International Journal of Engineering& Scientific Research
Vol. 6 Issue 3, March 2018
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://esrjournal.com, Email: esrjeditor@gmail.com Double-Blind
Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

E-Commerce: Models and digital signature

ANJU DEVI
Department of Computer Science and IT
GNG College, Santpura, Yamuna Nagar

Abstract -Internet is most popular now a days. Internet is used in every field of life like: entertainment, shopping, e-billing, video conference, communication etc. In this era, Internet age changes the business exchange style and conveys numerous business chances to the e-commerce. E-commerce is characterizes as the purchasing and selling of item on the web. Nowadays electronic commerce services have risen to become more and more popular on Internet and Web environment. Exchange something through the help of internet, security on network is very important for e-commerce service. These are some of the most popular examples of e-commerce websites across the world like: Amazon, eBay, ALIBABA, Priceline and OLX etc. In this paper, we discuss some security related issues such as authentication, authorization, non-repudiation, and integrity. E-Commerce can help enterprises reducing cost, obtaining greater market and improving relationships between buyers and sellers. Security is very important in online shopping and in every field of life. Digital signature is similar like to handwritten signature but more secure than the handwritten signature also discuss.

Keywords: E-Commerce business model, security, digital signature, advantages and disadvantages of e-commerce

Introduction: E-Commerce is the activity of buying or selling of products on online services over the Internet. Electronic commerce draws on technologies such as mobile commerce, electronic funds transfer, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems etc.

When working, selling, or buying with any of these models, it is important to be familiar with what each model contains. B2C represents most of E-Commerce websites. Businesses that sell to consumers are considered B2C. Online stores and shopping are all examples of B2C. B2B are businesses selling products to other businesses. B2B are usually larger companies that are supplying a service to other businesses. Also, they are almost always doing business over the web. C2C is a website that consumers sell to other consumers. People are brought together to sell and buy products for this model. These four E-Commerce business models are very common in this day-in-age. There are various types of advantages and disadvantages of the e-commerce like as: product will be available easily and low prices. Customer can easily select the services and products without physical movement. E-commerce there are some disadvantages also which are given below like that: can't check the products, can be fraud etc. Security is very important concept in almost every field but when we sells or buys a product that it will becomes very important for our life some security related issues such as authentication, authorization, non-repudiation, and integrity, confidentiality etc. A digital signature is the electronic equivalent of a handwritten signature, verifying the authenticity of electronic documents. In fact, digital signatures provide even more security than their handwritten signature

E-Commerce Business Models

There are various types of E-Commerce business models which are given below:

- B2C which stands for Business-to-Consumer,

- B2B which stands for Business-to-Business model,
- C2C which stands for Consumer-to-Consumer, and
- B2G which stands for Business-to-Government.
- G2B which stands for Government-to-Business.
- C2B which stands for Consumer-to-Business.
- G2C which stands for Government-to-Business.
- C2G which stands for Consumer-to-Government.

Business-to-Consumer(B2C)

It means Business-to- consumer (B2C) model. It is a type o e-commerce in which business sells its products, while on the other hand buys its services and products by consumers. The concept was first developed in 1979 by Michael Aldrich. For example:Amazon.com.

Business-to-Government(B2G)

A "B2G", meaning business-to-government. When a government entity uses the Internet to purchases goods or services from a business, the transaction may fall under B2G ecommerce. It is a type of e-commerce in which business sells its products, while on other side government sells its products. It refers to businesses and government agencies using the Internet to mutually exchange information and trade with each other more efficiently. For examples: Tenders etc.

Business-to-Business(B2B)

It means business to business. It is a type of e-commerce in which buyers and sellers both are businesses. In this one business is sell its products and services, while other are buyer its services.

Consumer-to-Business(C2B)

It stands for consumer to business. It is also a type of e-commerce in which consumer sells its products and business buys its products. Its most common example are advertisements that people puts on different sites. For examples: priceline.com etc.

Consumer-to-Consumer(C2C)

Consumer-to-Consumer (C2C) is a type of electronic commerce in which consumers sells its products to another side also consumer buys its products through internet. For example olx.com

Government to business (G2B)

It is a type of e-commerce in which government to sells its products and on the other hand business buys its products.G2C transactions take place when a company pays for government goods, services, or fees online. Examples could be a business paying for taxes using the Internet.

Government to Consumer (G2C)

It is also a type of e-commerce in which government sells the products and consumers buys its products. Consumers can also engage in G2C ecommerce. People paying for traffic tickets or paying for their car registration renewals online may fall under this category.

Consumer to Government (C2G)

C2G stands for Consumers to Government. It is also a type of e-commerce in which consumers sells the products and government buys its products.

