-files-signed-with-digital-certificates/.

digital certificate. This ensures that the malicious code would remain undetected and could easily be installed on the targeted computer systems.[109]

6.1.5. ECONOMIC FRAUDS

Cybercriminals are committing economic frauds through phishing scams in which they steal the bank credentials of people. In this section we are going to talk about Corporate Hijacking which has emerged as a new type of cybercrime with the misuse of the digital signature certificate which has become a major concern for the corporate entities. Corporate hijacking which is also known as identity theft of corporate is the crime in which the defrauders take control of the company's website using the digital signatures of its member directors to achieve illegal financial gains.[110] After taking control of the company's website the cybercriminals can make fraudulent transactions in the name of the company, make illicit transfer of shares and they can also upload fake minutes of the meetings.

To commit corporate hijacking the attacker has to first fraudulently obtain the Digitals signature of any one of the directors of the company. The DIN: Director Identification Number issued by government to each applicable director is associated with the digital signature issued to the director. The identification details about a director can easily be retrieved from the company's website which includes the information regarding DIN: Director Identification Number. The cybercriminals can misuse these identification details of the director of any company to obtain a fake digital signature from the certificate authority in their name. Once the attacker becomes successful in obtaining the fake digital signature of director; he can replace the original digital signature of the director from the website portal of the Ministry of Corporate Affairs with the fake digital signatures.[111]

---

[109] Val S, *Malware is being signed with multiple digital signature certificates to evade detection*, Symantec connect Blog, (Feb. 26, 2017, 12:35 PM), https://www.symantec.com/connect/blogs/malware-being-signed-multiple-digital-certificates-evade-detection.

[110] Brenda Hamilton, *What is corporate Hijacking?* , Security lawyers 101 Blog, (Feb. 26, 2017, 02:25 PM), https://www.securitieslawyer101.com/2017/traders-charged-trading-hacked-lawyers-posted-brenda-hamilton/.

[111] Bipasha, *Hijacking in the Corporate Sector: Issues and Challenges in India*, Industry study channel, (Feb. 26, 2017, 04:45 PM), http://www.indiastudychannel.com/resources/170383-Hijacking-in-the-Corporate-Sector-Issues-and-Challenges-in-India.aspx.

There have been several cases reported of security breach at large corporations and their computer network being hacked by cybercriminals.[112] In one of the Indian case the certifying authority E-Mudhra issued fake digital certificates in the name of director of the company to the cybercriminals. Bombay High Court judge in (MMPL) Maneklal Mansukhbhai Private Limited case has described Corporate Hijacking as an upcoming storm which is going to have enormous effect on the corporate organisations, capable of causing a huge catastrophe if much attention is not given to stop these kind of crimes.[113]

6.1.6. CYBERWARFARE

The rapid technological advancement has left a great impact on the society. Every aspect of an individual's life is now heavily dependent on the internet and information structure. Essential government sectors, private sectors and also the intelligence organisations are now controlled through use of computer systems, internet and computer networks. The defence officials of a nation have a constant fear that the cybercriminals or the government of the enemy states or terrorist groups may indulge in cyberwarfare activities by launching cyberattacks on the network of the country. These cyberattacks can be launched against essential networks that might be controlling Power plants, nuclear plants, banking system, stock exchange, telephone networks and transportation system. Such kinds of attacks would create disorder in daily lives of individuals, compromise the national security, disable the nations essential functioning within seconds and cause huge economic loss as well.[114]

Cyberwarfare is the act by a nation or terrorist groups or cybercriminals to infiltrate into the computer networks of other nation with the intention of causing damage to the nation. Cyberwarfare attack is the intended cyberattack on the crucial information systems of other nations. In today's modern world Cyberwarfare attacks are now politically motivated and sponsored at nation level. It is very unclear now which cyber

[112] Jerome Segura, *Digital certificates and Malware: a dangerous mix*, Malwarebytes Blog, (Feb 28, 2017, 01:40 PM), https://blog.malwarebytes.com/threat-analysis/2013/02/digital-certificates-and-malware-a-dangerous-mix/.
[113] *Id.* at 55.
[114] SANS Institute, *Information Warfare: Cyberwarfare is the future warfare*, Global Information Assurance Certification repository, (2004).

event caused by anonymous attackers or enemy nations might possibly trigger a war.[115]

Through Cyberwarfare attacks the way of fighting the wars between nations has changed. Cyber weapons can now be used as surprise strike anonymously to cause great damage to other nations. Such cyber weapons require a lot of manpower, time and huge amount of money for developing such long code malwares. Stuxnet attack and flame virus attack is very prominent examples of Cyberwarfare attacks which were sponsored by United States. The Malware used in these attacks was digitally signed with digital signature of trusted software vendors which lead to security breach at crucial information infrastructure and nuclear plant facilities in Iran. These cyberattacks caused huge economic loss to Iran.[116] Such cyberattacks can cause aggression in the victim state which might opt to war against the state that organised such attacks.

6.2. IMPACTS OF DIGITAL SIGNATURE CRIMES

Digital signature holds a very vital place in the e-commerce world today. Not only it is important for organizations dealing in e-commerce, but every organization that has some confidential information and exchange of it takes place in the cyber space. It would be right to say, that every entity is now on cyber space, henceforth it is important for all. Since cyber space is vulnerable and at the same time provides for so much anonymity, it is very difficult to prove who was the other side of the table for communication and whether the actual information is received or not. It has been widely discussed in the above chapters, the working of Digital signatures, reason for using it, mode of usage, advantages and other aspects of digital signatures. It would be incomplete to the knowledge of Digital Signatures if one doesn't know the impacts and consequences it can have in case of any tampering or theft of Digital Signature or its certificate. To bring it into the consideration, it is discussed in detail in the following chapter.

[115] Margret Rouse, *Cyberwarfare*, Tech target blog, (Feb 28, 2017,11:20 PM), http://searchsecurity.techtarget.com/definition/cyberwarfare.
[116] Patrick Lin, Neil Rowe & Fritz Allhoff, *Is it possible to wage a just Cyberwar?*, The Atlantic, (Feb. 30, 2017), https://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/.

Data is an important asset to any organization today. The more data one has, the better prospects of the business can be believed. It is not only required for analysis and knowing user preferences but also for the purpose of important business dealings and transactions to enter into. Every minute some or the other data is generated and information is being exchanged on the internet. The information might be a part of an important business dealing contract, some confidential information, some proprietary information, or maybe some sensitive personal data. During the exchange of such data, it is important to ensure and promote secure transmission. Indian legislators in this regard, took a step in promoting secure cyber space and cyber environment in laying down promotive steps, objective and other frame work by the virtue of National Cyber Security Policy, 2013. Since, a lot of loopholes and security concerns persist due to cyberspace; digital signature is significantly required and encases a lot of advantages. The importance of data, vulnerability of cyber space, and also malified intentions of many, if all coupled together and any digital signature is compromised, it has have an unavoidable impact on the organizations as well as individuals. Let us in brief see a few of the consequential impacts:

6.2.1. ECONOMIC LOSS

As stated earlier, data has value to business and so does confidential information and proprietary information. Since there are high chances that either of the three can be transmitted through electronic communications and could be encased in the digital signature, it is very important that the digital signature be kept safe. Theft of digital signature and further misuse of the same can be used to get access to such information, to impersonate the organization and related parties. Also, it can be misused to enter into fraudulent contracts resulting into economic damages. The signature is an association of the identity and also, by affixing it, acceptance of terms and conditions are deemed. If the data is misused or hacked or stolen, it can be used to impersonate, represent in any wrongful agreement, or enter into any agreement which the digital signature subscriber would not want to or didn't intend to enter into. For an illustration, A subscriber of a digital signature, has no clue that B has an access of his digital signature and B enters into a contract with C for delivery of some goods after using A's signature. C believing A to be the contracting party executes the contract.

On delivery of the contract, A refuses to have entered into any such agreement. C files a suit against A.

In the said illustration, A not only suffers economic losses, business relationships, but also loss of reputation. The same illustration can be thought of in case of a situation where the information in transit was confidential information or a trade secret. An impersonation in such a case would have caused an access to the data which only the organization and its prime members are supposed to know. Also, such information has a commercial value; any loss to it would result in indefinite loss and reputational loss to the organization. Since, digital signatures, bind people in the transaction, might result in wrongful or illegal transaction resulting into damage. There can be gain of access to the private key, which the person can himself, or through other, after selling the same, can bind the organization into any malicious contract[117]. Hence, if the control over the signature is lost, it can be used in any and every situation resulting into monetary losses. In case the data is lost, the liability as an intermediary would be an additional economic constraint on the organization, to not only defend the cases but also pay damages for the data lost.

Another dimension of huge economic loss suffered by big corporate giants is because of the crime of corporate hijacking which is accomplished by stealing the digital signature of the directors of the company. Since directors exercise the control over the entire business of the company, any cybercriminal by stealing the digital signature of the director can take over the control of the entire company. Once the cybercriminal or attacker has taken control they may illicitly transfer huge amount of shares in their own name or credit it to any other person.[118] The cybercriminals can impersonate to be the directors of the company by changing the details on the company's website through which they can enter into contracts in the name of the company. The criminals can fraudulently sell the assets of the company by falsely representing themselves to be the directors of the company to the third party. The criminals after obtaining the digital certificate of the directors can also upload false minutes of the

[117] Andrew Ladikov, *Why you shouldn't Completely trust files signed with Digital Certificates* , SecureList, (Mar. 02, 2017, 07:10 PM), https://securelist.com/blog/security-policies/68593/why-you-shouldnt-completely-trust-files-signed-with-digital-certificates/.
[118] Menaka Doshi, *Corporate Hijacking!*, MoneyControl, (Mar. 02, 2017, 11:30 AM), https://www.google.co.in/search?q=Corporate+Hijacking!&oq=Corporate+Hijacking!&aqs=chrome..69i57j0l3.721j0j7&sourceid=chrome&ie=UTF-8.

meetings to cheat the shareholders of the company and make the company suffer economic loss.

6.2.2. TAMPERING OF INFORMATION

Another impact can be loss or repudiation of information. It is difficult to ensure that the data in the transit will not be tampered by the attackers. Though using hash value, one can identify any kind of change in the content of the document, but the same cannot be thought as an evitable act. The contents of the electronic records become prone to repudiation. Also, any misuse of the digital signature might result in the original data being deleted or even lost. The manipulations made on a hand written signature or even the contents of it, can be detectable and visible. But manipulations in the signature and the contents in the digital medium are not identifiable barely at the first instance and are subject to investigation and known in case the same is under doubt. Tampering of the information and being able to detect merely looking at the document is not possible in the electronic medium.[119] Also, once a digital signature gets stolen, or if attacker has made an unauthorized use of the digital signature, a lot of data can be accessed and lot of modifications, alterations, inclusions etc. could be made to the original documents of the owner of the digital signature.

6.2.3. BREACH OF CONFIDENTIAL COMMUNICATIONS

As repeatedly discussed the importance of data for an organization, the same is equally important for an individual or client, as the case may be. People would share information with organization that can guarantee secure and reliable capabilities. In case an organization's data is lost or the digital signature is compromised, a lot security, privacy, and reliability concerns might crop up. Clients and shareholders might start losing faith in the internal working of the organization or may also lose trust in the technical base of the organization. Security breach incidents would be more expected and clients and even business partners and shareholders start withdrawing. One small act loss or unauthorised access to the digital signature can result into the company becoming infamous and the stakes going down since the organization might leave its name in the business and its market.

[119] Rahim Kaba, *Understanding Digital Signatures : Part II*, EsignLive, (Mar. 03, 2017, 11:50AM), https://www.esignlive.com/blog/understanding-digital-signatures-part-ii/.

