iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80961

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 14 Issue IV Apr 2026- Available at www.ijraset.com

Cybersecurity Risks in Online Shopping: Challenges, Solutions, and Future Directions

Ms. P. D. Toraskar[1], Ms. A. S. Mardhekar[2].
Karmaveer Bhaurao Patil Polytechnic, Satara.

Abstract: ***Online shopping has become a major aspect of daily life. It offers convenience, a wide range of products, and cost savings to consumers. However, this growth has increased cybersecurity risks. Online shoppers and businesses face numerous threats, including phishing, payment fraud, data breaches, malware, and fake websites. This study clarifies the main cybersecurity risks associated with online shopping, examines current security solutions, and discusses their strengths and weaknesses. It also highlights the future trends in cybersecurity. The study concludes that multiple layers of security, such as encryption, authentication, and smart monitoring systems, are necessary to make online shopping safe and reliable.***
Keywords: Online Shopping, Cybersecurity, E-Commerce, Digital Payments, Data Privacy, Cyber Fraud.

I. INTRODUCTION

Online shopping has changed how people buy goods and services. With easy Internet access and digital payment options, many people prefer shopping online rather than visiting physical stores. However, this convenience comes with certain risks. Online platforms store sensitive information, such as personal details and payment data, making them attractive targets for cybercriminals.

Cyberattacks can cause financial loss, damage a company's reputation, and result in a loss of customer trust. For businesses, especially in management studies, understanding cybersecurity is important for their long-term success.

This study focuses on identifying key risks and suggesting effective solutions to improve security in online shopping.

II. LITERATURE REVIEW

Previous research has described that cybercrime is increasing along with the growth of e-commerce. Common threats, such as phishing and payment fraud, occur mainly because of low user awareness and weak security systems. Studies have also revealed that data breaches reduce customer trust and impact business performance.

Recent research suggests that technology alone is insufficient. Cybersecurity also requires user awareness, appropriate management policies, and strong governance. New technologies, such as Artificial Intelligence, blockchain, and biometric authentication, are promising; however, they also come with challenges, such as high prices and complexity.

This study combines these ideas to provide a clear understanding of the risks, solutions, and future developments.

III. MAJOR CYBERSECURITY RISKS IN ONLINE SHOPPING

A. Phishing Attacks

Phishing involves fake emails, messages, or websites that appear real and trick users into sharing their personal information.

Risks:

Theft of login credentials

Unauthorized account access

Financial fraud

B. Payment Card and Digital Wallet Fraud

Hackers steal card details or wallet information using insecure systems or infected devices.

Risks:

Loss of money

Extra charges and penalties

Legal issues

C. Data Breaches

Online platforms store large amounts of customer data, which can be stolen by attackers.
Risks:
Exposure of personal information
Violation of privacy laws
Loss of customer trust

D. Malware and Ransomware

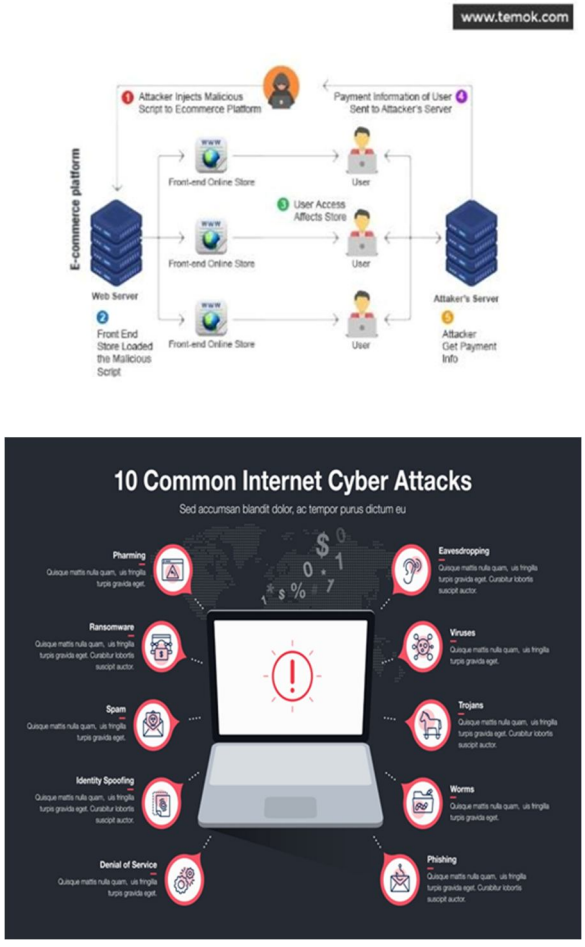
Malware can damage systems, whereas ransomware locks data and demands money to unlock it.
Risks:
Disruption of business operations
Loss of important data
High recovery costs

E. Man-in-the-Middle (MITM) Attacks

These attacks occur when hackers secretly intercept communication between users and websites.
Risks:
Data theft or modification
Session hijacking

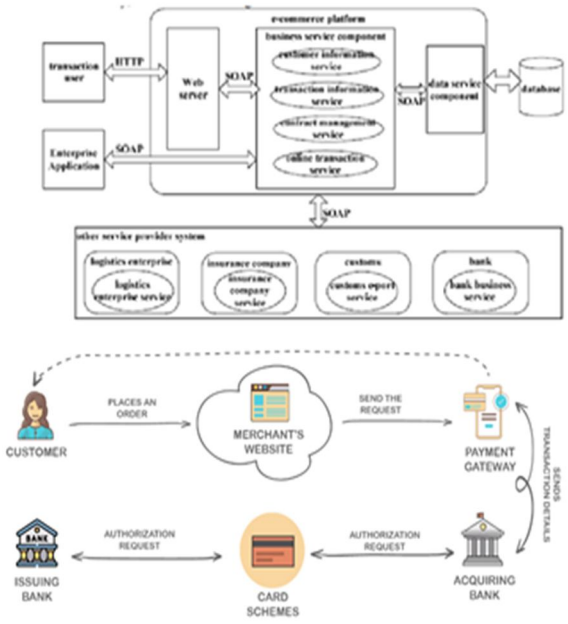
IV. CYBERSECURITY FRAMEWORK FOR ONLINE SHOPPING

Figure 1: Cybersecurity Threat Landscape in Online Shopping



This figure illustrates common cyber threats targeting online shopping platforms, including phishing, malware, payment fraud, and data breaches.

Figure 2: Secure Online Shopping Architecture



The architecture demonstrates how SSL/TLS encryption, secure servers, authentication layers, and payment gateways work together to protect transactions.

V. EXISTING CYBERSECURITY SOLUTIONS

1) Encryption (SSL/TLS): Protects data during transmission between users and websites.
2) Two-Factor Authentication (2FA): Requires users to verify their identity with an additional step, such as OTP or biometrics.
3) Tokenization: Sensitive payment data are replaced with secure tokens.
4) AI-Based Fraud Detection: It uses machine learning to detect unusual or suspicious activities in real time.

VI. COMPARISON OF SECURITY TECHNOLOGIES

Technology	**Advantages**	**Limitations**
SSL/TLS	Keeps data secure during transfer	Cannot stop phishing attacks
2FA	Provides strong security	It may be inconvenient for users
Tokenization	Protects payment data	Costly to implement
AI Systems	Detects fraud quickly	Needs high-quality data

VII. BENEFITS OF STRONG CYBERSECURITY

Builds customer trust
Reduces financial losses
Ensures legal compliance
Improves company reputation
Supports long-term business growth

VIII. CHALLENGES AND LIMITATIONS

High cost of advanced security systems
Increased complexity in implementation
Users may resist extra security steps
Lack of skilled cybersecurity professionals

IX. FUTURE SCOPE

Cybersecurity in online shopping will continue to evolve with new technologies such as:
i) Artificial Intelligence for predictive security
ii) Blockchain for secure transactions
iii)Biometric authentication (fingerprint, face recognition)
iv) Zero Trust security models
v) Advanced encryption methods resistant to future threats

X. CONCLUSION

Cybersecurity is a major concern in online shopping because of increasing cyber threats. Attacks such as phishing, fraud, data breaches, and malware affect both consumers and businesses.

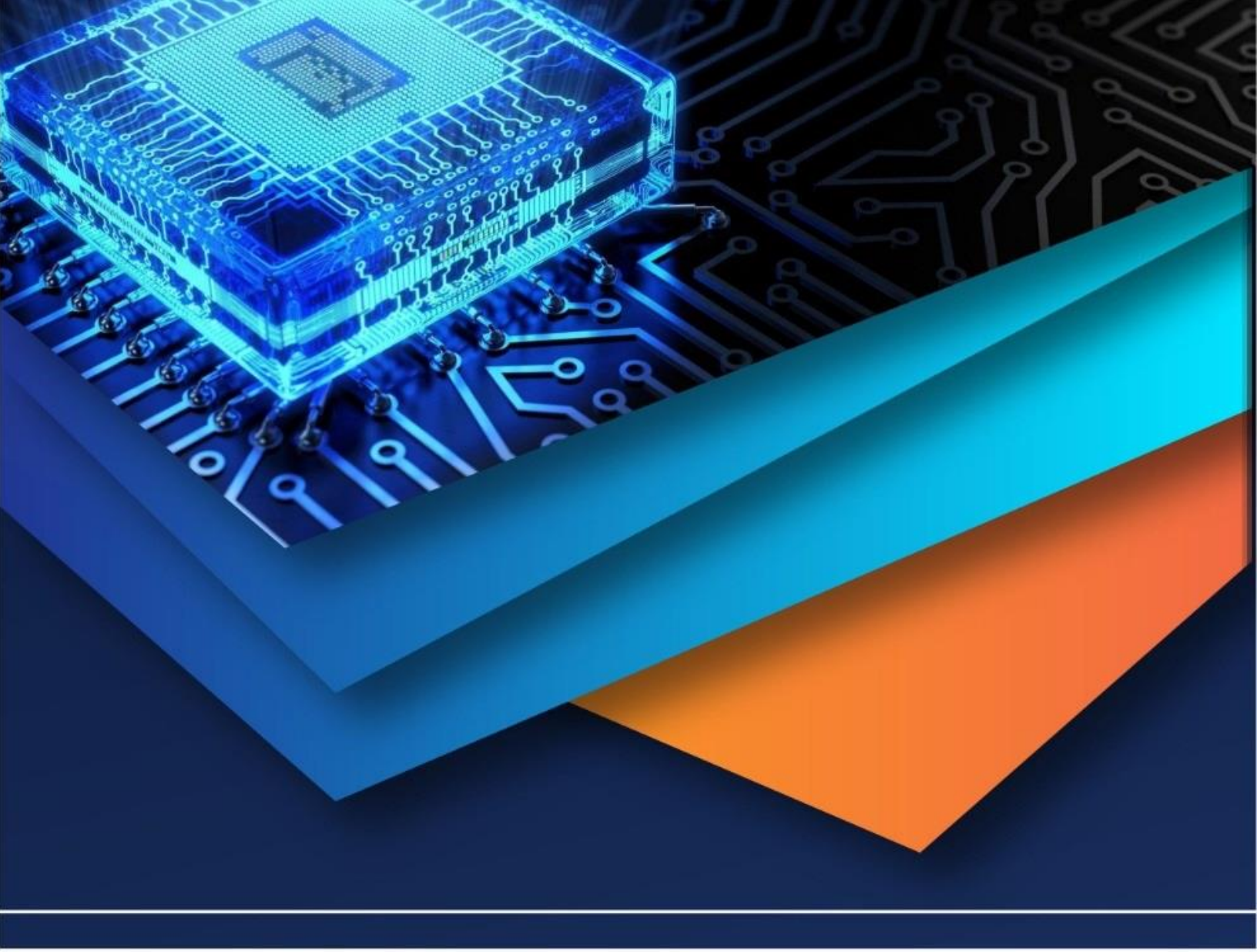
The best approach to security is a multilayered system that includes encryption, authentication, tokenization, and intelligent monitoring. From a business perspective, cybersecurity is not just a technical issue; it is essential for maintaining trust, ensuring safety, and achieving long-term success.

XI. ACKNOWLEDGEMENT

A secure online shopping system uses multiple layers of protection, including Secure communication through encryption, Strong authentication methods,
Safe payment gateways, Continuous monitoring of suspicious activities
This layered approach helps to reduce risks and ensure safe transactions.

REFERENCES

[1] Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
[2] Laudon, K. C., & Trever, C. G. (2022). E-commerce: Business, Technology, Society. Pearson.
[3] OECD. (2021). Consumer strategies and scams in online markets. OECD Publishing.
[4] ISO/IEC. (2018). ISO/IEC 27001: Information Security Management Systems.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY