Role Of Encryption In E-Commerce

Amit Kumar Mandle; Dr. Varsha Namdeo

ABSTRACT: Believe it or not, e-commerce or electronic commerce has grown to epic proportions. In fact, it has become one of the fastest growing and transforming domains of industry in the last two years, or so. Billions of dollars have passed hands in the process, and each progressive entrepreneur wants a slice of the pie. To make this possible, methods of data encryption plays a very crucial role in ensuring customers that are paying for anything online, is safe and completely secure. As the development of Internet in the recent years, e-commerce has given a new dimension; and emerged by giving new forms of business activities; since every boon of Science has its downsides too, the security of the traditional cryptographic technique application method is under threat as well. By using cryptographic technique with e-commerce to the application of cryptographic technique and the development of E-commerce is very important to practical significance. This paper will briefly evaluate, analyze, study, highlight and measure encryption techniques, their overall roles in e-commerce and the future of encryption, as far as e-commerce is concerned.

Key Words: Cryptography, Encryption, Decryption, Plaintext, Ciphertext, E-commerce.

1. INTRODUCTION:

What Is E-Commerce?
The different types of e-commerce models available are –
- Business to business (B2B),
- Business to customer (B2C),
- Customer to customer (C2C),
- Customer to business (C2B),
- Business to government (B2G).

The seminal purpose of e-commerce is to perform Business-to-Business (B2B) as well as Business-to-Consumer (B2C) online transactions, and to exchange goods and services from a distance by any electronic and networked device that can use the Internet, that has now covered all the existing platforms worldwide. E-commerce is all about the exchange of information by Electronic Data Interchange (also known as EDI). The success of e-Commerce will continue to be a critical part of business growth & development and enhanced performance only if it can overcome the concerns businesses and consumers have with stolen identity, secure banking, payments, and transactions. One of the finest ways to wipe out these concerns (and secure e-Commerce) is to use the concept of cryptography (briefly - the practice as well as study of techniques for secure communication).

What is Encryption?
Encryption is the defined procedure of converting normal text (data) into “Cipher text.” Once completed, this makes it impossible for someone to read/scan/understand or interprets the original data until it is decrypted back into its original state. This allows the secure and safe exchange of data between companies and even individual-to-company without the risk of someone “in the middle” intercepting this data and using it in a harmful or illegal sense. Once the data has been encrypted, only the person who has originally encrypted the data or the recipient, who has been provided the decryption key, will be able to decrypt it and read the data. These days we often hear about hacking, where hackers are often found to be stealing data from large-scale companies, banks and retailers, which presents a possible threat to those databases where the data is stored and somehow makes it not-so-reliable. In order to conquer this unauthenticated and illegal activity, encryption methods are vital. It takes a very significant effort and very expensive technology to decrypt this stolen data in an effort to keep your information secure.

2. RELATED WORK AND METHODOLOGY:
Certain techniques for encryption and decryption of a message applied in E-Commerce have been discussed by Rane [3], Gudimetla [1], Yadav [7], Rathi [4], Vishvalingam [6], Zaru [8], Murphy [2], Ritu [5] and others. Subsequent them in this paper, we will discuss the techniques for encryption applied in E-Commerce and give the suggestions for future security in E-commerce.

3. USING ENCRYPTION TECHNOLOGY IN E-COMMERCE:
As our use of E-commerce continues to soar, the need for encryption of customer data (as well as inventories, company financial information, etc.) increases exponentially as well. You must be knowing the fact that whenever you sign up on a website for a membership, club, or even just for their weekly newsletter, your personal information is stored in a certain database. Once you start to purchase products or services from that retailer or service company, those transactions are stored in your “history” for a record of your activity with that company. If you think about it, you now have a majority of your personal information tied to your purchase history, including your basic personal details and the most secret of all the information and that is none other than your credit card information and more. If it weren’t for encryption, if a hacker were to breach the initial security of these websites, they would have access to all of your vital information. To try and prevent our system from this unethical approach that generally leads to a serious consequences of mishap, companies have special and dedicated teams within their organization that, not only are responsible for encrypting the data to keep it secure, but are also constantly reviewing new technologies to support an even stronger encryption and data security solution. It is

IUSTR©2019
www.ijstr.org

2881
a continuing fight and commitment to an increased vigilance that keeps these experts steps ahead of hackers and thieves to keep your data safe. Here at Unleaded Group, we are committed to keeping our clients and their customers safe with the latest encryption technologies.