6.2.4. STEALING SENSITIVE INFORMATION

All the sensitive information including the credit card details, personal information such as name, date of birth, residential address all of these can be stolen by the cybercriminals through phishing. The cybercriminals can make a fake website and after obtaining a fraudulent digital signature, the criminals can launch this website on the internet. Any user who visits the fake website might enter their login credentials. They might also be tricked to enter their credit card details. All the details entered by the user on the website directly go into the hands of the cyber criminals. The cybercriminals can easily commit the crime of identity theft and also steal money from the account of the users once they have obtained their credit card details from the fake website.

6.3. CASE STUDIES

6.3.1. DDPL & UNIFORM INFRA PROJECT CASE

The incident took place on 9th March 2015, when it came to the notice of auditors while auditing the accounts of the company DDPL Global Infrastructure Pvt Ltd that the directors name were changed on the website of government[120]. This was found while reviewing the profiles of the company's directors on the portal of Ministry of Corporate affairs. DDPL is a 9 year old company that is into the business of land development. Supposedly the hackers would have hacked the government website made the changes to perpetrate the crime of corporate hijacking.

The entire profile and names of the original three directors of the company were replaced with the names of unknown persons as fake directors who appeared to be from Pune, Delhi and Madhya Pradesh. Police found out that the name and addresses of these fraudsters imposing as directors did not match. The hackers had also made the same changes to the names of directors of the DDPL associate company i.e. Unicorn Infra projects.

The digital signature of Sunil Sarda who is director of DDPL was fraudulently obtained by the hackers. The fraudsters also used the MTNL Bill and fake pan card along with the digital signature. With the help of these the hackers were able to secure

[120] V kumara swamy, *The mystery of forged signatures* , The telegraph, (Mar. 03, 2017, 8:10 PM), https://www.telegraphindia.com/1150524/jsp/7days/story_21744.jsp.

access to the MCA portal and were successful in modifying the profile details of the directors on the company page. The criminals even got successful in obtaining the Director Identification Number for themselves by using the forged digital signature of Sunil Sarda. The present case clearly reflected the approach adopted by the criminals in corporate hijacking.

The company DDPL was developing a Land project worth of Crores, it is presumed that the hackers had this project as their financial interest behind the commission of this crime. Possibly the hackers were portraying themselves as directors of the company and had the intention to cheat the unaware parties by negotiating a deal with them for the land project. Later on 19th March, 2015 the authorised share capital of the DDPL Company was illegally, without authorization raised to Rs 45 crore. The initial share capital of the company was Rs 5 crore. The aim of the hackers behind this unauthorised raise in share capital was to take all these increased shares. This would have resulted in depriving the directors of the share capital which they owned in the company.

6.3.2. MMPL CASE

Maneklal Mansukhbhai Pvt Ltd. is a ninety two year old company. MMPL is also a Mumbai based company which suffered the same fate as that of company DDPL. In this case the names of two directors of MMPL were replaced with names of five other unknown people from the company's page on the Ministry of Corporate Affairs portal.[121] Not only director's name was changed but also the registered office address of the company was also changed by the hackers in this case. The defrauder had also uploaded many forged documents on the company's page. Both the directors whose names got replaced were unaware about this incident of corporate hijack that took place online on the companies' webpage.

During the investigation of the case it was revealed that the defrauders had illicitly acquired the DSC i.e. Digital Signature Certificate of one of the former deceased director of the MMPL Company. The director whose credentials and digital signature were used to access the website had passed away in year 2010, which were further used by the defrauders to change the details of the company online on the website.

[121] *Id.* at 62.

Mumbai Police was unable to trace any of the hackers behind this cybercrime and make any arrest in this case.

The defrauder's after illicitly securing access to the digital signature of directors can perpetrate the crime of corporate hijack on a company and further cause illicit transfer of shares and also cause the reconstitution of all the board of directors of the company. This sort of white collar crime can be committed only by professional criminals or network of literate criminals who exploit the loopholes in law and corporate entity. The High court of Bombay has stated in its order in the MMPL case that "In today's time be it in any sector not even a single corporate entity is safe from these raiders". The court has described this case as the "*Tip of the iceberg*"[122]. The court has further advised the Ministries of Information Technology and Corporate Affairs to take steps for ensuring stronger digital security measures against these corporate hijack crimes.

6.3.3. STUXNET ATTACK

Stuxnet was the first Cyber Weapon developed as nation sponsored project by the US government to attack on the critical infrastructures of the enemy state.[123] Stuxnet was the most unprecedented and a malicious code developed by the countries Israel and United states under the joint project code named "Olympic games" as part of a classified program. The worm was designed to uncovered, select targeted systems only and destroy the uranium centrifuges of Iranian Nuclear Plant. Stuxnet was a 500 kilobyte computer worm that infected at least 15 of the Iranian industries which includes Natanz facility that is a major centrifuge of uranium in Iran. Natanz facility computer systems were infected with the malware via USB drive by the spies and unaware employees.[124] The worm was signed with the digital certificate of Realtek and Jmicron to make the drivers appear legitimate, which helped the malicious code to infect the target systems and remain undetected.

[122] *Id.* at 65.
[123] Pierluigi Paganini, *Stuxnet & Duqu, update on cyber weapons usage*, Wordpress, (Mar. 04, 2017, 11:10 AM), http://securityaffairs.co/wordpress/4544/hacking/stuxnet-duqu-update-on-cyber-weapons-usage.html.
[124] Mathew J. Schwartz, *Stuxnet Launched By United States And Israel*, SecurityAffairs, (Mar. 04, 2017, 01:20 PM), http://www.networkcomputing.com/government/stuxnet-launched-united-states-and-israel/1195063318.

Malware Stuxnet developed by the experts of both the countries, attacked in three phases: First, The malware was digitally signed with the certificate of Realtek (manufacturer of hardware). This digitally signed malicious code targeted systems that had Microsoft windows. Once the system was infected the malware kept on cloning itself repeatedly. Second, the malware further looked out for windows based software, Simen Step7 which is used to program industrial control systems. The control systems are used to operate the physical equipment's in the industry. Third, the malware provided unauthorised access and control of logic controllers of the industrial plant.[125] Stuxnet could spread to systems running on Windows through USB drives even if the systems were not connected to the internet. The purpose of the attack was to spy on the industrial systems and impair the centrifuges in the nuclear-enrichment plants. The malware attack in a surgical mode delayed Iran's nuclear enrichment by 2 years.

In 2010 an error in the code led the widespread of the worm outside of the Natanz facility to the computer systems in the outside world which led to the detection of the presence of the Malware in other computer systems. The International atomic energy agency along with the inspectors visited the Natanz facility, where they found high rate of failure of centrifuges in enriching the uranium gas.[126] The Iranian's requested Belarusian computer experts to investigate into the matter, who detected the presence of digitally signed malware in their systems. The experts by performing reverse engineering on the code found that the malware was designed to gain system level control and was nation sponsored with support of millions of dollars for the coding the malware. The malware was attacking the targeted systems and as a result it altered the functioning of the valves in the centrifuge which would increase the pressure inside them eventually impairing the equipment and hampering the enrichment process.

6.3.4. COMMODO ATTACK

Trusted partner of Commodo in Southern Europe was attacked by hackers on March 15, 2011. The affiliated Registration Authority of Commodo got compromised

[125] Dan Goodin, *Stuxnet spawn infected Kaspersky using stolen Foxconn digital certificates*, (Mar. 04, 2017, 10:10 AM), https://arstechnica.com/security/2015/06/stuxnet-spawn-infected-kaspersky-using-stolen-foxconn-digital-certificates/.

[126] Kim zetter, *An unprecedented look at Stuxnet, the world's first digital weapon*, (Mar. 04, 2017, 10:20 AM), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

leading to issuance of 9 unauthorised SSL Certificates for 7 major domain names. The hackers were successful in obtaining the login credentials of the Registration Authority and by making unauthorised use this stolen user id and password the hacker managed to fraudulently obtain 9 SSL Certificates for predominant domain name such as Skype, Yahoo, google and addons for mozilla.[127]All these major domain names were the targeted by the attacker with the motive of stealing the login credentials and personal information of the users of these sites by fooling them with the fake websites.

The account of the Registering Authority was still being used by the hacker when the intrusion into the account and fraudulent issue of certificate was detected by the Commodo officials. Within few hours of the attack all the fraudulently issued SSL certificates were revoked by the authorities. All the Domain owners and web browsers who were to be affected by this attack were informed about the compromise and unauthorised issuance of the certificates. The web browsers were told to enable certificate check and not to accept the SSL certificates which were issued fraudulently by the attackers. Investigation conducted by the officials disclosed that the IP address involved in attack which was used by the hackers belonged to Internet Service Providers of Iran. Commodo officials were claiming this attack to be state-funded or politically motivated.[128] They believe such kind of attacks to be an attempt by the government of other countries for surveillance of users of internet by obtaining there login credentials and intercepting there communications over the internet.[129]

Few weeks later a person from Iran took the responsibility for the attack on the affiliated Registration Authority of the Commodo. The hacker represented himself as "*Commodo Hacker*" a cryptography expert in an online post, claiming to be the man behind the compromise of the Registration Authority and misappropriating SSL certificates which belonged to big domain names.[130]Further the hacker also stated in

[127] Phillip, March, Commodo SSL affiliate the recent RA compromise, (Mar. 04, 2017, 11:11 AM), https://blog.comodo.com/other/the-recent-ra-compromise/.
[128] Brain Prince, *Commodo attack sparks SSL Certificate security discussions*, (Mar. 04, 2017, 11:20 AM), http://www.crn.com/news/security/229400284/comodo-attack-sparks-ssl-certificate-security-discussions.htm.
[129] Elinor Mills, *Comodo web attack broader than initially thought*, (Mar. 04, 2017, 12:10 AM), https://www.cnet.com/news/comodo-web-attack-broader-than-initially-thought/.
[130] Gregg Keizer, *Solo Iranian hacker takes credit for Commodo attack*, (Mar. 04, 2017, 12:20 AM), http://www.computerworld.com/article/2507258/security0/solo-iranian-hacker-takes-credit-for-comodo-certificate-attack.html.

his post that he had installed key logger on the servers of Registration Authorities to monitor the administrators. In light of the Commodo attack on the Registration Authority huge concerns regarding security through SSL Certificate have surfaced. It is clear that SSL does not provide any authentication of the user; it only provides the encryption of the communications over the transport layer. By stealing the digital certificates or obtaining unauthorised digital certificates the fraudster can channelize the traffic of users to this fake the website and not only intercept their communication but also steal their personal information. In order to deal with such kind of attacks the Registration Authorities should improve authentication of all their accounts along with IP address restrictions.

6.3.5. DIGINOTAR ATTACK

DigiNotar is a Dutch Certificate Authority which issues digital certificates. On July 2011, it came to the notice of the officials of DigiNotar that there has been a security breach at the Certificate Authority and the hacker had issued unauthorised Digital certificates for predominant domain names like Microsoft, Yahoo and Google. In this attack the hacker had compromised the security of the Certificate authority and issued a total of 531 rogue digital certificates.[131]

The purpose of digital certificate is to authenticate a legitimate website hence it verifies the genuineness of a website visited by a user on the web browser. The digital certificate holds encrypted data which is used to verify and allowing access to legitimate website on the web browser and allow access to legitimate website. The web browser will show security error while accessing an illegitimate domain name on the web browser for which digital certificate is not issued. The verification process through digital certificates helps in preventing attacks of cyber criminals who attempt committing identity theft and steal sensitive information through illegitimate websites having fake domain names. Hence by obtaining an unauthorised digital certificate or using a fake digital certificate a fraudster can intercept communications of the users, install malwares on their systems and also steal their personal information by creating and launching a fake website such as facebook and yahoo etc. which would identically resemble to the original website.

[131] Robert Lemos, *Fake certificates reveal flaws in the internet security*, MIT Technology Review, (Mar. 04, 2017, 01:20 AM), https://www.technologyreview.com/s/425461/fake-certificates-reveal-flaws-in-the-internets-security/

All the certificate servers at DigiNotar were being controlled alone by a single account and also the password assigned to the account was too weak. This weakness was exploited by the hackers to give effect to the security breach at DigiNotar. Not only the users but the Dutch government also heavily relied upon the Digital certificates which were issued by the DigiNotar CA. In the investigation it was revealed that one of the rogue digital certificates issued for google domain encountered to at least 3000 IP addresses. After this security breach DigiNotar had filed for bankruptcy.[132] Dutch government had taken control over this Certificate authority's operation as the digital certificates issued were being used by the government for encrypted communications. In response to this attack majority of the browsers have uncredited the digital certificates issued by DigiNotar.

6.3.6. ATTACK ON NIC CERTIFICATE AUTHORITY

On June, 2014 it was detected that a security breach had occurred at the Certificate Authority which was under the control of Indian government. NIC i.e. National Informatics Centre CA which is a branch of branch of Ministry of communications and Information technology was attacked by hackers. In this attack several unauthorised digital certificates had been issued from the digital certificate authority which predominantly targeted the big domain names such as Google and Yahoo.[133] National Informatics Centre CA is subordinate to Indian controller of Certificate Authority. The certificates issued by NIC CA are predominantly trusted by most of the program running on windows and are also stored on the Microsoft root store which is a logical container on the operating system that stores the trusted certificates. These stored certificates are utilised for accessing domain names on the Internet Explorer and Google Chrome.

When the Certificate Authorities are requested they are only expected to issue the Digital certificates to the genuine Domain name owners and not entertain any other person's request. The Certificate Authorities need to exercise this precaution in order to avoid issuing digital signature certificate to the hackers who will eventually utilise

[132] Lucian Constantin, *Digital certificate breach at Indian authority also targeted Yahoo domains, possibly others*, PCWorld, (Mar. 04, 2017, 02:50 PM), http://www.pcworld.idg.com.au/article/549741/digital_certificate_breach_indian_authority_also_targeted_yahoo_domains_possibly_others/.
[133] *Id.* at 70.

these rogue digital certificates to impersonate original websites in order to perpetrate the crime of identity theft and fraudulently obtain sensitive personal information of victims. The hackers can also use the rogue digital certificates to intercept the encrypted communications of the end-users connected to the website.

On investigation the security breach at NIC it was identified by the Indian CCA that four rogue digital certificates had been issued without the authorisation by NIC. It was still suspected that more than four unauthorised digital certificates had been issued by NIC in this breach. Out of these four rogue digital certificates one digital certificate was issued for yahoo domain and rest three certificates were issued for domain name belonging to Google. In response to this breach Indian CCA has revoked all the digital certificates signed by NIC CA. This step of revocation taken against certificates signed by NIC has also affected the SSL Certificates signed by it. Further it had been displayed by NIC on its website that it will not be issuing digital certificate for a period due to some security reasons. Public key pinning feature of Google Chrome had been used to avert the rogue digital certificates issued by NIC CA. This feature of Google Chrome accepts only few of the Digital certificates which are predefined for few Domain names.

6.3.7. RANSOMWARE ATTACK ON APPLE

First of the Cyberattack on Apple systems using a ransomware was detected in 2016. "KeRanger" is the name of the ransomware which was launched to infect the apple systems that were running windows. The malicious software was spreading through torrent software on the apple systems. BitTorrent which is a client of Apple Operating System was infected by the ransomware "KeRanger". BitTorrent is installed by the Apple operating system users for accessing the shared file in Torrent swarms.[134]

The cybercriminals managed to upload the infected version of transmission on the website of BitTorrent. The ransomware "KeRanger" was enveloped inside the transmission. The original transmission files on the website of BitTorrent were replaced with the infected versions of the transmission files. The infected versions of the transmission files were digitally signed with the certificates of legitimate Apple

[134] Claire Reilly, *Apple users beware: first live ransomware targeting Macs found 'in the wild'*, CNet, (Mar. 05, 2017, 08:37 PM), https://www.cnet.com/news/apple-users-beware-first-live-ransomware-targeting-mac-found-in-the-wild/.

developers to bypass gatekeeper protection provided by Apple. The security settings of the Mac systems is such that it allows all download from the apple developers who are already identified.

Once the transmission i.e. BitTorrent which was infected with the ransomware was installed on the system by the apple user, the ransomware infects the system. For two days there will be no problem but on the third day the ransomware connects to command servers on anonymous network. The malicious software starts locking up all the functionality and the files on the system of the users by encrypting them. After the ransomware has finished encrypting the essential files and functionality on the drive it starts demanding from the victim an amount of 1 bitcoin i.e. $400 as ransom if they want to decrypt and retrieve the files.[135]The ransomware was also suspected to prevent the users from retrieving their backup data on the system.

Antivirus programs fail to defend systems against such ransomwares as these malicious software's tend to fool them. Apple in action against this attack has revoked the digital certificates which had been exploited by the ransomware. BitTorrent has removed from its website the infected versions of the transmission. Further the website also has a notice for users informing them to upgrade their software's to latest version 2.92 as measure to protect the systems from the ransomware.

[135] Jeremy kirk, *Apple shutdowns first-ever ransom attack against Mac users*, PCWorld, (Mar. 05, 2017, 10:50 PM), http://www.pcworld.com/article/3040987/security/apple-shuts-down-first-ever-ransomware-attack-against-mac-users.html.

CHAPTER – 7

7. COMPARITIVE ANALYSIS OF INDIAN AND FOREIGN LAWS

7.1. Digital Signature Laws of United States

Since US has been a technologically advanced country with the major of the developments in the field of computer science and related technologies. US has been developing technologies and at the same time been diligent about its misuse and grave consequences. In my opinion, I believe, United States have been proactive in taking decisions and maintaining the technical and legal frameworks in the country. The country has been taking of uniform nature of transactions and electronic ad digital signatures from late 1990s while India was still struggling to get access to the cyber space. In the field of digital and electronic signatures, a lot of research and amendments have been done by US law enforcement agencies.

In 1995, Utah was the first country, where the American legal stem branched out in roots into the electronic signatures and related laws. In years, most of the countries have taken progressive steps to introduce electronic signature law. Since early laws were domain or industry specific, more and more laws were enforced in the countries to make it applicable to all the spheres of the life today. This is the specific reason for multiple legislations on the same subject matter in most of the American countries today. Due to time difference in enforcing different laws and also jurisdictional challenges, there had been challenges faced by many of the legislations and their enforceability. To overcome the same, **Uniform Electronic Transaction Act**[136] was introduced. The act gave legal recognition to electronic signatures and also laid emphasis on legality of the contracts if affixed with an electronic signature. The act also enlisted what all constitutes electronic signatures. The act has given a wide interpretation to electronic signatures and has acknowledged even an electronic sound

[136] Uniform Electronic Transaction Act (1999).

or a symbol as an electronic signature to an extent used to sign the record[137].the provision lays an emphasis that no contract or signature should be denied an effect of legal recognition merely on the basis of the formation of the contract or the medium in which it was affixed respectively[138]. The section reads as follows:

"(*a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.*

(b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

(c) If a law requires a record to be in writing, an electronic record satisfies the law.

(d) If a law requires a signature, an electronic signature satisfies the law."

The another progressive step taken by federal government was introduction of Electronic Signatures and Global and National Commerce Act (**E-sign Act[139]**)to strengthen the electronic signature laws in the country. It was the act which gave legal recognition to e-contracts, records and signatures throughout the United States. Both the Acts have been overlapping and been correspondence to each other so that in countries where the federal laws are not applicable, state laws are sufficient and where the federal law applies, the E-sign Act makes it a mandate. The positives of the act include legal recognition to documents requiring traditional signatures yet signed with digital signature, recognition of such records as evidence and correspond to all the Acts demanding need of a traditional signature. Section 101(b)(1) of the Act preserves right of the individual who do not wish to transact by the use of electronic signature, rather prefer physical signatures. It is an interesting piece of legislation that not only allows use of traditional signatures but also legally recognizes electronic signature under one single Act. The provision reads as follows:

"*(b) Preservation of Rights and Obligations.--This title does not--*

(1) limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons under

[137] Entrust, *Digital Signatures –The Silver Bullet for E-Signature Laws*, Entrust, (Mar. 06, 2017, 10:15 PM), https://www.entrust.com/wp-content/uploads/2013/05/digsig_legislation.pdf
[138] Section 7, Uniform Electronic Transaction Act, (1999).
[139] *Id.* at 73.

such statute, regulation, or rule of law other than a requirement that contracts or other records be written, signed, or in non-electronic form[140]."

It is rightly noted that the party autonomy has been granted for the purpose of recognizing the signatures in the electronic medium. The parties to the contract or transaction have to agree to the use of electronic signatures for the purpose of the fulfilment of any of the requirements of a valid contract or a valid and enforceable communication.

7.2. Digital Signature Laws of United Kingdom

United Kingdom has been a part of the European Union and the directives and regulation of the Union applies well to it. The UK directives define electronic signatures as signatures which are capable of not only identifying the signatory but also is unique to him under his sole control and supervision and is so affixed that any change in the subject matter can be identified[141]. The eIDAS of the EU has been implemented under the UK laws as well but into two different laws governing the same. Initially, before the said EU regulation, the government of UK had taken a step for an improvised business market in the UK itself and recognize electronic communication. The Electronic Communication Act and Electronic Signature Regulation were introduced in 2000 and 2002 respectively. These laws were upgraded by the eIDAS and hence the fame was incorporated under two different provisions of Section 7 of the Electronic Communication Act 2000 and Electronic Identification and Trust Service for Electronic Transactions Regulations 2016. The purpose of the Electronic Communication is to enable an independent and neutral law for the purpose of electronic business practices and methods and also for neutral data storage capabilities[142]. The act aims at building trust of the people in the public key cryptography and to remove any barriers in the business and electronic transactions due to electronic signature or any other signature requirements. The purpose has been fulfilled by the Act by giving electronic signatures a legal status equal to that given to a traditional physical signature[143]. The act legally recognizes the legality of e-contracts, electronic signatures and also admissibility of the same as an evidence in the court of law.

[140] Electronic Signatures in Global and National Commerce Act (2000).
[141] Article 26, EU Regulation (2000)
[142] *Id.* at 74.
[143] *Id.* at 75.

Section 7 of the act reads as:

> "*(1) In any legal proceedings—*
> *(a)an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and*
> *(b)the certification by any person of such a signature,*
> *shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data*[144]."

There has also been recognition of electronic seal under the EU legislation and is available to corporates and other legal persons recognized under the law and not to everyone else[145]. The same provision has been incorporated under the UK laws. Most of the regulations under EU have been ratified by the UK government under the Electronic Communication Act by the virtue of section 7.

7.3. Digital Signature Laws of European Union

The European Union is said to be a proactive Union in taking up decisions and making laws for all of its state members. In 2016, the union took a very bold decision for its member in terms with electronic signatures. The directives differentiate between electronic as well as advance electronic signatures. The regulation through its Electronic Identification and Authentication Service Regulation known as eIDAS, directives through legal recognition to electronic signatures, identification and even records. The aim of such a directive was to have a uniform law. It is believed, uniformity in the legal systems can allow better business decisions and discussions. Keeping this in mind, EU brought a law granting legal recognition to electronic signatures and makes any state law which are not in accordance with the said directives, inconsistent[146]. The same act also made the signatures and related activities as admissible piece of evidence to the case. Website authentication certificates and time stamp stamps also were included in electronic signatures. The country recognizes digital signatures as an advanced level of electronic signatures which verify the

[144]Section 7, Electronic communication Act (2000). available at http://www.legislation.gov.uk/ukpga/2000/7
[145] *Id.* at 75.
[146] *Id.* at 75.

integrity of agreement and is in furtherance of a Digital Signature Certificate[147]. The Law is similar to that of Indian. The certificate of an authority can issue certificate that shall be legally valid only if such authority comes under the control and supervision of authorities appointed by EU member states. It gives equal recognition to certificates from non-member Certifying Authorities or to say, from Foreign Certifying Authorities. The EU directives have made it neutral for the certification issued from any of the member state to be equally recognized. Henceforth, there can be a restriction free circulation within the entire European Union of electronic signature[148].

7.4. Legal Issues in the Laws governing Digital Signature in India

Indian has been progressive in Information technology and related laws; but the same has been lacking the present demand of the standards across the world. Though the legislation on Digital signature had been adopted in India in the year 2008 but it is still in its very nascent stage. The law on the subject matter has not been fully developed to address the current issues and challenges of digital signatures. The grey areas of the same have not been touched through the IT Act 2008.[149] The law has failed to recognize crimes using digital signature and have not covered the same under offense chapter. The act also fails to cover all the aspects of digital signature. There is no proper regulation to curb the misuse of the said signature or to punish for any breach or fraudulent or unauthorized use. There are various other issues with the law in the country.

There is a need for making the certificate authority more responsible for not issuing fraudulent digital certificates. They must act diligently and must verify the identity of the individual properly before issuing the digital signature certificates in order to avoid such challenges. There is absence of any regulatory mechanism of the Certifying authorities. No strict punishment provisions are mentioned in the act for crimes related to digital signature such as corporate hijacking, cyberwarfare and other new emerging crimes which are accomplished by using digital signature.

[147] Admin, *Global Guide To Electronic Signtature Law: Country Laws*, Adobe, (Mar. 01, 2017, 11:30 PM), https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/document-cloud-global-guide-electronic-signature-law-ue.pdf
[148] *Id.* at 77.
[149] Section 24, The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000(India).

Revocation of the digital signature is not timely updated in the list of revoked digitals certificates. The criminals take advantage of this and still use these revoked digital certificates. Immediate actions are not taken against fraudulent digital certificates issued from the office of Certifying authorities. The certifying authorities must be made responsible for notifying the concerned authorities and stakeholders about the fraudulent issues of digital certificates so that preventive measures can be taken against them. Yet no major court cases related to digital signature crimes and the legality of digital signatures have been addressed by the Indian judiciary. The financial accountability in cases of fault on the part of the certifying authorities has not been clearly defined in the act. The certifying authorities need to be held more accountable for their acts. The law provides for no remedies of crimes related to digital signatures and the same has been talking a new turn in emerging crimes. It is very important to introduce the provisions related to such crimes and their remedy before they number increases and justice is denied.

As a technology, the Digital signature is very promising in the field of security to the communications and electronic document. But the application of digital signature is still limited to only the financial transactions, electronic contracts, domain websites, banking sector and online stock market. The Information Technology Act, 2008 is inefficient in promoting the correct use pf digital signatures in other sectors also.

CONCLUSION

The paper revolved around the theme of digital signature, the need to use the same, how integrity and non-repudiation can be assured using the same. The paper brought out and highlighted the significant role of the digital signature in the authentication of digital communications and day to day online business transactions. We have also tried to understand the core mechanism, technical requirements, encryptions and algorithms involved in the implementation of the digital signature to analyse the level of security that is provided by the digital signature to any document. The dissertation called out the major advantages and disadvantages of using digital signatures. There are some unknown crimes that can take place using the digital signature. To bring those crimes in the lime light was the purpose of the dissertation, since they have not been discussed in the list of the cybercrimes commonly known and are limited to case studies. Major concerns have been identified regarding the misuse of digital signatures and various other crimes perpetrated by using fraudulent digital signature to commit identity theft, economic fraud and cyberwarfare. Various case studies in reference to attacks on the digital certificate authorities have been discussed which highlight the need for implementation of strong security measures by the Certificate authorities to prevent the increasing number of security breach and fraudulent issue of digital signatures. Analysis of the digital signature laws across the world was the prime focus.

Digital signature laws have been taking progressive steps in the world today. Countries across the globe are recognizing legality of the electronic records, digital signatures, and their admissibility as evidence in the court of law. The evolution of digital signature and laws related to it has been traced out throughout the history. The paper discusses the guidelines on electronic and digital signature developed by the International Organisations namely UNICITRAL and ABA. These guidelines play a very important role in shaping the domestic legislation on the digital signature of the member countries. Majority of the members have implemented these provisions into their domestic law. The countries have made attempts to give functional equivalence to digital signatures like that of a traditional signature. Also, countries such as United States have also granted party autonomy in deciding whether or not the parties want to settle communications in electronic signature or would prefer to pursue traditional signature, thus preserving their right. The country recognized any sound also to be

included in the definition of electronic record. European Union has recognized free circulation of digital signature within the Union. Similar to India, the European Union has recognized two types of signatures, though differ in names. The said signatures in EU are known as electronic signatures and advanced electronic signatures, whereas in India they are known as electronic signature and digital signature. Digital signatures include wide range of website authentication certificates and time stamps in electronic signatures. United Kingdom also undertook EU obligations to legally recognize electronic signatures and even electronic seals, though latter one only for legal persons. The motive behind such acceptance of obligations is to ensure hustle free trade and business in the country and to maintain people's trust therein.

Though the Indian laws have met the basic standards that are maintained by other developed countries, yet the laws are not very strong. In case where the laws exist, there is minimal or no enforcement of the same. A stricter mechanism for regulation of certifying authorities is required. Most of the countries have introduced multiple laws on the subject matter whereas in India, the entire information technology is limited to one single act. It is very important that the certifying authorities are streamlined before these crimes become known and often. Stricter liabilities should be imposed on authorities in case they are found guilty for any kind of negligence. India is a big IT hub; it is important for the government to maintain the standards and ensure its application and regulation. To have better influx of business and foreign investments, it is necessary that the government wins trust in the global market by providing strict, secure and reliable platform for nations to come for business in India.

RECOMMENDATION

The Dissertation has highlighted various digital signature related crimes that are not only unknown to the organisations but has also marked its absence in the Indian Information Technology Act. The Act does not recognise the above stated crimes and also the judgements on the same are silent. The Digital signature crimes can be covered under the existing law as an "unauthorised use or access" but a concrete or comprehensive legislation is the requirement of the hour. To bring out an argument one may suggest that the existing laws are adequate but the same can't be said to be true. A counter argument would be that if old legislation is adequate for new upcoming crimes then Indian penal code would have been equally adequate for crimes in cyberspace. On the basis of the said argument it is recommended to formulate and enforce a special law dedicated to digital signature. If the same cannot be done in the present scenario, it is highly recommended to understand the potential crimes and huge harm that can be caused because of misuse of digital signature and the same shall be incorporated under the IT Act by an amendment. Since the dependency on the Information technology is increasing the value of data, the electronic communications have also increased. It is thus very vital for India to secure cyberspace and to gain trust of other nations by promoting safe, viable, sound electronic communication and electronic transactions. A detailed analysis of the possible threats related to digital signature and related crimes need to be done and laws for the same should be laid down. It is also recommended that survey should be conducted for the purpose to know whether or not the crimes brought out in this dissertation are already known to the organisations. On the basis of the survey report awareness on the same should be spread. The law should mandate on the organisation and government departments to ensure that on the digital signature should be protected but also mandatory disclosure in case of breach. Also the organisations and government departments using digital signature should have proper mechanism to prevent, detect and recover from such breach and digital signature crimes. The NIC should be entrusted with an additional function of providing aid to such organisations and government department in case of digital signature breach.

BIBLIOGRAPHY

WEB SOURCES

- https://legalesign.com/blog/history-of-signatures/.
- https://www.esign.com/blog/bid/108804/A-Brief-History-of-Signature.
- http://www.uth.tmc.edu/med/students-current/SCAIP/signature-value.html.
- https://www.signix.com/blog/bid/108804/Infographic-The-History-of-Digital-Signature-Technology.
- http://www.certificatetiger.com/News/law-of-digital-signature.html.
- https://www.signix.com/blog/bid/92791/The-Difference-Between-Digital-Signatures-and-Electronic-Signatures.
- http://computer.howstuffworks.com/encryption5.htm.
- http://lerablog.org/technology/datasecurity/advantagesanddisadvantagesofdigitalsignatures/.
- http://digitalindiainsight.com/advantagesanddisadvantagesofdigitalsignature/,
- http://supercustomessay.com/essayadvantagesanddisadvantagesofdigitalsignatures/.
- http://www.pcworld.idg.com.au/article/549741/digital_certificate_breach_indian_authority_also_targeted_yahoo_domains_possibly_others/.
- https://www.cnet.com/news/apple-users-beware-first-live-ransomware-targeting-mac-found-in-the-wild/.
- http://www.computerworld.com/article/2507258/security0/solo-iranian-hacker-takes-credit-for-comodo-certificate-attack.html.
- https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/,
- https://arstechnica.com/security/2015/06/stuxnet-spawn-infected-kaspersky-using-stolen-foxconn-digital-certificates/.
- http://securityaffairs.co/wordpress/4544/hacking/stuxnet-duqu-update-on-cyber-weapons-usage.html.
- https://www.esignlive.com/blog/understanding-digital-signatures-part-ii/.
- https://www.google.co.in/search?q=Corporate+Hijacking!&oq=Corporate+Hijacking!&aqs=chrome..69i57j0l3.721j0j7&sourceid=chrome&ie=UTF-8.

BOOKS

- Karnika Seth, Computers, Internet and New Technology Laws, 1st Edition, Lexis Nexis, 2013.
- Stephen Mason, Electronic signature in Law, 3rd Edition, Cambridge University Press, 2012.
- Ashish Srivastava, Legal Understanding and Issues with Digital Signature, 1st Edition, Springer India, 2013.
- S.K. Bansal, Cyber Millennium Challenges and Opportunities, APH Publishing, 2001.
- Rohus Nagpal, Cyber Crimes & Digital Evidence – Indian Perspective, Asian School of Cyberlaws, 2008.

ONLINE JOURNALS/ARTICLES

- Vijaykumar Chaube, "***Digital Signature: Nature & Scope under IT Act, 2000***," SSRN Electronic Journal, (September, 2010).
- V. Kumar Swamy, "***The mystery of forged signatures"***, The Telegraph, (May, 2015).
- David Fillingham, "***A Comparison of Digital and Handwritten Signature"***, Ethics and Law on the Electronic Frontier, (1997).
- R Jason Richards, "***The Utah Digital Signature Act as "Model" Legislation: A critical Analysis***", John Marshall Journal of Information Technology & Privacy Law, (1999).
- C. Bradford Biddle, "***Misplaced Priorities The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure***", San Diego Law Review, (1996).
- Yogesh Kolekar, "***Electronic Signature – Legal and technical Aspect"***, LegalServicesIndia, (2016).
- Abhinav, "***The Role Of Digital Signatures In Digital Information Management"***, International Monthly Refereed Journal of Research In Management & Technology, (2013).

- Hongjie Zhu & Daxing Li, "***Research on Digital Signature in Ecommerce***", Vol. I, Proceedings of the International MultiConference of Engineers and Computer Scientists, Hong Kong, (2008).
- Bhagyashree, Arpita, Chandana & Soujanya, "***A Role Of The Digital Signature Technology Using RSA Algorithm"***, IJSR, (2017).
- C. R. Rachana, "***The role of digital signature in Information Management***", Vol. II, International Monthly referred journal of research in Management & Technology, (2013).
- J. Katz and Y. Lindell, "***Introduction to Modern Cryptography***", Chapman & Hall CRC Press, (2007).
- Mao Wenbo, "***Modern Cryptography: Theory & Practice***", Prentice hall of technical reference, New Jersey, (2004).
- Robert Lemos, "***Fake certificates reveal flaws in the internet security"***, MIT Technology Review, (2017).

NEWS ARTICLES

- The International News, (Article updated on November 2, 2015).