International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 8.141
Peer Reviewed Bi-Monthly
Vol. 6 No. 22 March - April - 2025

Securing the Digital Marketplace: Cybersecurity Challenges and Solutions for E-Commerce Platforms

Trupti Gaikwad[1], Mohini Vaidya[2], Rupali Yeshi[3]
[1,2,3] *Assistant Professor, Haribhai V. Desai College of Arts, Science and Commerce, Pune*
Corresponding Author – Trupti Gaikwad
DOI - 10.5281/zenodo.15502108

Abstract:
Global trade has been revolutionized by e-commerce, which offers smooth online transactions. However, because of this quick digital shift, fraudulent individuals now target online marketplaces. Business integrity and customer trust are at threat from safety risks like phishing attacks, financial fraud, and data breaches. In order to strengthen digital transactions against new cyber threats, this paper examines the cybersecurity issues that e-commerce platforms confront and proposes novel approaches, such as Multi Factor authentication, Secure Socket Layer (SSL), and Web Application Firewall etc. The research also covers standards for cybersecurity, emerging technology, and legislative frameworks that will impact the security of digital marketplaces in the future.

Keywords: E-Commerce, Cybersecurity, Challenges, Cyberattacks, Threats

Introduction:

As sensitive financial and personal information is involved in online transactions. The exponential growth of e-commerce has increased cybersecurity issues. Business operations, consumer trust, and regulatory compliance are all at risk from cyber threats. Effective risk-minimization techniques, strong cybersecurity frameworks, and modern encryption technologies are necessary for protecting the digital economy. In this paper new cybersecurity threats and novel methods to protect online transactions in e-commerce are reviewed. It also emphasizes the significance of using next-generation security technologies and adhering to regulations in creating a robust e-commerce environment.

Cybersecurity Challenges in E-Commerce Platforms:

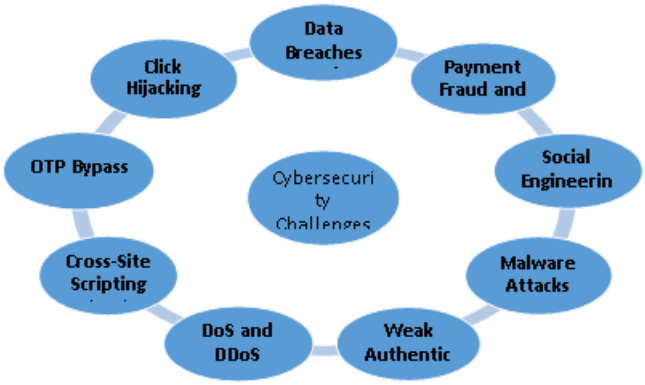

Fig. 1: Cybersecurity Challenges in E-Commerce Platforms

1) Data Breaches and Identity Theft: Unauthorized persons intruding into databases, networks or computers in order to obtain private information is known as a data breach. Financial records, property rights, private information and all other protected information which turns up in the wrong hands is considered breached data. A data breach can have serious consequences, including monetary losses, harm to a person's reputation, legal implications and possible harm to victims. Individual customers, small organizations and even big international corporations might all fall under this category.

2) Payment Fraud and Transaction Security: E-commerce is gravely endangered by chargeback abuse, card-not-present (CNP) fraud and unauthorized transactions. Cybercriminals use tactics like credential injection and MITM (man-in-the-middle) attacks to intercept payment details. Traditional fraud identification approaches are not any longer effective due to the rise of deepfake technology, which has additionally rendered fraudulent account takeovers possible. In addition, marketplaces on the dark web make it easier to trade credentials that were actually stolen, making fraudulent transactions more prevalent.

3) Social Engineering Attacks: Social engineering refers to a broad range of manipulation techniques that allow an attacker to manipulate victims and persuade them to either exchange private information, credit card numbers or login credentials. Attackers conduct activities that damage security, such as clicking on a file that installs malware. The following methods are frequently employed in combination by criminals attacking e-commerce clients using social engineering:

- Phishing: Phishing is the practice of an attacker misrepresenting a trustworthy company or organization in order to send consumers misleading emails or communications. Phishing is an approach used by attackers to fool victims into disclosing credit card numbers or passwords followed by attackers accessing the account and start purchasing.
- Pretexting: This technique comprises generating an incident or pretext in order to mislead the customer into disclosing their information. For example, an intruder may pretend to be a member of the customer service department and ask a client to provide details about their accounts.
- Baiting: This method of social engineering attracts the victim with the promise of a reward (such a discount or giveaway). For instance, an attacker could encourage a victim to check in to a fraudulent duplicate website that steals login information after sending one of clients a fake giveaway as a reward.

4) Malware Attacks: Any software intended to harm, interfere with, or obtain unauthorized access to a system is known as malware or malicious software. The following malware categories are the most dangerous for e-commerce websites:

- Credit card skimmers: These criminals attack online stores in an attempt to obtain customers' credit card information. Usually, this kind of virus affects the website's checkout or payment page. Payment form data is gathered by a skimmer, which then provides the hacker with the sensitive information.
- Rootkits, backdoors, and remote access trojans (RATs): These malware permits unauthorized users access to a hacked website. Later logged in, hackers take over the website and install more harmful spyware, alter content or steal data.
- Keyloggers: This kind of malware collects user keystrokes. If a customer becomes a victim of a keylogger, the

application will record credentials and offer an intruder with the login details.

- Ransomware: Ransomware poses an imminent danger to all sectors of the economy, including e-commerce. Files are encrypted by this kind of virus and the attacker then requests payment to deliver a decryption key.

5) Weak Authentication and Access Control: E-commerce platforms are prone to account takeovers and illegal data access due to insufficient authentication procedures. Exploitable security holes are generated by poor session management, weak password policies, and the lack of multi-factor authentication (MFA). Client accounts are further placed in danger by credential stuffing attacks which are supplied by stolen login credentials from prior breaches. Furthermore, users are more vulnerable to identity theft due to insufficient session expiration restrictions and the reuse of credentials across multiple sites.

6) DoS and DDoS Attacks: Denial of Service (DoS) and Distributed Denial of Service (DDoS) assaults is a threat where actors can overwhelm a website with an excessive amount of traffic. Malware networks which are infected machines with malicious software used by intruders to perform attacks. These attacks often result in interruptions, making the website unavailable to users for a long duration. Since customers have no way to visit the online shop, it leads to an interruption in revenue. Due to frequent interruptions customers begin to use other service providers. Additionally unsatisfied customers frequently post their online negative experiences which harms the website's image furthermore.

7) Cross-Site Scripting (XSS): Whenever attackers inject harmful scripts into an e-commerce website that other users view, this is known as cross-site scripting (XSS). Attackers may deploy spyware and scripts that can steal sensitive information, take over user activities, or reroute users to hostile domains when a web page fails to validate input from users. Eventually, it will result in financial loss and information theft.

8) OTP Bypass: It is one of the most recent security threats in e-commerce. This threat occurs at the moment where attackers attempt to get around OTP for user authentication. Here, the OTP is delivered to the user's registered email address or mobile number during the authentication process. It gets intercepted or altered by the attacker. Hackers can obtain unauthorized access to user accounts by taking advantage of flaws in OTP delivery or validation. Hackers thus have the capability to carry out fraudulent activities or acquire private information.

9) Click Hijacking:

In order to misguide a user intruder, hide a malicious element on a page with a defected link. The defected link has unexpected actions like modify the account's settings, put a product in a shopping cart and carry out an illegal transaction.

Solutions to Cybersecurity Challenges:

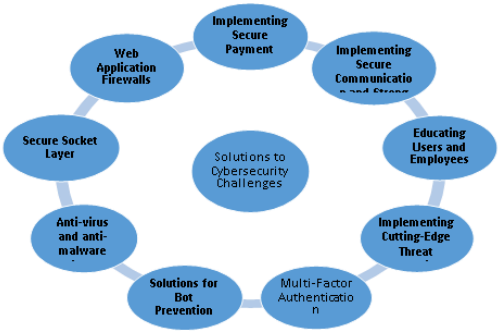

Fig.2: Solutions to Cybersecurity Challenges

1) Implementing Secure Payment Processing:

It protects consumer financial data while performing online transactions. This measure is essential for the security of e-commerce. It allows you to safeguard private information, preserve the confidence of clients, and observe industry rules. E-Commerce websites use Third-party payment gateways to process online payments. Gateways serve as bridges between financial institutions and websites. Use a secure payment processing solution that provides the following characteristics to protect the gateway:

- Data in transit encryption that ensures all payment data remains safe during transmission.
- Tokenization: It replaces sensitive payment card data with unique identification tokens to reduce the risk of storing sensitive data on the server.
- Address Verification Service (AVS)- It verifies whether the billing address matches the one associated with the credit card.
- Biometric verification: This method is used for high-value transactions. It improves payment security by decreasing reliance on static authentication methods.
- AI-powered fraud detection systems: It examines transaction patterns and detects anomalies in real-time.

2) Implementing Secure Communication and Strong Encryption into Practice:

Unauthorized data interception is avoided by using secure transmission protocols, such as TLS 1.3, and end-to-end encryption. Homomorphic encryption and quantum-resistant cryptographic techniques provide enhanced protection against emerging decoding threats. Communication security among digital platforms has been enhanced via secure API architecture, including OpenID Connect and OAuth 2.0. By integrating cloud-based security services with VPN and firewall characteristics, the implementation of Secure Access Service Edge (SASE) frameworks enhances network security.

3) Educating Users and Employees:

To stop malicious social engineering attacks cyber security awareness training is necessary. AI-powered security education tools replicate phishing attempts to teach staff and customers how to identify fraudulent schemes. The probability of effective cyberattacks decreases via behavioural-based security training. It improves retention and response times. Excitement of security training courses promotes user participation and strengthens digital safety best practices.

4) Implementing Cutting-Edge Threat Detection Technologies:

Intrusion detection systems (IDS) with machine learning capabilities examine network activity to spot irregularities and possible dangers. SIEM (security information and event management) systems provide real-time threat visibility by combining threat intelligence from many sources. Ethical hacking and automated red teaming mimic cyberattack to evaluate a platform's resistance to emerging threats. By integrating endpoint, network, and cloud security monitoring, extended detection and response (XDR) technologies improve threat hunting capabilities.

5) Multi-Factor Authentication:

A customer must present two or more forms of identification in order for MFA to authenticate their identity. In this manner, even if an attacker manages to get someone's login and password (for example, through a data breach or phishing attempt), it will be more difficult for them to achieve illegal access.

This is how MFA usually operates:

1) To access their account, the user inputs their username and password.
2) After successful valid credentials, the platform prompts the user for a second form of authentication.

The second step in the MFA process can be one of the following:

- Hardware tokens.
- Biometric factors such as fingerprint or facial scanning.
- Onetime password tokens: The user receives through a text message, email, or mobile app.
- Push notifications on the registered mobile device.
- Security questions.

6) Solutions for Bot Prevention:

These activities are a serious threat to e-commerce websites like account takeover attempts, credential stuffing, brute force assaults, inventory scalping, content scraping, DDoS attacks, etc. Use a prevention tool to identify and stop harmful bot activity.

To prevent threatening bots, the majority of bot avoidance systems combine the following strategies:

- Rate restriction.
- CAPTCHA difficulties.
- Behaviour analysis (such as surfing habits, session length, and mouse movements).
- Fingerprinting of devices.

7) Anti-virus and anti-malware software:

Anti-virus and anti-malware software safeguards both the end-user devices that use the platform and the underlying architecture of e-commerce websites. These programs assist in preventing viruses and other cyber threats that may compromise customer information by infecting servers which also includes Trojan horse, worms, Keyloggers, Ransomware, Spyware, and Adware. In addition, these solutions have anti-phishing features to protect users from scams involving hacked accounts.

8) Secure Socket Layer (SSL):

The communication between a user's browser and a web server is safeguarded by this encryption protocol. SSL makes assurance that no data is intercepted or altered by unauthorized parties. An SSL certificate from a recognized certification authority (CA) is required inorder to use SSL encryption. SSL certificates come in a variety of forms, such as

- Domain Validation (DV) certificates.
- Certificates of Organization Validation (OV).
- Certifications for Extended Validation (EV).

Frequently update SSL certificates and set up web servers which require HTTPS (HTTP over SSL/TLS) connections. Additionally, HTTPS will improve E-Commerce website's Google ranks.

9) Web Application Firewalls (WAFs):

It protects web applications from unauthorized access and attacks. It plays mediator between server and internet. It performs following tasks:

- Examine requests.
- Implement security regulations.
- Stop harmful traffic.

WAFs are essential for e-commerce websites for the following reasons:

- WAFs stop unwanted access attempts and block malevolent users.
- Cross-site request forgery (CSRF), XSS attacks, and SQL injections are just a few of the e-commerce security risks that WAFs successfully stop.
- Granular inspection capabilities for HTTP/HTTPS traffic are offered by WAFs.
- The majority of WAFs provide DDoS protection features that use rate-limiting questionable traffic to identify and stop assaults.
- A WAF aids in meeting PCI DSS compliance standards.

Because WAFs have real-time monitoring and logging capabilities, they are capable of detecting and responding to suspicious activity quickly.

Conclusion:

Threats to e-commerce security are a recurring worry in this quickly changing cyber environment. It includes protecting networks, computer systems, and private data from theft, damage, and unwanted access. Cyberattack risks and hazards have escalated along with our growing reliance on technology and the internet. Malware, phishing, hacking, ransomware, and other types of attacks can all be used to seriously harm people, companies, and even governments. Because of this, e-commerce security is not only necessary, but also an investment for establishing credibility and ensuring the sustainability of an organization. To overcome cyberattacks, techniques like Firewalls, antivirus software, encryption, strong passwords, frequent backups and staff training can be used. Technologies, regulations, and practices are all part of effective defence against cybersecurity threats. It is also necessary to stay up-to-date with the latest threats, vulnerabilities and also regularly monitor the effectiveness of security solutions.

References:

1. https://phoenixnap.com/blog/ecommerce-security-threats
2. https://medium.com/@zomev/top-ecommerce-security-threats-and-how-to-deal-with-them-a6de2ad432bd
3. What is Cybersecurity? Types, Threats and Cyber Safety Tips (kaspersky.co.in)
4. https://www.ijser.org/researchpaper/Cyber-security-in-E-commerce.pdf
5. Ecommerce Security – How to Prevent Cyberattacks (qualysec.com)
6. (PDF) Cyber security threats: A never-ending challenge for e-commerce (researchgate.net)
7. (PDF) THE CHALLENGES FOR CYBER SECURITY IN E-COMMERCE (researchgate.net)
8. (PDF) Cybersecurity Threats in E-Commerce: Trends and Mitigation Strategies (researchgate.net)
9. 69-o-Niranjanamurthy -The study of E-Commerce Security Issues and Solutions.pdf (ijarcce.com)
10. (PDF) ECOMMERCE AND ONLINE SECURITY (academia.edu)