Advantages of e-Commerce

There are a lot of advantages of e-commerce like –:

- Products and services are easy to find.
- More reach to customers, there is no theoretical geographic limitations.
- Higher quality of services and lower operational costs.
- No need of physical company set-ups.
- Easy to start and manage a business.
- Customers can easily select products from different providers without moving around physically.

Disadvantages of E-commerce

- Anyone can easily start a business. And there are many bad sites which eat up customers' money.
- There is no guarantee of product quality.
- As there is minimum chance of direct customer to company interactions.
- There are many hackers who look for opportunities to attack on the e-commerce site.
- Hackers target web shops more often than you think.
- Fraud and online insecurity
- Data privacy issues
- No testing or checking of services or goods
- Dependence on electronic technologies

E-Commerce Security

Security is an essential part of any transaction that takes place over the internet. Following are the essential requirements for safe e-payments/transactions −

Confidentiality –

Unauthorized users unable to understand the message except the actual receiver. For example, unauthorized users able to intercept information, but the information is transmitted and stored as cipher text and is useless without a decoding key that is known only to authorized users.

Integrity –

Information should not be modified during its transmission over the network. When sender sends the message to receiver then unauthorized users cannot modify or change the message. Therefore, many cryptosystems use techniques and mechanisms to verify the integrity of information.

Authenticity –

Only authorized persons can access the data or to do communication with each others. Unauthorized are not allow to communication. cryptosystems use various techniques to authenticate both the sender and receiver of information.

Non-Repudiability –

Non repudiation prevents either sender or receiver from denying a transmitted message. Once a sender sends a message, the sender should not be able to deny sending the message. Similarly, the recipient of message should not be able to deny the receipt.

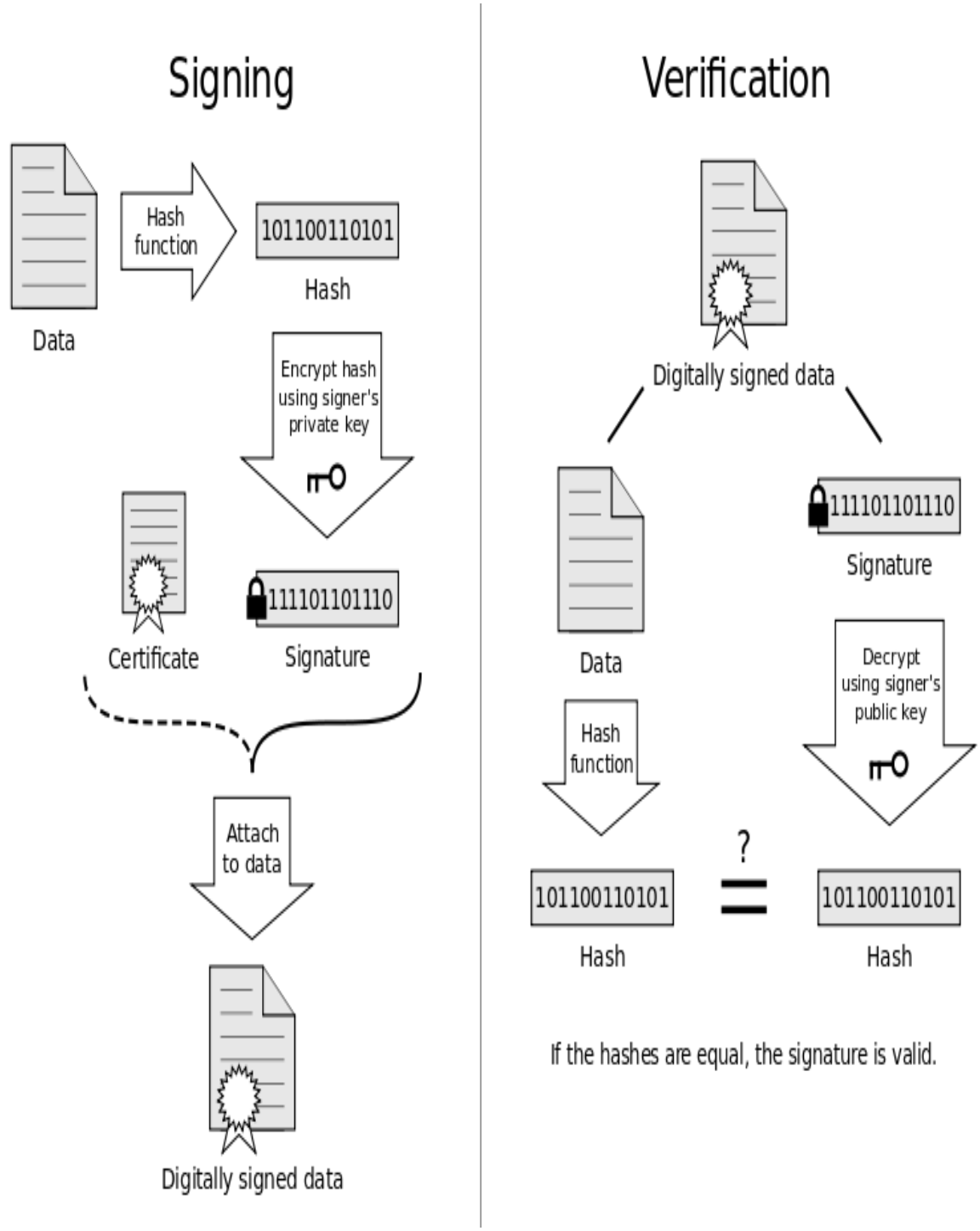
Encryption –

Information should be encrypted and decrypted only by an authorized user.

Digital Signature

A digital signature is the electronic equivalent of a handwritten signature, verifying the authenticity of electronic documents. In fact, digital signatures provide even more security than their handwritten signature. Some banks and package delivery companies use a system for

electronically recording handwritten signatures. Digital Signature is a electronic signature whose authentication are guaranteed through data security like encrypt, decrypt password etc. A digital signature is used to authenticate digital information such as e-mail messages, and documents by using computer cryptography. A digital signature is a mathematical scheme for presenting the authenticity of digital messages or documents. Digital signatures employ asymmetric cryptography, asymmetric means both private and public key are used. The mathematical algorithm acts like a cipher, creating data matching the signed document, called a hash, and encrypting that data.



In this scheme , a message is encrypted with the sender's private key to generate the 'Signature '.The message is then sent to the destination along with the signature. The receipt decrypts the signature using the sender's public key. And if the result matches with the copy of the message

received, then it is sure that the transmission of the message are not modified. A hash of a text unique, fixed-length value. In some documents, a *hash* of a text is also called a digest. Hash, then, can be used as a unique identifier of its associated data. The receiver can then compute a hash on the data received and compare the hash computed with the hash received. If the two match, the data received must be the same as the data from which the received hash was created.

To verify a signature, both the message and the signature are required. First, a hash value must be created from the message in the same way the signature was created. This hash value is then verified against the signature by using the public key of the signer. If the hash value and the signature match, you can be confident that the message is not corrupted by others users.

Certificate Authority (CA)

A digital certificate is an electronic document issued by a Certificate Authority (CA). It contains the public key for a digital signature and specifies the identity associated with the key, such as the name of an organization. The certificate is used to confirm that the public key belongs to the specific organization. The CA acts as the guarantor. Digital certificates must be issued by a trusted authority and are only valid for a specified time. They are required in order to create a digital signature.

Conclusions

The digital signature has become most significant tool in international commerce. Both side sender or receiver comes from the information without corrupted are most important problems in E-commerce. Until e-commerce vendors achieve the necessary delicate balance of privacy, trust and security, effective and quantitative ecommerce transactions will remain a problem. Thus the mechanisms of encryption, protection, verification and authentication indeed influence perceptions of security. The market place can be trustworthy only when consumers feel trust in transacting in that environment. Digital signatures in an increasing percentage of their commercial transactions. Within the digitally signed documents may be emailed from one country to another country less than one minutes, while the same document could take a day to arrive if sent through a commercial delivery service. So here we only talk about digital signature technology the safety of the public key will be investigated in future.

References

1. Selected articles on Digital Signatures (2014-today), by Ashiq JA, Guillaume Forget, Peter Landrock, Torben Pedersen, Dawn M. Turner and more
2. www.wikipedia.com/digital signature/definations etc.
3. www.google.com
4. Online Advertising To Reach $33 Billion Worldwide By 2004. Forrester Research Press (1999) http://www.forrester.com/ER/Press/Release/0,1769,159,FF.html.
5. Online Advertising To Reach $33 Billion Worldwide By 2004. Forrester Research Press (1999) http://www.forrester.com/ER/Press/Release/0,1769,159,FF.html.
6. Bellare M, Miner S K. A Forward-secure Digital Signature Scheme[C].
7. Proc. of Advances in Cryptology-CRYPTO. 1999:431-448.
8. Kain K. Electronic documents and digital signatures.
9. Kain K, Smith SW, Asokan R. Digital signatures and electronic documents: a cautionary tale. In advanced communications and multimedia security 2002 (pp. 293-307). Springer US.
10. Pordesch U, Berger A. Context-sensitive verification of the validity of digital signatures. Multilateral Security for Global Communication. 1999.