International Conference on Role Of Digital Transformation in Commerce: Leveraging Technology for Sustainable Growth, 4 Sep, 2025

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Role of Cyber Security in Protecting E-Commerce Platforms

Mrs.P.Thavamani, Assistant Professor in Computer Science of M.Com (CA), Sri Vasavi College (Self Finance Wing), Erode - 639316.
Mrs.P.Jeevitha, Assistant Professor in Computer Science of M.Sc.(Computer Science), Sri Vasavi College (Self Finance Wing), Erode - 638316.

Abstract- Cyber security is now a major concern for people, companies and governments worldwide due to extensive use of digital technology and the internet. Cyber security protects computer system from information discloser, misdirection, damage or theft of electronic data, software or hardware. In e-commerce, it is all about electronic security related to e-commerce activity. e-commerce platforms have prime target for cyber threats, posing significant risk to business and consumers. The integrity, privacy and safety of customers and e-commerce business is essential to safeguarding the Cyber security. In this paper we use techniques for security purpose in detecting, preventing and predicting the cyber-attack. The study provides a comprehensive understanding of how these threats affect the different sectors within e-commerce.

Keywords- Cyber security,Digital technology,Internet security,E-commerce security,Cyber threats,Data protection.

I. INTRODUCTION

The cyber security is a crucial aspect of modern society that aim to protect computer system network and sensitive data from unauthorized access. In order to protect the integrity, privacy and safety of consumer and E-commerce enterprises cyber security place an essential role. The organizations and individuals must have a variety of security measure such as firewalls, antivirus software, encryption and strong password to reduce the risk associated with cyberthreats. To guard against emerging vulnerabilities, it is necessary to keep up with the most resent threats and to upgraded systems and software.

II. TYPES OF CYBER SECURITY

There are many different types of cybersecurity, each of which focus on protecting different aspects of computer systems and networks. Here are some of the most common types of cybersecurity.

- Network Security: The security focus on protecting computer networks from unauthorized access or attacks, as viruses, malware, and denial of service attack.
- Cloud Security: The security focuses on protecting data and applications that are hosted in the cloud from unauthorized access or attack.
- Mobile Security: The Security focuses on protecting mobile devices and their data from security threats, such as malware, data breaches and hacking.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

- Internet of Things (IoT) Security: The security focuses on protecting the growing number of connected devices that make up the Internet of Things, such as smart home devices, medical devices and industrial control systems.
- Application Security: The security focuses on protecting software application from vulnerabilities that could be exploited by hackers.
- Cryptography: The security focuses on protecting data by using encryption techniques to prevent unauthorised access or interception of sensitive information.

III. CYBER SECURITY CHALLENGES IN E-COMMERCE

- Payment Fraud: Payment fraud is one of the most significant cybersecurity challenges faced by e-commerce businesses. Fraudsters use stolen credit card details to make unauthorised purchases, Payment fraud can be divided into two categories: account takeover fraud and card not present fraud.
- Phishing attacks: Phishing attacks are common in e-commerce and they involve tricking customers into divulging their personal information, such as login credentials, payment card details and sensitive information. Phishing attacks are usually carried out via email, social media, or SMS
- Ransomware: Ransomware is malicious software that can cause irreparable damage to our data and computer. It revokes our data to access by locking the device by itself or encrypting the files stored on it.

IV. IMPACT OF THREATS IN E-COMMERCE

- Financial Losses: Cyberattacks can result in direct financial loss through fraud, chargebacks and the cost of remediating breaches. Downtime from attack also causes lost income.
- Reputation Damage: Security breaches that compromise customer trust and lead to negative publicity, reduced customer loyalty and a damage brand image
- Legal and Compliance Issues: Failure to protect sensitive customer data can lead to significant fines and lead to negative publicity, reduced customer loyalty and a damaged brand image.
- Loss of Customer Trust and Loyalty: When customer financial or personal data is compromised, they become wary of platform, leading to distrust and a decline in customer retention.
- Operational Disruption: Threats like DDoS attack can overwhelm a website's server leading to crashes and making the site unavailable, which directly impact sales.
- Market Share Loses: A poor reputation combined with operational failures can lead customer to switch to competitors, impacting market competitiveness.

V. OVERCOME THE CHALLENGES IN CYBER SECURITY

Cyber security has to processes the comprehensive strategies that demand continual attention and continuous reinforcement, employing solutions like two-factor authentication, alerts far malicious activity, encryption algorithm, and safe password practice will help to keep cyberspace safe. Regularly assess vulnerabilities through audits and penetration testing, adopt a zero-trust model, and leverage threat intelligence to continuously adapt the defence against evolving threats. These steps not only help to achieve compliance but also lay the foundation for a culture that prioritizes security over anything.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

VI. CYBER SECURITY AWARENESS

- Cyber security awareness refers to the understanding and knowledge about potential cyber threats and how to handle them.
- It involves recognizing the various types of cyber threats, such as phishing, malware, ransom ware, social engineering attacks,
- By awareness of these threats and knowledge of responding to then, individuals and organizations can better protect the sensitive information and systems from being compromised.
- Implementation of practice and regularly conducting penetration testing, training employees on phishing, social engineering and educating customers on secure online habits

VII. CONCLUSION

Cyber crimes have started to make a fear in the minds of many people connected to the networks mostly worried to ecommerce technology as its success lies in the internet. The various mechanisms used for securing web-based transactions or communications can be grouped into authorization, authentication, integrity and privacy are necessary to safe guard the present success of ecommerce. It is also essential to stay up-to-date with the latest threats and vulnerabilities and continuously monitor and evaluate the effectiveness of security measures. Overall, cybersecurity is a critical issue that requires constant attention and proactive measure to ensure the safety and security of our digital world.

REFERENCES

1. R. Nagalakshmi, Dr. P. Yashoda" Cyber Security in E-commerce" International journal for Multidisciplinary Research (IJFMR)
2. Dr. Nupur Saboo, "Cyber Security concern in E-Commerce" International journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS)
3. Dr. Ruchi Gupta," Cybersecurity threats in E-commerce: Trends and Mitigation Strategies" Journal of Advanced Management Studies.