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

Cyber Security Frameworks for E-Commerce Enterprises

Mrs.M.Brindha, Assistant Professor in Department of English Language, Sri Vasavi College (Self Finance Wing), Erode - 638316.
Mrs.S.Shanmugapriya, Assistant Professor in Department of English Language, Sri Vasavi College (Self Finance Wing), Erode - 638316

Abstract- In today's rapidly changing digital landscape, e-commerce platforms have become prime targets for cyber threats, posing significant risks not just to businesses but also to consumers. This paper delves into the most pressing cybersecurity threats facing e-commerce and outlines the current trends in these dangers. It highlights key categories of threats identified by the authors, including phishing attacks, malware, data breaches, and insider threats, emphasizing their increasingly sophisticated and destructive nature. The discussion also addresses major issues in cybercrime, such as the misuse of artificial intelligence and machine learning by criminals, the security vulnerabilities introduced by Internet of Things (IoT) devices, and how evolving regulations impact these threats. By providing a thorough understanding of how these risks affect various sectors of e-commerce, the research reveals challenging cases and industry-specific threats highlighted in recent news. To effectively navigate this shifting threat landscape, the paper outlines a range of mitigation strategies. It discusses technical solutions like encryption, secure payment gateways, and intrusion detection systems, alongside organizational practices such as employee training, incident response planning, and access control policies. Additionally, the paper raises the important issue of "business legal and regulatory obligations," stressing the need for companies to comply with regulations like GDPR and CCPA, echoing the sentiment found in the King James Version of the New Testament. Finally, it explores the importance of collaboration and information sharing within the industry, as these efforts can significantly enhance the collective cybersecurity measures.

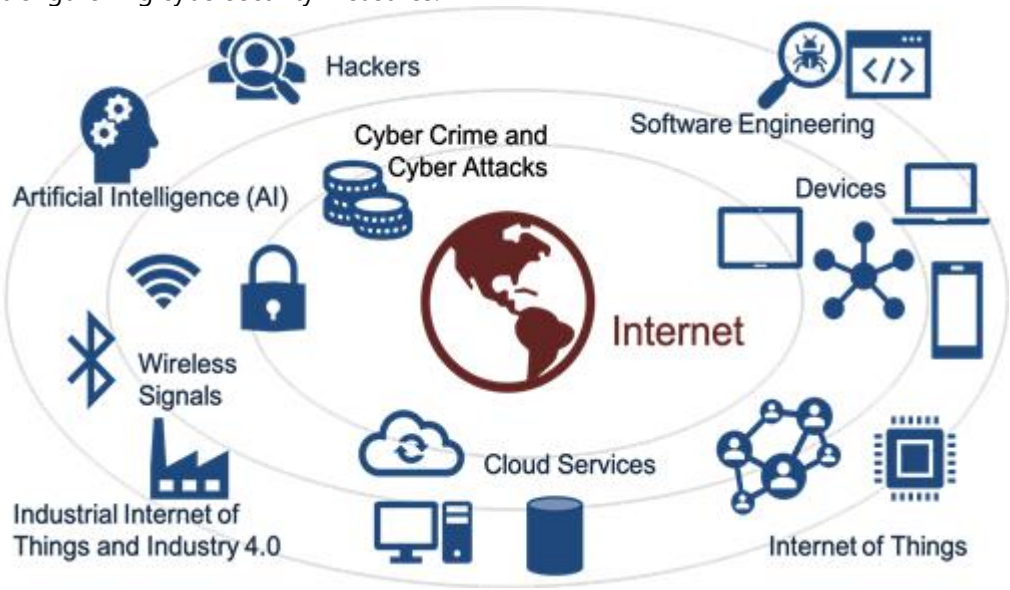
Keywords: Cybersecurity, E-Commerce, Cyber Threats, Phishing Attacks, Malware, Data Breaches, Insider Threats, Encryption.

I. INTRODUCTION

In our fast-paced digital world, e-commerce has taken off like never before, completely changing the way businesses and consumers connect and make purchases. But with this incredible growth comes a whole new set of challenges, particularly when it comes to cybersecurity. E-commerce platforms have become prime targets for cybercriminals looking to exploit any weaknesses they can find. The landscape of cyber threats is constantly evolving, making it tough to protect sensitive information and ensure that online transactions remain secure. From big-name retailers to small online shops, everyone is at risk of facing various cyber threats. These include phishing scams that trick users into giving away personal details, malware that can wreak havoc on systems and steal data, and data breaches that expose confidential information. On top of that, insider threats and advanced ransomware attacks add even

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

more complexity to the cybersecurity scene. This paper aims to give a thorough look at the current trends in cybersecurity threats affecting the e-commerce industry and to discuss effective strategies for mitigating these risks. We'll dive into emerging issues, like how cybercriminals are increasingly using artificial intelligence and the vulnerabilities that come with the rise of Internet of Things (IoT) devices in e-commerce. We'll also touch on how changing regulations impact cybersecurity practices and the unique threats different e-commerce sectors face. By examining recent high-profile security breaches and successful mitigation case studies, this paper will provide practical recommendations for strengthening cybersecurity measures.



II. THE SCOPE OF CYBERSECURITY

1.System and Network Protection:
This involves keeping our computer systems, mobile devices, networks, and other digital assets safe from harm, unauthorized access, and various attacks.

2.Data Protection:
It's all about safeguarding data in every form—whether it's being stored, sent, or processed—to stop it from being stolen or misused.

3.Incident Response:
This is about crafting strategies and systems to tackle security incidents, manage crises effectively, and bounce back from attacks.

4.Application Security:
Here, we focus on securing web-based applications, which are often prime targets for attackers, to prevent any vulnerabilities from being exploited.

5.Critical Infrastructure Security:
This ensures the safety and resilience of essential national infrastructure, like power grids and financial systems, which are becoming more and more digital.

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

III. OBJECTIVES OF CYBERSECURITY

1.Confidentiality:
This means keeping sensitive information under wraps, only allowing access to those who are authorized. Techniques like encryption and multi-factor authentication help us achieve this goal.

2.Integrity:
We want to make sure that our digital data is spot-on, complete, and safe from any unauthorized changes or corruption.

3.Availability:
It's all about making sure that information and systems are up and running when we need them, so operations can keep flowing smoothly without any hiccups.

4.Risk Mitigation:
Here, we focus on reducing the overall risks that come from cyber threats, like data breaches, fraud, and ransomware attacks.

5.Resilience and Recovery:
We aim to equip systems and organizations with the ability to bounce back quickly from cyber incidents and withstand challenges.

6.Trust and Compliance:
Building trust among individuals and businesses is key, and that comes from ensuring data security while sticking to regulatory frameworks and global security standards.

IV. TYPES OF CYBER SECURITY

1. **Network Security:** Safeguarding your computer network from unauthorized access and other intrusions.
2. **Application Security:** Protecting software and devices from threats that exploit vulnerabilities.
3. **Information Security**: Protecting digital and physical data from unauthorized access, modification, or destruction.
4. **Cloud Security:** Protecting data, applications, and infrastructure in cloud computing.
5. **Endpoint Security:** Protecting the end-user devices such as desktops and smartphones from malicious activities.
6. **Mobile Security:** Protecting mobile devices and data on mobile devices from threats and vulnerabilities.
7. **Critical Infrastructure Security:** Protecting systems and networks that are essential to national security and the health, safety, and well-being of the public. (Includes power grids and financial systems).
8. **Operational Security (OpSec):** Identifying and protecting sensitive information through analyzing daily operations and activities.

V. CONCLUSION

In wrapping things up, tackling cybersecurity threats in the world of e-commerce calls for a well-rounded and proactive strategy. This means embracing cutting-edge technologies, solid organizational practices, and adhering to strict regulations. By examining recent incidents and the successful strategies used to counter them, we see that strong defenses rely on constant monitoring, thorough employee training, and flexible security measures. By taking lessons from high-profile breaches and applying tried-and-true methods, e-commerce businesses can enhance their protection of sensitive data, keep consumer trust intact, and reduce potential risks. As cyber threats keep changing, staying alert and innovating in cybersecurity practices will be crucial for protecting the digital economy and ensuring that e-commerce platforms remain resilient.

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

REFERENCE

1. Beyari, H. (2021). RECENT E-COMMERCE TRENDS AND LEARNINGS FOR ECOMMERCE SYSTEM DEVELOPMENT FROM A QUALITY PERSPECTIVE.International Journal for Quality Research, 15(3), 797–810. https://doi.org/10.24874/IJQR15.03-07
2. D'Adamo, I., González-Sánchez, R., Medina-Salgado, M. S., & Settembre-Blundo,D. (2021). E-Commerce Calls for Cyber-Security and Sustainability: How European Citizens Look for a Trusted Online Environment. Sustainability, 13(12), 6752. https://doi.org/10.3390/su13126752
3. Deligianni, F., & Robbins, S. (2024). Building a Robust Cyber Defense Strategy: Integrating AI-Driven Threat Mitigation and Blockchain Security in E-Commerce. Unpublished. https://doi.org/10.13140/RG.2.2.21587.80168