Security Threats in E-Commerce environment

The rapid advancement in technology allows everyone to send and receive information from anywhere in the world. People initially used to share information but slowly this technology began to emerge in business areas like marketing, buying and selling, called e-commerce. All commercial transactions are performed online. E-commerce provides many amenities for everyone at the same time there is an opportunity for misuse of technology. In this article, e-commerce is discussed in detail on related security issues. Knowledge of securities maximizes the benefits of e-commerce.

Security issues concerned with e-commerce

Despite its advantages and limitations, e-commerce has some security problems in practice. The security of e-commerce is nothing but preventing loss and protecting the regions financially and informally from unauthorized access, use, or destruction. Due to the rapid developments in science and technology, the risks involved in using technology and security measures to avoid organizational and individual losses change day by day. There are two important types of encryption that we follow in secure e-commerce transactions.

- **Symmetric Encryption (Private Key):** This is an encryption system in which the sender and receiver have the same key. The key used to encrypt the message is also used to decrypt the encrypted message from the sender.

- **Asymmetric encryption (public key):** In this method, the actual message is encrypted and decrypted with two different mathematical keys, one called the public key and the other called the private key.

Ecommerce Security Threats & Issues

There are quite a few threats that you need to protect your online store from. Let's talk about some of the common types that often afflict businesses online.

i. **Financial Frauds**

Financial fraud has infected an online business since its inception. Hackers make unauthorized transactions and erase the path that costs companies large amounts of losses.

Some fraudsters make requests to return counterfeit money or returns. Refund fraud is a common financial fraud in which companies return funds for illegally obtained products or damaged goods.

For example, Jimmy loves to take advantage of fraudulent activities. He knows that friendly fraud is an easy way where he can buy and use an item and then get it back in order to get his money back, so he does it!

ii. Spam

As emails are known to be a powerful medium for high sales, they also remain one of the most used spam media. However, comments on your blog or contact forms are also an open invitation to online spammers as they leave the infected links in order to harm you. They often send them through a social media mailbox and wait for clicks on such messages. Moreover, spam does not only affect the security of your website, it also damages the speed of your website.

iii. Bots

You might learn about robots from your good books like those that crawl the web and help you rank your website on search engine results pages. However, there are exclusive robots developed to scrape websites to obtain pricing and inventory information. Hackers use this information to change the prices of your online store, or to get the best-selling inventory in shopping carts, which results in lower sales and revenue.

iv. DDoS Attacks

Distributed Denial of Service (DDoS) attacks and DOS (denial of service) attacks aim to disable your website and affect overall sales. These attacks flood your servers with many requests until you surrender to them and your website is down.

v. Brute Force Attacks

These attacks target your online store dashboard in an attempt to discover your password with brute force. It uses software that creates a connection to your website and uses every possible combination to hack your password. You can protect yourself from such attacks with a strong and complex password. Remember to change it regularly.

vi. SQL Injections

SQL injection operations are cyberattacks aimed at accessing your database by targeting your query submission forms. They enter malicious code into your database, collect data and then delete it later

vii. XSS

Hackers target visitors to your website by infecting your online store with a malicious code. You can protect yourself from applying the content security policy.