4. CRYPTOGRAPHY IN E-COMMERCE:
The Internet is not known for its secure environment. In fact, the Internet is not safe for e-Commerce that usually involves tremendous amount of transactions, unless it involves using cryptography and making its users aware of the concerns with e-Commerce. PC users need to know, how to improve e-Commerce security. Both PGP and SSL encryption provide cryptography; they can form the basis of a secure e-Commerce infrastructure. It is fair to say that, when performing an e-Commerce transaction, people still tend to provide their credit information to just about anyone asking without first knowing for sure, that the person or the Web site is completely safe and can be trusted. Trust in e-Commerce is indeed a real concern. Being in e-Commerce involves risks (such as spoofing and eavesdropping) and possible threats (such as privacy). The use of cryptography in e-Commerce provides a safety layer, which is the only way to ensure highly secure e-Commerce transactions and Web applications that contain a customer's personal information. If e-Commerce is allowed to handled by SSL, server security and digital certificates, then it will be completely in safer hands and this will provide the authentication, privacy and data integrity through encryption that is needed to overcome threats associated with Internet-based transactions. The importance of cryptography is that, it can protect e-Commerce and reassure businesses and consumers that they are safe and secure from prying eyes (hackers who utilize the Web to steal information). The use of cryptography allows the integrity of e-Commerce transactions and can safeguard information. Thinking practically, providing cryptography is the only way to secure an e-Commerce environment for banking; and SSL encryption is necessary to handle payments—to establish a secure channel, that can guarantee a customer's financial data remains secure.

5. THE FUTURE OF E-COMMERCE:
Simply said, e-Commerce is the way of the future. It changes how people will conduct business, buy and sell things, and provide goods and services right from a PC. Knowing this, e-Commerce must have a secure environment so that people and business alike, need not to worry about unethical access (like hackers) stealing their identity and data to gain access to their credit cards or banking related information. If e-Commerce is going to continue to be a significant part of conducting business online, then it will require: security and trust. And, the use of cryptography and encryption is a must to protect the customers who provide their personal information online.

6. RECOMMENDATION:
With all the above realizations, that some encryption techniques can be cracked if the right resources are channeled and synched towards the process, this paper recommends that those loopholes should be perused and they are supposed to be solved amicably. This could be done by, investing the right kind of resources or more, that maybe needed to break the code if possible, and exploring the number of bit blocks that are used to break that code. After all this is done, the developers will be in a good way to determine the exact requirements needed to improve the existing algorithm. Such techniques, for example, are the likes of Data Encryption Standard (DES). AES is said to be a direct improvement/replacement to the DES, as it uses transformations on 128bit blocks as compared to the 64bit blocks of DES. Also, this research suggests that online customers should be advised to opt for latest encryption enabled software environments like SSL enabled browsers, as their payment information needs to be confidential between them and their retailers and only such environments can guarantee such confidentiality and integrity.

7. CONCLUSION:
For the comprehensive security measures of transactions and information that sandwiches the layer between the buyer and the seller online, there has to be versatile and robust technological advancements thus, ensuring the benefits that different techniques of e-commerce are catered for. It has been acknowledged in the paper, that hackers are also improving their cyber intellect and resources to counter or manipulate the existing encryption techniques for e-commerce systems, so the authorities should act well in time to save the customers from such incidents. However, with integration of other online security mechanisms and protocols like the Intrusion Detection Systems, the encryption techniques used for e-commerce industry would not come costly as the intrusion detection systems would keep hackers at bay as well as deter any other security breaches.

REFERENCES