iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** I **Month of publication:** January 2023

DOI: https://doi.org/10.22214/ijraset.2023.48475

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue I Jan 2023- Available at www.ijraset.com

Security Challenges and various methods for Increasing Security in E-Commerce Applications

Aashutosh Bansal[1], Tejna Khosla[2], Vinay Kumar Saini[3]
[1, 2, 3]*Department of Information and Technology, Maharaja Agrasen Institute of Technology, Delhi, India*

Abstract: ***E-Commerce security is a component of information security framework and applied to avenues including data security, computer security etc. It includes protection of E-Commerce assets against illegal access, use modification or demolishing of data. However, due to increase in sensitivity to assaults, the attackers employ phony websites and apps to breach the security of payment related activities over the internet. This paper presents the review of various security challenges encountered in e-commerce applications and the methods to avoid or overcome them. The paper provides a survey of some techniques employed by various researchers. The majority of banking transactions now take place online due to the expansion of e-commerce. They use merchant-provided websites or pay-per-use apps which increases their sensitivity to assaults and increases the likelihood that attackers will employ phony websites and apps. There are numerous strategies for protecting against vulnerabilities that can be used. In this paper, we have provided a survey of the Security methods employed for safeguarding the banking transactions.***

Keywords: E-commerce, security, banking, payment gateway.

I. INTRODUCTION

E-Commerce, also known as electronic commerce or internet commerce, is an activity of buying and selling goods or services over the internet or open networks. So, any kind of transaction (whether money, funds, or data) is considered as E-commerce.

E-commerce models can generally be categorized into the following categories.

1) *Business to Business (B2B):* In this type of model a wholesaler places order directly to a company and further he sells the products to the customers as retails
2) *Business to Consumer (B2C):* In this model a customer orders his desired product directly from the website. And the company ships the product to his customer.
3) *Consumer to Consumer (C2C):* This model helps customers to sell their assets like residential property, vehicles, etc., or rent a room by publishing their information on the website.
4) *Business to Government (B2G):* As the name itself suggests, in this type of model, websites are used by the government for trading and exchanging information.
5) *Government to Business (G2B):* This model websites are used by the government in the case of auctions, tenders etc.
6) *Government to Citizen (G2C):* This model websites are for helping the citizens which supports auction of vehicles and also provides services like birth, marriage, death certificates.G2C)
7) *Business to Administration (B2A):* This model consists of online transactions that takes place between companies and public administration like government.
8) *Consumer to Administration (C2A):* This model consists of online transactions that takes place between people and public administration like government. C2A transactions includes paying taxes and paying fines or paying tuition fees to the college or university.

Since the previous decades, e-commerce has been used much more frequently, and as a result, there are now an exponentially greater number of payment transactions done on online platforms. In this regard, E-Commerce security is a part of information security framework and gives guidelines for securing the networks and systems involved in the implementation.

II. LIFE CYCLE OF A DIGITAL E-COMMERCE ORDER

The majority of transactions are online due to expansion of E-Commerce. The use merchant provided apps to place their order. Some popular websites are Amazon, Flipkart, E-bay and much more. Fig.1 shows the life cycle of an order placed using e-commerce platform. It starts with a customer who places a request order using the client browser.

The request is sent to the merchant's web server and received by the merchant. Both the client browser and merchant's server are linked to the payment server where customer and merchant are verified, order information and payment information are reviewed, the order is confirmed or payment is denied. These payment servers are third party computers which uses multiple payment systems like Credit card (VISA or Master card), Bank Accounts (Debit Card or Online Banking), E-bill payments (UPI, PAYTM) etc. once the order is verified, the details are sent to the customer, merchant are warehouse and the shipping is done. The customer receives the product and request is closed.

Fig. 1. Life Cycle of order placed in E-Commerce

III. RECENT SECURITY CHALLENGES IN E-COMMERCE

E-Commerce security is categorized into 4 features:

1) *Authentication:* Ensuring the identity of the user. It makes it clear that nobody else is permitted to get on to your internet banking account.
2) *Authorization:* Controlling of your resources like increasing the account balance or removing a bill.
3) *Encryption:* Hiding the information for others so that our banking transactions become safe.
4) *Integrity:* Preventing unauthorized modification of data.

