iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.53050

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 VI Jun 2023- Available at www.ijraset.com

E-Commerce Application Security Issues and Various Security Enhancement Techniques

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

Abstract: ***A part of the information security framework, e-commerce security is used in areas like data security and computer security, among others. It covers safeguarding electronic commerce assets from unauthorized access, use, modification, or destruction of data. However, due to heightened awareness of attacks, the attackers use phoney websites and apps to circumvent the security of payment-related online activities. This article provides an overview of the many security issues that arise in e-commerce applications and discusses solutions. The study offers a survey of some methods used by different researchers. Due to the growth of e-commerce, most financial transactions now take place online.. They use websites or apps that are offered by businesses, making them more vulnerable to attacks and increasing the probability that attackers may use fake websites and apps. There are several methods that can be employed to defend against vulnerabilities. We have given a survey of the security measures used to protect banking transactions in this paper.***
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 orders directly to a company and further he sells the products to the customers as retails. Recent B2B innovators have carved out a niche for themselves by eschewing order forms and catalogs in favor of e-commerce storefronts and better niche market targeting. Millennials made up 60% of B2B buyers in 2021, an almost double increase from 2012. B2B selling online is growing increasingly crucial as younger generations enter the age of commercial interactions.

2) Business to Consumer (B2C): In this model goods or products are sold directly to the end users. Anything a customer buys from an online store related to their household products or any other products. It's done as a part of a B2C transaction. In particular for lower-value items, the decision-making process for a business-to-consumer (B2C) transaction is much quicker than a business-to-business (B2B). Compared to their B2B counterparts, B2C businesses often spend less on marketing while also having shorter sales cycles, smaller average order values, and fewer repeat business. B2C encompasses both goods and services. B2C innovators have used technology to directly sell to their customers and improve their lives, such as mobile apps, native advertising, and retargeting.

3) Consumer to Business (C2B): C2B model enables people to offer products and services to businesses. In this e-commerce model, a website might allow users to post the work they need done and request quotes from companies. Services for affiliate marketing would also be categorized as C2B. The pricing of goods and services is the competitive advantage of the C2B e commerce model. With this strategy, customers have the authority to set prices or to influence company competition to satisfy their wants. Recently, creative thinkers have connected businesses with social media influencers to market their products.

4) 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.

5) Business to Government (B2G): As the name itself suggests, in this type of model, Business-to-government (B2G) is an e-commerce model in which a company offers and sells its products to public administrations or government agencies, whether they be municipal, county, state, or federal. This business strategy depends on winning government contract bids. A request for proposals (RFP) will normally be posted by a government agency, and e-commerce companies will then be required to submit bids for these projects. B2G is different from other firms or consumers even if it is a more secure business model. Government organizations frequently move at a significantly slower speed due to their bureaucratic structure, which might restrict their ability to generate income.

6) Government to Business (G2B): This model websites are used by the government in the case of auctions, tenders etc.
7) 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)
8) Business to Administration (B2A): This model consists of online transactions that take place between companies and public administration like the government.
9) Consumer to Administration (C2A): This model consists of online transactions that take place between people and public administration like the government. C2A transactions include paying taxes and paying fines or paying tuition fees to the college or university.
10) Business to Business to Consumer (B2B2C): It is a business strategy in which a company partners with another organization to offer its goods or services to final consumers.

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 the 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. For customers to place their orders, the retailer offered apps. Some popular websites are Amazon, Flipkart, Ebay and much more. The life cycle of an order placed through an e-commerce platform is depicted in Fig. 1. It starts with a customer who places a request order via the client browser. The request is delivered to the merchant's web server, which then receives it. Both the client browser and merchant's server are linked to the payment server like Stripe, Razorpay etc. 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 including Credit card (VISA or Mastercard), 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 the request is closed.

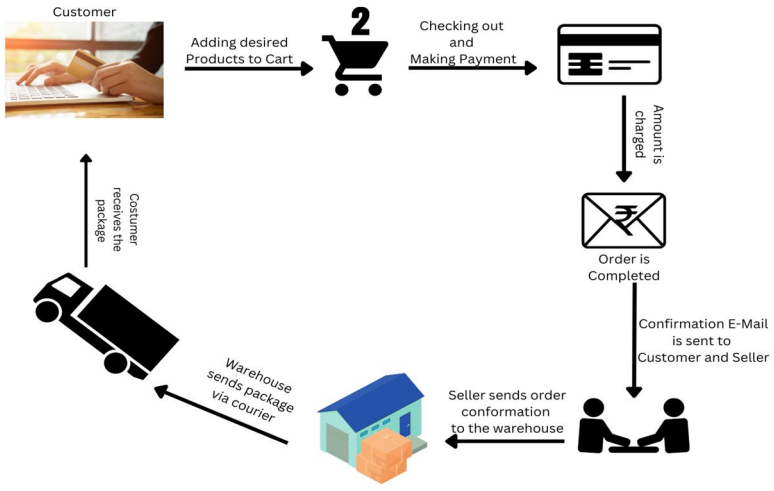


Fig. 1. Life Cycle of order placed in E-Commerce

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 emails to everyone. The hackers place software agents in the third party system and keep sending requests to different targets. Sometimes thousands of email messages target a computer or network and are referred to 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 studies demonstrate that there are a number of issues related to DOS, theft, fraud, and unauthorized access. Malware: In today's world, E-Commerce is especially susceptible to malware (viruses, trojans). 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 the act of an attacker tricking a user into doing "the wrong thing," such as opening a malicious link or visiting a dubious website. Threats to SSL encryption include the ability for hackers to gain the private keys associated with SSL certificates, usernames, passwords and other private information undetected. An insider threat is a malicious danger to an organization that originates from individuals who work there, such as current or former employees, contractors, or business partners, and who have inside knowledge of the company's security procedures, customer information, and computer systems. Drive-by downloads are unintentional Internet software downloads. permitted drive-by downloads are downloads which a person has permitted but without knowing the repercussions.

Today, bots pose a serious security risk. These are some specialized programmes created by the attackers who often browse your website to gather data. To reduce the revenue generated, they can change the prices of the goods listed on your websites. or to decrease sales

Some Vicious Bots can be classified as:

- *Account Takeover Bots:* Account Takeover is a sort of identity theft in which thieves gain unauthorized access to user accounts. Credential Stuffing (massive login attempts used to verify the validity of stolen username/password pairs) and Credential Cracking (validating login credentials by testing multiple username and/or password values) are two automated methods that can be used to take over an account. It is important to treat identity theft seriously, especially when it is done on a wide scale. An attack might, if successful, have a significant impact on both businesses and clients. Brownouts and denial of service may also be brought on by unrestricted assaults, which could increase infrastructure costs and result in lost revenue.
- *Scalping Bots:* These have been an issue on the internet for a long, but they have just lately attracted notice thanks to their comeback and targeting of new markets amid the worldwide pandemic. Scalping is the practice of unfairly obtaining desirable or in-demand goods and services with the goal of reselling them at a higher price for a profit. Scalpers have been a problem at popular sporting events, concerts and sneaker launches for a while now.
- *Spamming Bots:* They are also referred to as comment spam and fake news spam. They frequently submit phony product reviews and are used to promote false information. They are also used to hide malicious content, such malware, behind click-bait URLs. These primarily affect social networking sites, news and media websites, and shopping 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 likely that your rivals are undercutting you on price in order to provide better options and defeat you in the fight for the lowest cost. In the case of conversion rates in the financial services sector, it might also be custom content theft. Competitor companies can advertise conversion rates that are more enticing to customers as a result.
- *Card Cracking Bots:* Financial fraud bots are one of the biggest threats to retail, entertainment, financial services, and travel. Actually, any website that accepts payments is vulnerable to credit card fraud. Bad bots are used to confirm credit card numbers that have been obtained by either conducting several tiny payments (carding) or attempting to locate missing information such as expiration dates and CVV codes (Card Cracking). To deal with bogus chargebacks, they increase customer support expenses, which decreases organization’s fraud scores right away.

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

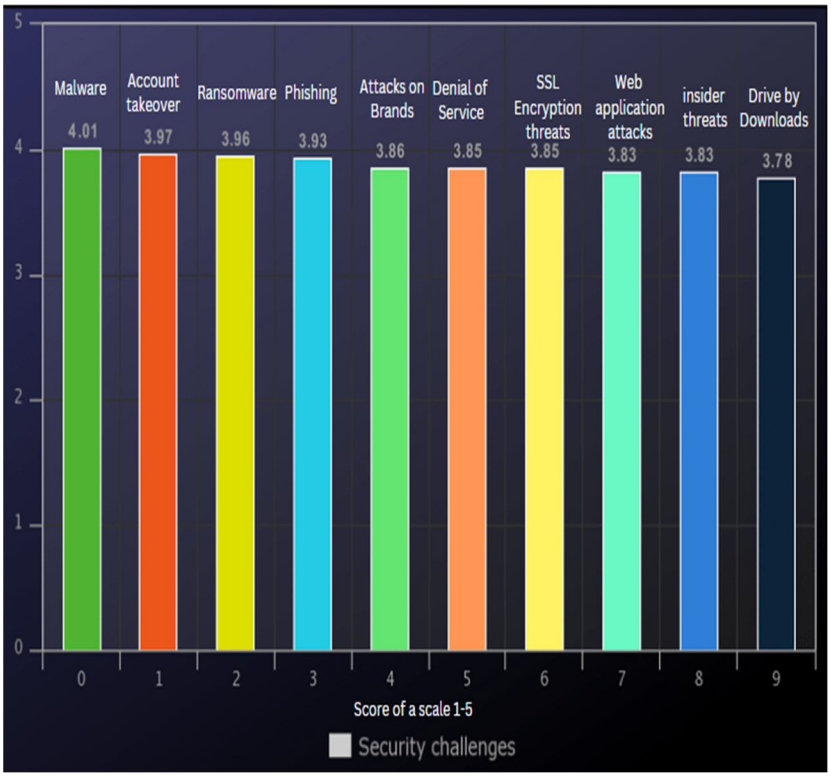


Fig. 2 Statistical analysis of E-Commerce and Security Challenges '2021

The figure shows that Malware has the 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

The security dangers that an e-commerce business is likely to face were recently covered. There haven't been many solutions to these problems put up in the literature thus far. Among them are:

A. Authentication of Secure Payment Gateway

Payments are an essential component of your online business, so you must take care to ensure the security of the payment gateway. There is no justification for not using a reputable payment gateway since most online store builders allow integration with dozens of well-known payment gateways like Paytm, Stripe, and other enterprise payment gateways. As a result, credit card and debit card theft affects numerous e-commerce enterprises. The only way to ensure safety is to use a secure payment channel. It can also be used in conjunction with other security measures.

B. Encryption

Dr. Varsha Namdeo's research, conducted by Amit Kumar Mandle. Every e-commerce website ought to use at least one degree of encryption. When you think about it, nearly every significant online retailer you can think of—companies like eBay come to mind first—have both at some point encountered a data breach. In other words, risk is constantly present in some form. As a result, your first step should be to make sure that any information collected about you in the case of a breach is essentially useless.
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

Using an SSL certificate is one of the best ways to protect your e-commerce company, according to Angamuthu Maheswaran and Rajaram Kanchana. An SSL certificate, when used properly, will encrypt all the information customers provide to your e-commerce website, making it more difficult for hackers to intercept this information or use it in any way.

Additionally, users are more likely to trust e-commerce websites that make use of wildcard SSL certificates, and Google generally gives SSL-enabled websites a higher ranking. Without one, a website would probably lose a lot of visitors. An SSL certificate will improve website traffic, raise conversion rates, and protect sensitive user data submitted 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 remains 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

The objective is to create complex passwords using a range of characters. Furthermore, you must regularly replace them. Both specifying user roles and controlling user access are excellent practices. Don't let anyone use the admin panel unless it's absolutely necessary. For further security, have the panel alert you whenever a foreign IP tries to access it.

E. Multiple-Layer Security

A developer may employ an additional layer of protection, such as multi-factor authentication.

A decent authentication method is two-factor. When a user logs in, they should receive an OTP or token on their registered email address or, if they add a mobile number, on that number as well.

This procedure decreases the possibility of user information being compromised.

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

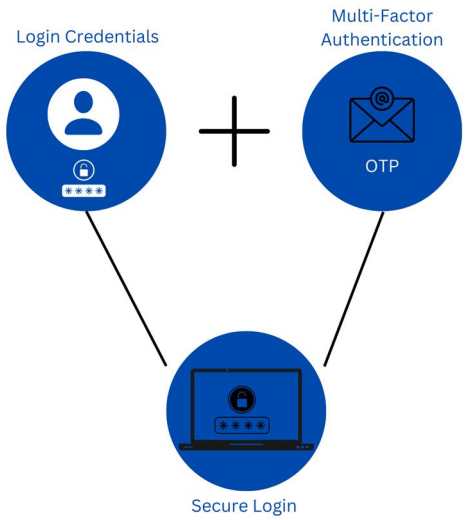


Fig. 3 How Multi Factor Authentication (MFA) works.

But most companies using MFA still got hacked.

F. Ecommerce Security Plugins

A very easy way to improve website security protection is by using security plugins. These plugins offer defence against numerous malicious bots that attackers may occasionally introduce. Astra is among the most reliable and feature-rich security plugins. Your website will become more secure as a result, and software will be added to stop malicious requests.

G. Providing Client Education

There may not always be security concerns on our end, but clients may use passwords that are too simple or may divulge private information to a website that is under the control 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 you should try to monitor each and every action that takes place there. Regular data scanning should be taken into consideration so that any errors may be fixed quickly.

I. Some good bots can be installed on the website.

That can be classified as below:

1) Monitoring Bots: Bots that are used to check the websites' uptime and system health. These bots examine and report on page load times, downtime length, and status on a regular basis.

2) Partner Bots: Bot partners who perform chores, conduct transactions, and offer crucial business services are helpful to websites. eg. PayPal IPN

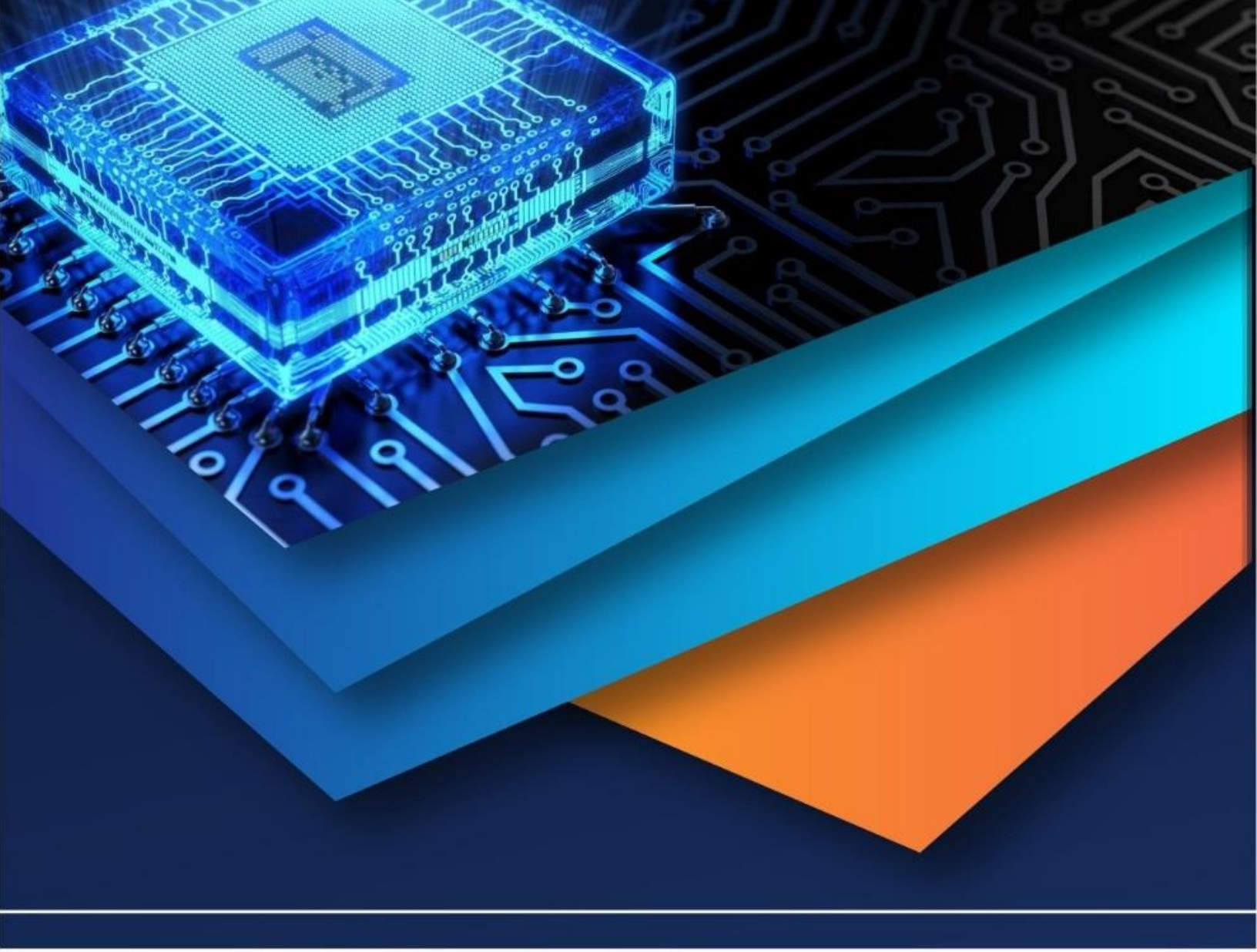
3) Search Engine Crawler Bots: In order to make web pages accessible on search engines like Google, Bing, etc., these bots or spiders crawl and index web pages. You may manage their crawl rates and set guidelines for these crawlers to adhere to when indexing your web pages in the "robots.txt" file on your website.

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 with 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