ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 10, March 2018

Digital Signature In E-Commerce

Harpreet Kashyap
Student, Department of Commerce, S.S.G.Janta Girls College
Raekot (PB) India

ABSTRACT: With the development of internet, digital signature becomes more and more important for the electronic commerce security because of its data integrity protecting and privacy. This paper is to propose kind a digital signature based on public key. By this way, digital signature and replication of digital products are effectively realized. Finally, a material digital signature is given with Java.

KEYWORDS: Digital Signature, E-Commerce, Data Integrity, Encrypting with public key

I.INTRODUCTION

With the development of network and software technology, applications of internet make great influence on traditional working. At the same time, e-commerce emerged and developed rapidly, playing great role in business activity. With contrast to traditional business pattern, e-commerce has great convenience and high efficiency. Still today, the volume of trade by e-commerce in whole world is little.

The data transferred on e-commerce system must have characteristics of integrity, security and identity authentication. Security restricts the development of e-commerce. Digital signature resolves the problem because of its data integrity protecting and privacy. So digital signature is widely used in e-commerce system.

II. OBJECTIVES OF THE STUDY

- To provide authenticity, integrity and non-repudiation of electronic documents.
- To use the internet as safe and secure medium for e-commerce and e-governance.

III. LITERATURE REVIEW

Review of literature paves way for clear understanding of the areas of research already undertaken and throws a light on the potential areas, which are yet too covered. The reviews of some of the important studies are presented below:

Pointchevala et al [2000] [1] provides some security arguments for digital signature as well as for blind signature. Here anyone can justify realistic parameters even if they are not optimal.

Gerić et al (2012) [2] provides information about XML signatures. XML signatures are type of digital signatures generally helps in XML Transactions. It also defines a particular schema for the storage of XML data's result based on digital signature operations.

Nguyen et al (2011) [3] presented a paper on functionality Extension of the Digital Signature Standards. The protocol used here is based on Belarusian DS standards, which are flexible and provide a possibility of natural extension of their functionality.

Zhang et al (2011) [4] makes an improvement on digital signature algorithm which is based on elliptic curve cryptography. In this paper, he obtained a new

digital signature scheme by improving the original digital signature based on elliptic curve cryptosystem.

Xuan et al (2009) [5] makes a research on the comparison of algorithms used by Digital signature in Mobile Web world. DSA, RSA and ECDSA are some algorithms, which are generally used in comparison in this paper.

Jian-zhi et al (2009) [6] gives a design of Hyper Elliptic Curve Digital Signature in which they described DSA and HEC algorithms to combine them and to generate DSA-HEC digital signature system. Which provide a high security to check the uniqueness of data.

IV. RESEARCH METHODOLOGY

The study is based on secondary sources of data/information. Different books, journals, newspaper and relevant websites have been consulted in order to make the study effective.

1. WHAT IS DIGITAL SIGNATURE?

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 10, March 2018

Digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signature is a type of asymmetric cryptography used to simulate the security properties of a signature in digital form, rather than written form. The output of signature process is called Digital signature.

2. HOW DIGITAL SIGNATURE WORKS?

- The use of digital signature usually involves two processes, one performed by the signer and the other by the receiver of the digital signature.

- Digital signature creation uses a hash result derived from both the signed message and a given private key. For the hash result to be secure, there must be only a negligible possibility that the same digital signature could be created by the combination of any other message or private key.

- Digital signature verification is the process of checking the digital signature by reference to the original message and a given public key.

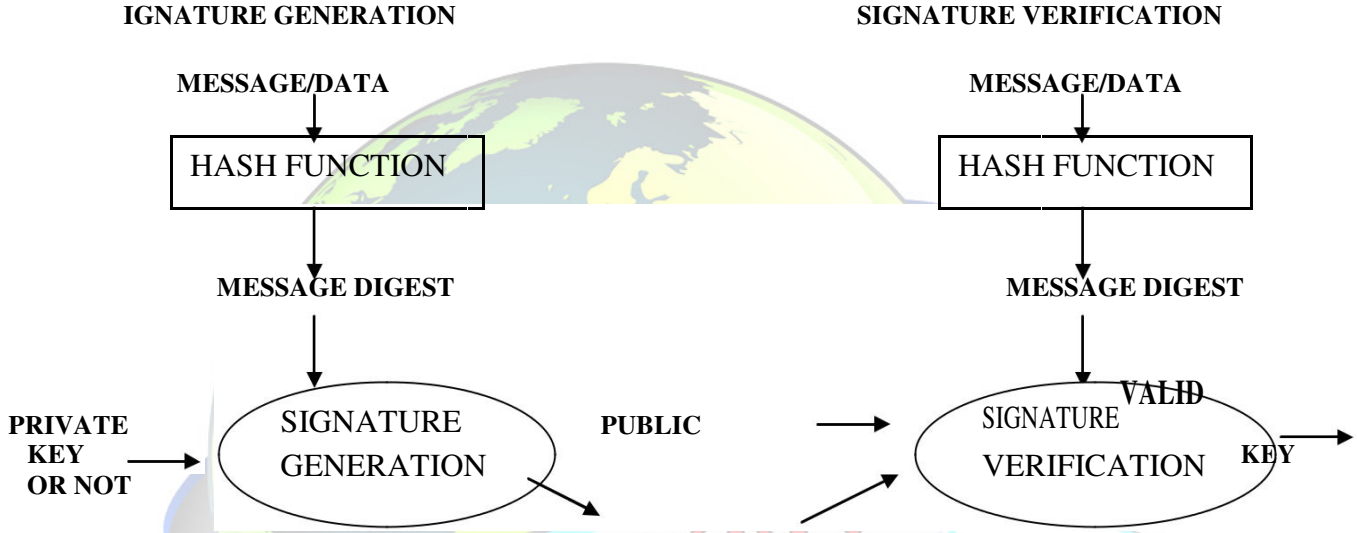

Fig.1 process of digital signature

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 10, March 2018

3. BASIC REQUERIMENTS

3.1 Private key: the private key is the one which is accessible only to the signer. It is used to generate the digital signature, which is then attached to the message.

3.2 Public key: the public key is made available to all those who receive the signed messages from sender. It is used for verification of the received message.

3.3 Digital signature certificate: A digital signature certificate contains information about the user's name, pin code, country, and email address, date of issuance certificate and name of the certifying authority.

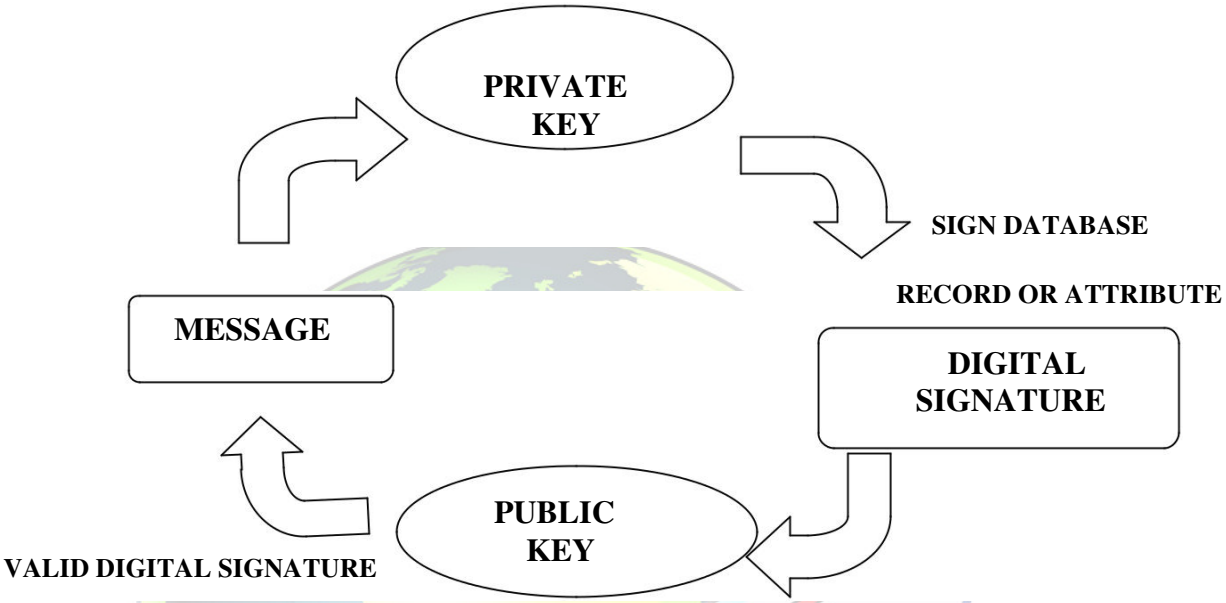

Fig.2 basic requirements of digital signature

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 10, March 2018

4. FEATURES OF DIGITAL SIGNATURE

4.1 Signer Authentication: The digital signature must be capable to identify and link the signer with the electronic record which subscriber of digital signature has created. It is also necessary to ensure that the tampering of documents should not be happened after its creation. The private key belongs to subscriber who signs it and incurs legal responsibility out of it.

4.2 Message authentication: The electronic record transformed by algorithm mapping with hash function by affixing private key of digital signature typically identify the matter to be signed, since verification also reveals any tampering with the message.

3 Verification: The ultimate aim of creation of digitally signed document is capability of its verification at latter moment of its creation. Thus the mechanism must be capable to verify the authenticity and non-repudiation to resolve the disputes between originators and recipient and a third party must be able to verify the signature as independent verifying institution.

5. BENEFITS OF DIGITAL SIGNATURE

5.1 Saves times: Digital signature ensures that businesses save on time and cost with documents and contracts signed off with a click of a button. Documents can be signed off almost instantly , from anywhere.

5.2 Cost savings: Many companies also see significant cost savings, with little or no expense in ink, paper, printing , scanning, delivery or other expenses.

5.3 Improve workflow efficiency: With the lesser delays digital signatures ensure better efficiency in workflow. Managing and tracking documents are made easier with lesser effort and time involved.

5.4 Better customer experience : Digital signature provide the convenience of signing important documents where ever a customer or a person to sign is located. Documents can be signed off at door step.

5.5 Security: When it comes to signatures, authenticity and security is a priority. Digital signatures reduce the risk of duplication or alteration of the document itself. Digital signature ensures that signatures are verified, authentic.

5.6 Legal validity: digital signature provides authenticity and ensures that the signature is verified. This can sand in any court of law like any other signed paper document.

6.LIMITATIONS OF DIGITAL SIGNATURE

6.1Expiry: Digital signatures, like all technological products, are highly dependent on the technology it is based on. In this rapid changing technology, many of these tech products have a short life.

6.2 Certificate: In order to effectively use digital signatures, both senders and recipients may have to buy digital certificates at a cost from trusted certification authorities.

6.3 Law: In some states and countries, laws regarding cyber and technology based issues are weak or even non-existence.

6.4 Software: To work with digital certificates, senders and recipients have to buy verification software at a cost.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 10, March 2018

6.5 Comparability: There are many different digital signature standards and most of them are incompatible with each other and this complicates the sharing of digitally signed documents.

7. WHAT IS E-COMMERCE?

E-Commerce can be defined as a modern business methodology that addresses the needs of organizations, merchants, and consumers to cut costs while improving the quality of goods and services and increasing the speed of service delivery. E-commerce is associated with the buying and selling of information, products and services via computer networks. Key element of e-commerce is information processing. The effects of e-commerce are already appearing in all areas of business, from customer service to new product design.

It facilitates new types of information based business processes for reaching and interacting with customers – online advertising and marketing, online-order taking and on-line customer service etc. It can also reduce costs in managing orders and interacting with a wide range of suppliers and trading partners, areas that typically add significant overhead to the cost of products and services. Also E-commerce enables the formation of new types of information-based products such as interactive games, electronic books, and information-on demand that can be very profitable for content providers and useful for consumer

8. FEATURES OF E-COMMERCE

8.1 Interactivity: Technologies used in eCommerce require consumer interactions in order to make an individual feel as though he is an active participant in the transaction process. As a result, eCommerce technologies can adjust to each individual's experience. For example, while shopping online, an individual is able to view different angles of some items, add products into a virtual shopping cart, checkout by inputting his payment information and then submit the order.

8.2Personalization:Technologies within e-Commerce allow for the personalization and customization of marketing messages groups or individuals receive. Pearson Education states that companies can base such messages on individual characteristics of a consumer. An example of personalization includes product recommendations based on a user's search history on a Web site that allows individuals to create an account.

8.3 Information Richness: Users can access and utilize text messages and visual and audio components to send and receive information. Pearson Education states that such aspects provide a rich informational experience in regards to marketing and the consumer experience. An individual may see information richness on a company's blog if a post contains a video related to a product and hyperlinks that allow him to look at or
rchase the product and send information about the post via text message or email.

8.4 Universal Standards: Individuals, businesses and governments only use one set of technological, media and Internet standards to use eCommerce features. Consequently, universal standards help simplify interactions. An individual can see these standards while shopping online, as the process to purchase items is similar on Web sites that use eCommerce technologies. Similarly, when an individual creates an online account, the site generally requires an individual to create a username and password so he can access his account.

8.5 Ubiquity: Because they are web-based, eCommerce technological features are available anywhere you can connect to the Internet at any time, including homes, offices, video game systems with an Internet connection and mobile phone devices. Because eCommerce is ubiquitous, the market is able to extend its traditional geographic boundaries and operating hours. An example includes the ability to access the Internet wherever there is a Wi-Fi hotspot, such as a cafe or airport. Moreover, individuals who have cell phones with data capabilities can access the Internet without a Wi-Fi connection.