Various researches show that to ensure a secure business transaction in the finance industries, the security challenges in e-commerce are a big concern. We have identified 3 types of security threats namely:

a) *Denial of Service:* In DOS majorly spamming and viruses are seen. Spamming includes sending unrequested commercial e-mails to everyone. The hackers place software agents in the third party system and keeps sending requests to different targets, Sometimes thousands of email messages target a computer or network and referred as email bombing. Viruses are the programs that replicate itself to perform undesirable events.
b) *Theft and Fraud:* Theft and Fraud occurs whenever the data is stolen, used and modified. It can be a data theft, a software theft or a hardware theft.
c) *Unauthorized Access:* Accessing the systems or data illegally. The system can be modified and content can be used for destroying purposes. Masquerading involves sending a message from a different identity.

The researches show that there are several challenges that are part of DOS, theft, fraud, and Unauthorized access. Malware: Malware (viruses, trojans) are most vulnerable in E-Commerce nowadays. Next comes, Account Takeover (ATO) in which cybercriminals take ownership of online accounts using stolen passwords and usernames. Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid .

Phishing is done when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website. SSL encryption threats: This bug allows attackers to steal private keys attached to SSL certificates, usernames, passwords and other sensitive data without leaving a trace. An Insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems. Drive by Downloads: the unintended download of computer software from the Internet: Authorized drive-by downloads are downloads which a person has authorized but without understanding the consequences.

Bots nowadays are a very big security concern. These are some special software that are developed by the attackers that usually brush your website to get some information. They can modify the prices of the items listed on your websites to lower the revenue generated. Or to degrade your sales.

Some Vicious Bots can be classified as:

- *Account Takeover Bots:* Account Takeover is a type of identity theft in which criminals access user accounts without authorization. Account takeover can be carried out utilizing a variety of automated attacks, namely Credential Stuffing (bulk login attempts used to confirm the legitimacy of stolen username/password pairs) and Credential Cracking (validating login credentials by testing various username and/or password values). Identity theft is not something to take lightly, especially when it is undertaken on a large scale. If successful, an attack might have far-reaching effects on both organizations and customers. Unrestricted assaults may also cause brownouts and denial of service, which could cost more in terms of infrastructure and result in lost revenue.
- *Scalping Bots:* These have been a problem on the internet for a while, but they have just lately gained attention because to their resurgence and targeting of new markets during the worldwide pandemic. Scalping is the practice of unfairly obtaining desirable or limited-supply products and services with the intention of reselling them for a profit at a higher price. For several years now, highly sought-after sneaker launches, concerts, and athletic events have been the targets of scalpers.
- *Spamming Bots:* They are also known as Fake News Spam and Comment spam. They are used to spread fake news and often post some fake reviews for products. Additionally, they are employed to conceal harmful material, such as malware, behind click-bait URLs. These mostly impact retail websites, news and media websites, and social networking websites. Spamming may, in some complex instances, even result in a number of fraud cases.
- *Scraping Bots:* Theft of proprietary data, such as pricing or custom content, directly affects the firm. It's possible that your rivals are undercutting you on price in order to provide better options and defeat you in the race for the lowest cost. It might also be custom content theft, like in the case of conversion rates in the financial services industry. This makes it possible for rival businesses to advertise more alluring conversion rates and get customers.
- *Card Cracking Bots:* One of the largest risks to retail, entertainment, financial services, and travel is the presence of financial fraud bots. Really, credit card fraud may happen on any website that accepts payments. Bad bots are used to validate credit card numbers that have been stolen by either performing numerous minor payments (carding) or attempting to locate missing information such as expiration dates and CVV numbers (Card Cracking). They raise customer service costs in order to handle false chargebacks, which immediately lowers organizations' fraud scores.

The statistical analysis of these security challenges in 2021 that fall under the above-mentioned categories are shown in Fig.2.

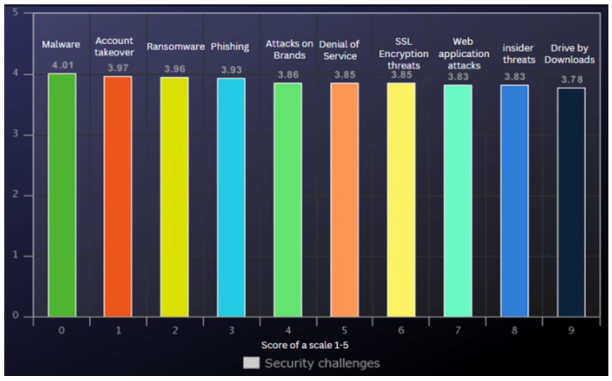


Fig. 2 Statistical analysis of E-Commerce and Security Challenges '2021

The figure shows that Malware has maximum impact out of all the challenges. It has a score of 4.01 on a scale of 5, which is 80.2% of all the challenges. Account takeover and Ransomware are 3.97 and 3.96, respectively. The lowest and most uncommon challenge is drive by downloads, which holds the score of 3.78 out of 5. Therefore, it can be concluded that there is a dire need to overcome these security issues.

IV. METHODS TO IMPROVE THE SECURITY CHALLENGES

We just discussed the security risks that an e-commerce company is likely to encounter. There are few measures to overcome these challenges, that have been proposed in the literature so far. Some of them are:

A. Authentication of Secure Payment Gateway

Since payments are a crucial part of your e-commerce operation, it is mandatory to take precautions to guarantee the security of the payment gateway.

There is no justification for not using a reputable payment gateway since most online store builders allows integration with dozens of well-known payment gateways like Paytm, Stripe, and other enterprise payment gateways. As a result, many e-commerce businesses suffer from credit card and debit card fraud. Using a secure payment gateway alone is not sufficient to guarantee safety. It can be accompanied with other security methods as well.

B. Encryption

According to research done by Amit Kumar Mandle , Dr. Varsha Namdeo. There should be at least one level of encryption on every e-commerce website. When you stop to think about it, practically every significant online retailer you can name—companies that immediately come to mind is eBay, both of which have at some point experienced a data breach. In other words, there is always some element of danger involved. Therefore, you should make sure that any data gathered about you in the event of a breach is essentially useless as your first action.

When encryption is turned on for an online store, user passwords are changed from "Normal Text" to a "Hashed Format" that is difficult to encode.

C. Securing Website with a SSL Certificate

According to Angamuthu Maheswaran and Rajaram Kanchana, One of the greatest ways to protect your e-commerce firm is to use an SSL certificate.

When implemented correctly, an SSL certificate will encrypt all the data users provide to your e-commerce website, making it difficult for hackers to intercept this data or interpret it in any way should they do so.

Users also have a tendency to trust e-commerce sites that utilise a wildcard SSL certificate, and Google generally ranks sites that employ SSL better. A website without one would likely lose a lot of customers. An SSL certificate will increase traffic to your website and boost conversion rates in addition to safeguarding sensitive user data supplied there.

Some types of SSL are:

1) SSL Record Protocol: SSL Record Protocol ensures that the data that is being transferred between a user and a server always remain safe.
2) Handshake Protocol: Handshake Protocol uses the public key infrastructure and makes a shared symmetric key. Which ensures integrity between both the user/client and server.
3) Change-Cipher Spec Protocol: Change-Cipher Spec Protocol is used to alter the secret sent between user and server.
4) Alert Protocol: Alert Protocol is the process of informing information regarding failure in authentication or any other irregularities.

D. Secure Server

Making complicated passwords with a variety of characters is the goal. Additionally, you must periodically replace them. Both defining user roles and regulating user access are very good habits. Only when absolutely essential, permit everyone to access the admin panel. Have the panel notify you anytime a foreign IP attempts to access it for added security.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue I Jan 2023- Available at www.ijraset.com

E. Using Multi-Layer Security

A developer can use extra security layer, like Multi Factor Authentication.

