The topic of this report is cybersecurity in e-commerce platforms, focusing on the importance of a thorough strategy to prevent data breaches and the implementation of strong security measures, routine evaluations, and cybersecurity training for clients and staff.

## Abstract

In today's world of online shopping, cybersecurity is of utmost importance to avoid data breaches on e-commerce platforms. The risks of vulnerabilities in the system, such as third-party services, payment gateways, and authentication systems, require e-commerce companies to adopt a proactive approach to cybersecurity. This project focuses on building a secure website with user authentication and encrypted data storage using AES Algorithm.

## Introduction

The rise of e-commerce platforms has revolutionized the way people shop, and the online marketplace is growing at an unprecedented rate. With this growth comes a growing risk of data breaches and cyber attacks that can lead to reputational and financial harm for e-commerce businesses. It is crucial to implement a thorough strategy to prevent such data breaches, including strong security measures, routine evaluations, and cybersecurity training for clients and staff. This report highlights the importance of cybersecurity in e-commerce and focuses on a project that aims to build a secure website with user authentication and encrypted data storage.

## Ecommerce Project

The e-commerce project focuses on building a secure website with user authentication and encrypted data storage. The project includes a 3x3 photo grid and a question to which the user would answer in the text box displayed. The response would be validated against the answers stored in the database, and accordingly, a decision would be made whether the user should be allowed to access the website or not. A similar security approach would be implemented at Payment Gateway. All user details including personal information, address, and Payment Gateway details would be stored in the database using AES Encryption. The AES Algorithm is currently considered one of the most secure encryption algorithms, and it is fast and easy to implement.

## Findings & Results

The implementation of strong security measures and routine evaluations can prevent data breaches and cyber attacks on e-commerce platforms. By adopting a proactive approach to cybersecurity, e-commerce websites can safeguard the personal and financial information of their consumers, foster trust, and prevent reputational and financial harm. The project focused on building a secure website with user authentication and encrypted data storage using the AES Algorithm, which is considered one of the most secure encryption algorithms.

## Conclusion

In conclusion, cybersecurity is of utmost importance for e-commerce platforms, and a thorough strategy is required to avoid data breaches. By putting in place strong security measures, carrying out routine evaluations, and giving clients and staff continual cybersecurity training, e-commerce businesses can prevent data breaches and cyber attacks. The project aimed to build a secure website with user authentication and encrypted data storage using the AES Algorithm. By implementing such a strategy, e-commerce businesses can safeguard the personal and financial information of their consumers, foster trust, and prevent reputational and financial harm.

References

1. H. Qin, et al. (2018). A Comprehensive Study of Cybersecurity of E-commerce Systems. Journal of Information Security, 9(1), 16-25.
2. A. Ozsoy, et al. (2020). Cybersecurity Strategies for E-Commerce Websites. International Journal of Computer Science and Network Security, 20(2), 89-96.
3. N. O. Al Zadjali, et al. (2021). A Comprehensive Review on E-commerce Security Issues and Challenges. International Journal of Emerging Trends & Technology in Computer Science, 10(4), 327-332.
4. J. G. Kim, et al. (2019). E-commerce Security: Trends and Challenges. International Journal of Computer Science and Network