8.6 Information Density : The use of eCommerce reduces the cost to store, process and communicate information, according to Pearson Education. At the same time, accuracy and timeliness increase; thus, making information accurate, inexpensive and plentiful. For example, the online shopping process allows a company to receive personal, shipping, billing and payment information from a customer all at once and sends the customer's information to the appropriate departments in a matter of seconds.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 10, March 2018

8.7 User-Generated Content: Social networks use eCommerce technologies to allow members, the general public, to share content with the worldwide community, according to Kurt Grashaw in an article for the Web site Merchant Circle. Consequently, consumers with accounts can share personal and commercial information to promote a product or service. When a company has a professional social networking account, a member of the same social network has the option of associating himself with the company or a product by saying he likes or recommends it. When an individual updates his status on a social networking account, he may also mention a product or company by name, which creates word-of-mouth advertising.

8.8 Global Reach: Technologies within eCommerce seamlessly stretch across traditional cultural and national boundaries and enable worldwide access. Pearson Education states that instead of just offering goods and services to a population within a specific boundary, businesses can market to and serve an international audience. The Internet and multilingual Web sites, as well as the ability to translate a Web page, allows international visitors all over the globeo access company Web sites, purchase products and make business interactions.

9 . ADVANTAGES OF E-COMMERCE

9.1. Enhances convenience: Customers can make orders for goods at their own convenience and from the comfort of their homes without having to travel to the business premise. Orders are also delivered to them at their most ideal locations. It's the best shopping option for people who are always busy.

9.2. Allows for product and price comparison: Again, when making purchases, customers want to get the best deals. This business model allows for product and price comparison by consumers so that the best products are bought at the fairest prices. They can also enjoy extra benefits like discounts, coupons, items on sale and also get the best deals.

9,3. Easy fund-raising for start-ups ventures: So many people have the desire to venture into business but lack sufficient funds to set up shop. Leasing a physical store can be quite expensive. E-commerce makes it easier for start-ups to do business and grow.

9.4. Efficient: E-commerce has the advantage of being efficient. Resources are used efficiently since most of the business services are automated. Business owners sometimes spend a lot of resources meeting business needs and this eats into profits. E-commerce thrives on efficiency.

9.5. Customer reach: It's easier to reach many customers on the internet. Using social media links and good search engine optimization strategies, an online business can increase brand awareness and grow its customer base. It also has the advantage of being able to connect buyers and sellers from all corners of the globe.

10. DISADVANTAGES OF E-COMMERCE

10.1. Poor quality products: You don't physically see and inspect whatever you are paying for before it's delivered. Customers, therefore, run the risk of falling victim to false marketing and buying poor quality products from the virtual shop.

10.2. Impulsive purchases: Online stores display a large number of products and due to the convenience of shopping, customers can find themselves making bad financial decisions through impulsive purchases.

10.3. Internet scammers: The internet is a good thing but some people have decided to use it for all the wrong reasons. Scammers have made this type of business model unattractive for some consumers.

10.4. Lack of after sales support: As a result of lack of physical premises, customers find it hard to access after sales support. It can take up to several
s before any help is accorded to a customer in need.

10.5. Fast changing business environment: Technology evolves so fast. Some entrepreneurs find it hard to keep up and lose a lot of business in the process. This may make business growth unattainable.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 10, March 2018

10.6. Loss of personal touch: Business is all about relationships. This business model erodes the personal touch between a customer and the business owner. Cultivating loyalty can thus be a problem since there are many such businesses that provide different options.

10.7. Delivery of goods can get delayed: It takes time before the goods ordered for are delivered. Sometimes the delivery delays and this inconveniences the customer. This is different from physical business premises where customers walk out with the products bought.

V. CONCLUSION : Digital signatures are difficult to understand. The public confidence is the key to e-commerce building and using. It comes from the information safety and the valid protection to privacy, so information safety and privacy protection are the most important problems in e-commerce development in many countries. The main aim of the text to apply digital signature technology in e-commerce system, advance the solution to the safety problems of digital signature technology in e-commerce and offer identity certification to those who take part in e-commerce activities, which prevent all kinds of potential safety hazards.

REFERENCES :

*J. Katz and Y. Lindell, "Introduction to Modern Cryptography" (Chapman & Hall/CRC Press, 2007)Stephen Mason, Electronic Signatures in Law (4th edition, Institute of Advanced Legal Studies for the SAS Digital Humanities Library, School of Advanced Study, University of London, 2016)..

*Lorna Brazell, Electronic Signatures and Identities Law and Regulation (2nd edn, London: Sweet & Maxwell, 2008);

*Dennis Campbell, editor, E-Commerce and the Law of Digital Signatures (Oceana Publications, 2005).

*M. H. M Schellenkens, Electronic Signatures Authentication Technology from a Legal Perspective, (TMC Asser Press, 2004).

*Jeremiah S. Buckley, John P. Kromer, Margo H. K. Tank, and R. David Whitaker, The Law of Electronic Signatures (3rd Edition, West Publishing, 2010).

Name: - Harpreet Kashyap

Student of M.COM 1st

Roll No.: - 2219

Department: - Commerce

Swami ganga giri janta girls college, Raikot(PB) India