Two factor authentication is a good practice. If a user enters a login information, user should get a token or OTP on his registered email address or on his mobile number if user adds his mobile number.

By implementing this step, it reduces the risk of getting the user's details getting leaked.

Fig 3. Below shows how Multi Factor Authentication (MFA) works.

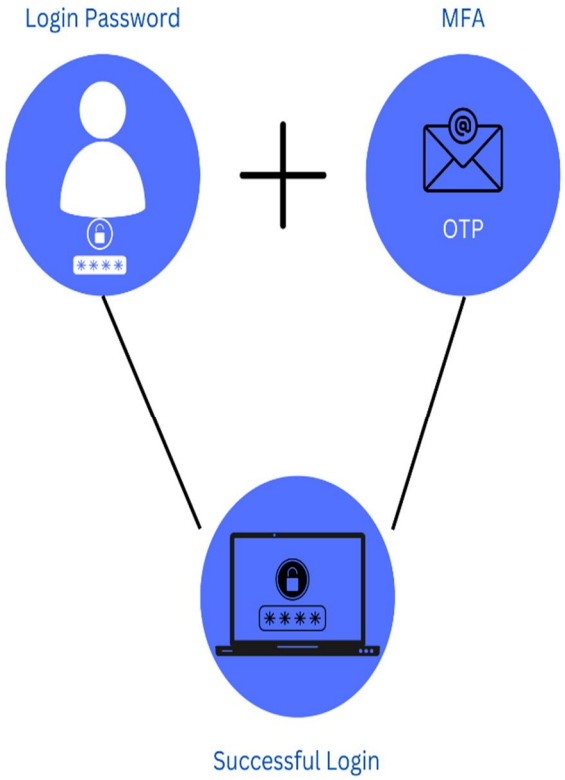


Fig. 3 How Multi Factor Authentication (MFA) works.

But most companies using MFA still got hacked.

F. Ecommerce Security Plugins

Security plugins are a very simple method which can increase security protection to the website. These plugins provides protection from various bad bots which sometimes attackers can add. One of the most secure and highly rich security plugins can be Astra. It will help to secure your website and will add software to your website which will help by preventing the bad requests.

G. Educating the Clients

Sometimes, there is no security issues at our end, but clients might be using some weak passwords or might leak some sensitive to any website which is in hand of hackers.

These issues can be solved by correctly educating or giving guidance to the consumers or the customers. Ask them to use a strong password including some special characters like "$, <, >, #, @" etc.

H. Regular Scanning

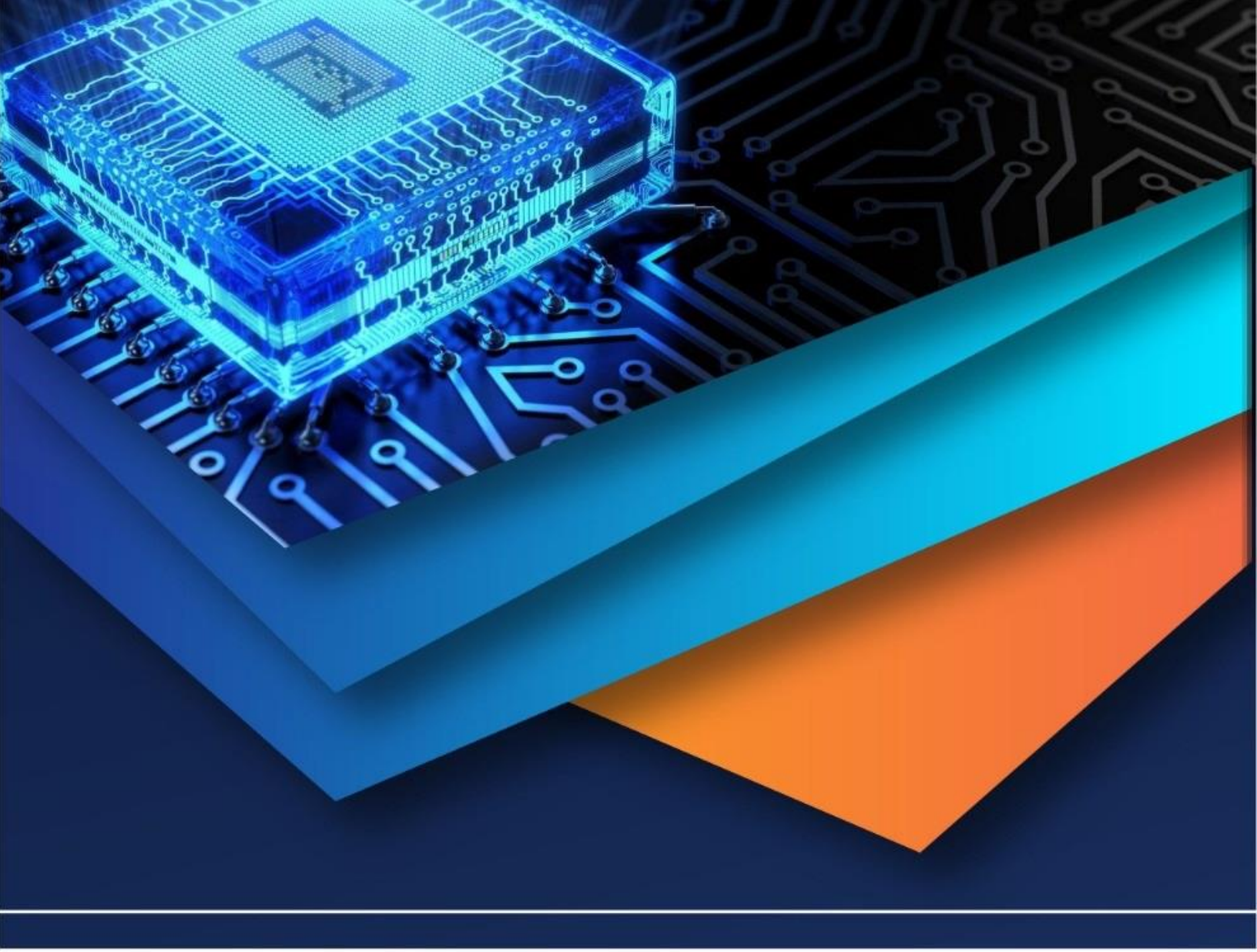
Keep an eye on your website which means each and every action happening on your website can be watched if possible. Regularly scanning of data should be considered, so that if something is going wrong, can be corrected within the time.

V. CONCLUSION

The study came to the final conclusion that data security is an important aspect of e-commerce in business industries. With regard to dealing secure dangers when shopping online, modern technology enables safe website design. We also concentrated on a few important security factors that are expanding quickly to support the expansion of e-commerce. It's crucial to remember that security precautions provide a good sense of protection. To find vulnerabilities in commercial industries' use of e-commerce, the security checks are also discussed.

REFERENCES

[1] Polsani Jahnavi , Balla Manoj Kumar. "SURVEY PAPER ON THE VARIOUS SECURITY ALGORITHMS USED FOR E-COMMERCE SECURITY."
[2] Yeow Chong Larry Tan "Recent Technological Trends and Security Challenges in Trust-Building in E-Commerce."
[3] Latif, R. M. A., Umer, M., Tariq, T., Farhan, M., Rizwan, O., & Ali, G. (2019, January)." A smart methodology for analyzing secure e-banking and e-commerce websites.
[4] Security issues in E-Commerce – How to Enhance Security: (https://www.cidm.co.in/security-issues-in-e-commerce/). Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.
[5] Nazmun Nessa Moon , Shaheena Sultana "A Literature Review of the Trend of Electronic Commerce"
[6] Zwaas Vladmir "Electronic Commerce: Structures and Issues." International Journal of Electronic Commerce / Spring 2003, Vol. 7.
[7] Shahid Amin "A Review paper on E-Commerce". Asian Journal of Technology & Management Research
[8] Dr.(Smt) Rajeshwari M. Shettar "EMERGING TRENDS OF E-COMMERCE IN INDIA: AN EMPIRICAL STUDY"



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY