The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 3, March 2025
PP 92–99

A Survey of Cyber Security Threats and Protective Measures in E-Commerce

A. Nagabhushan Rao [1], Koyya Sravanthi[2], Datla SivajiVarma[3], Chilla AravindReddy[4], Abburu Akshith[5]
[1,2,3,4,5] Department of Computer Science and Engineering,
Nadimpalli Satyanarayana Raju Institute of Technology, Visakhapatnam
Andhra Pradesh, India
Corresponding Author *: Koyyasravanthi123@gmail.com

Abstract

Cyber threats are any possible harm or malevolent activity that targets computer networks, systems, or digital data with the intention of causing damage, stealing information, or interfering with services. E-commerce is the short term for electronic commerce, purchasing and selling goods and services online. It involves internet exchange between companies, customers, or other companies. Many cyber threats can threaten the e-commerce companies and consumers. Phishing is the false practice of using phony emails or websites to dupe consumers into revealing private information. Ransom ware encrypts or locks files and then demands to unlock them, whereas malware refers to malicious software meant to invade computers and compromise private information.

Keywords: Cyber Security, E-Commerce, Online Shopping, Threats

1. Introduction

Businesses and consumers must put in place a comprehensive cyber security program to protect e-commerce platforms from the increasing danger of Cyberattacks like Ransomware, malware, and phishing. First and foremost, cutting-edge security tools such as Antivirus, anti-malware, and endpoint protection should be used by e-commerce sites to protect against Ransomware and malware. In order to ensure that the sensitive client and transaction information is not intercepted or stolen, data encryption—SSL/TLS for data in transit and encrypted storage for data at rest is considered a must. By adding another layer of security onto user accounts, multi-factor authentication (MFA) makes it tough for hackers to gain illegitimate access

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 3, March 2025
PP 92-99

2. Literature Survey

Kuruwitaarachchi et al. (2019) claimed that security worries regarding the growth of e-commerce platforms have been amplified by the fact that the global market is virtual and unknown. E-platforms need to adequately analyze the security threats that surround e-commerce in order to get rid of this barrier.

According to (Priyadarshini, 2019), who researched "Cyber security In Parallel And Distributed Computing," computer science is a constantly changing discipline that includes networks, data, software, and hardware. Ranging from Ransomware, a term that is used to imply ransomware, and others, more and more are being targeted by cybercrimes. It becomes incumbent upon responsible specialists in cyber security to protect such precious cyber infrastructures by incorporating relevant policies, guidelines, and procedures.

According to the study titled "Impact of data science and cyber security in e-commerce using machine learning techniques," by (Fatunmbi, 2022), this essay evaluates the growth of online sales from the aspect of how data science and cyber security change companies. Machine learning algorithms facilitate information security enhancements, pricing strategies, stock organization, and customer-related insights.

.

3. Methodology

This technique provides a structured approach toward analysis and evaluation of the e-commerce industry's cyber threats and defences. There is a strong focus on total data gathering, methodological categorization, comparative evaluation, and fair judgment about the existing solutions and cutting-edge technologies. Your research paper will give a full overview of cyber security issues that occur within an e-commerce company and also of the techniques that might be used to minimize risks if you follow this approach.

Algorithms used to prevent Cyberattacks:

a. Advanced Encryption Standard(AES): In e-commerce, effective encryption techniques are frequently used to protect sensitive information, such as login details and credit card information. An example of such a technique is Advanced Encryption Standard.

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 3, March 2025
PP 92-99

ALGORITHM:

1. Begin
2. At an ecommerce website, the user enters its credit card details
3. The ecommerce website uses AES encrypting the credit card details through a secret key that are shared between the client and the server prior to communicating the data over the web
4. The Cipher text, or encrypted message, is communicated over the network
5. Since AES is symmetric, the server receives the encrypted message and uses the same secret key to decrypt
6. The server accepts the transaction after verifying the decrypted payment information
7. Stop

b. Anomaly Detection Algorithms (K-Means Clustering and Decision Trees): Some of the most effective machine learning algorithms that can be used to identify unusual activity in user activity or e-commerce transactions include K-Means Clustering and Decision Trees.

ALGORITHM:

1. Initial
2. Generate a set of "normal" data points; e.g., sensor readings, previous transactions
3. Compute mean and standard deviation of data to determine range of "normal"
4. Determine Z-score (number of standard deviations from the mean) for new data
5. Any data set with a Z-score more than some predefined cutoff (say three standard deviations) must be marked anomalous
6. If an anomaly is found, notify or take appropriate action (e.g., halting a transaction, alerting a system)
7. Stop

c. Bot Detection Algorithms (CAPTCHA and Behavioural Analytics): By using CAPTCHA and behavioural analytics algorithms, bot-driven attacks, including price scraping, inventory hoarding, and credential stuffing, can be effectively curtailed. CAPTCHA presents the challenge

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 3, March 2025
PP 92-99

of solving puzzles or objects, and behavioural analytics looks at a user's behaviour, such as the path of the mouse, where people click, and in that regard, differentiates between human and bot activity.

ALGORITHM:

1. Begin
2. Collect data of the visitors to the site. This data should include request frequency, time spent, and number of clicks by the user.
3. Train a machine learning model, such as Random Forest or SVM, on historical data to classify user sessions as "human" or "bot".
4. Apply the trained model in identifying whether a new user session is human or bot-generated. Extract features, such as the number of requests and time spent.
5. Take action, such as blocking the request or displaying a CAPTCHA challenge, if the model predicts a bot.
6. Monitor the sessions identified for further confirmation and reaction
7. Stop

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 3, March 2025
PP 92–99

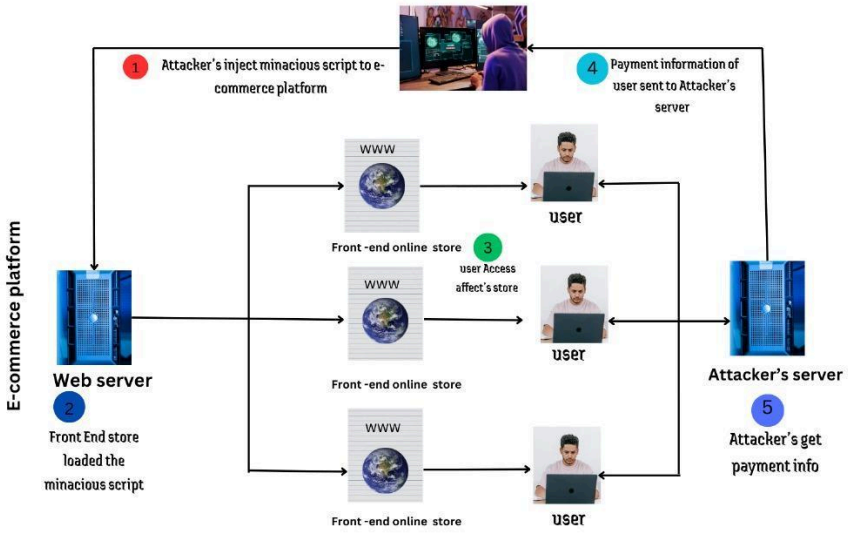


Figure 1. Cyber Attacks Architecture

5. Result And Discussion

A way that can be used for security of e-commerce platform using AES encryption is anomaly detection algorithms as well as bot identification. Even so, there is a number of drawbacks: large challenges include the distribution and management of cryptographic keys in the use of AES encryption; substantial processing power required in its encryption and decryption procedure particularly to low-power systems. False positives in anomaly detection interfere with valid transactions and get complicated when new fraudulent behaviours demand constant model modifications. Growingly complex bots that can bypass conventional CAPTCHA systems are another challenge for bot detection, leading to errors and user annoyance. Moreover, legitimate consumers may also get frustrated if behavioural analytics designates them as bots. As the nature of cyber threats changes, existing methods have to be supplemented with increasingly sophisticated solutions like multi-factor authentication, AI-based fraud detection, and quantum-resistant encryption to guarantee future security without sacrificing user experience. Some cutting-edge tactics can be used to get around the shortcomings of the e-commerce security methods now in use. Hardware security modules (HSMs) ensure the safe storage of keys, but Public Key Infrastructure (PKI) and better use of keys by key rotation can even ensure the safety of AES. All these will boost the precision of anomaly identification while bringing down false positives. Machine learning, algorithms looking at user patterns in the aim of telling

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 3, March 2025
PP 92–99

between human and bot traffic, behavioural biometrics and invisible CAPTCHA can, therefore, be all part of reaching advanced bot detection.

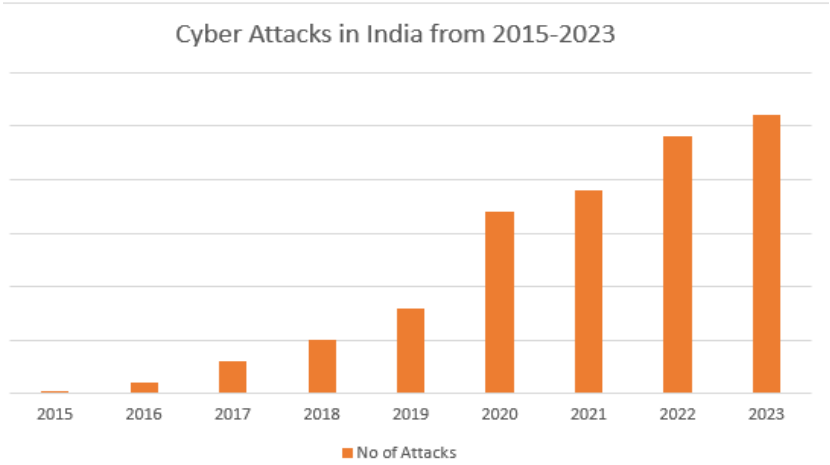
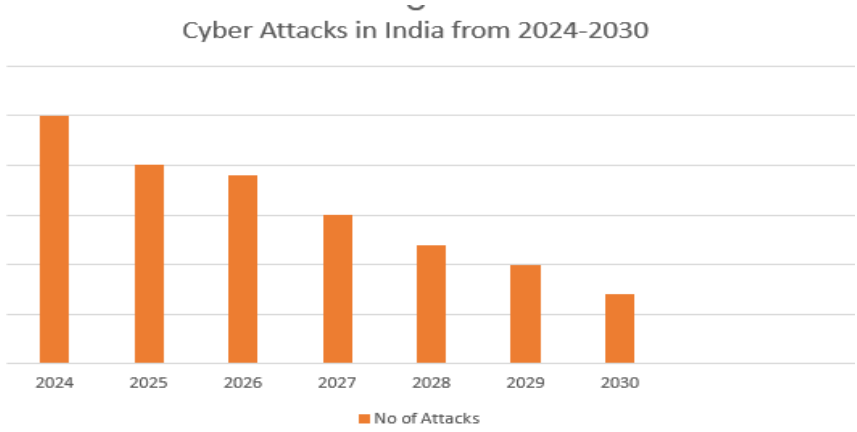


Figure 2. Cyber Attacks in India in the span of 2015-2023

After applying the algorithms mentioned in "methodology" we cannot completely reduce the cyberattacks but we can reduce the attacks in a small amount. As mentioned in the "results" by using the few more efficient techniques, we can control the rate at which the attacks are going. After applying the techniques here is the estimated result.



The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 3, March 2025
PP 92-99

Figure 3. Estimated Cyber Attacks in India in future

6. Conclusion

In summary, cyber security risk in the e-commerce process requires holistic and proactive methodology that contains advanced technologies, efficient organizational mechanisms, and strict compliance to regulations. Effective defense structures are realized through continuous monitoring and training the employees and flexible security measures, as is shown by study of current incidents and effective prevention methods. E-commerce firms can learn from highly publicized breaches and put proven techniques into action to strengthen the security of sensitive data, maintain customer trust, and minimize potential threats. The creation of the internet and other technologies has made e-commerce operations now easier and quicker to complete. E-commerce is now used for a large number of transactions, and most of the data is stored. We come to the conclusion that the challenge of cyber security threats will always be there as a sword to hurt the business, and no one knows when. This is true, regardless of how much the e-commerce firm implements and focuses on the implementation of cyber security protocols and policies, how much advanced technology is being used to conduct the e-commerce business activities, or how much the employees and customers are getting trained and skilled to do e-commerce.

References

[1]. Niranjanamurthy, M., and Dharmendra Chahar. "The e-commerce security problems and their solutions." International Journal of Advanced Research in Computer and Communication Engineering 2.7 (2013): 2885-2895.

[2]. Al Naim, Abdullah Faisal, and Arsalan Mujahid Ghouri. "Cyber Security Measures to counter Cyber-Attacks on E-commerce websites: The role of Encryption, FireWalls and Authentication Protocols." International Journal of eBusiness and eGovernment Studies 15.1 (2023): 44-469.

[3]. Khan, Dr Shazia W. "Cyber security issues and challenges in E-commerce." Proceedings of the 10th international conference on digital strategies for organizational success. 2019.

[4]. Gupta, Ruchi. "Cybersecurity Threats in E-Commerce: Trends and Mitigation Strategies." Journal of Advanced Management Studies 1.3 (2024): 1-10.
[5]. Tonge, Atul M., Suraj S. Kasture, and Surbhi R. Chaudhari. "Cyber security: challenges for society-literature review." IOSR Journal of computer Engineering 2.12 (2013): 67-75.

[6]. Chen, Hongliang, Christopher E. Beaudoin, and Traci Hong. "Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors." Computers in human behavior 70 (2017): 291-302.

[7]. Chai, Sangmi, et al. "Internet and online information privacy: An exploratory study of preteens and early teens." IEEE Transactions on Professional Communication 52.2 (2009): 167-182.

[8]. Ghelani, Diptiben. "Cyber security, cyber threats, implications and future perspectives: A Review." Authorea Preprints (2022).
[9]. Kavya, P., Vineesh, P. S., Sneha, P., Jayanth, S., & Vardhan, M. H. (2024). Stock market price prediction using machine learning. The Journal of Computational Science and Engineering, 2(2).
[10]. Vyshnavi, K., Shaik, S., Kumar, M. S., Praveen, M. S. V., & Potti, S. (2024). Facial recognition based attendance system using OpenCV. The Journal of Computational Science and Engineering, 2(3).
[11]. Gupt, S., & Gupta, N. (2024). Flight fare prediction using machine learning. The Journal of Computational Science and Engineering, 2(3).
[12]. Gadakh, S., Gadhave, O., Gangawane, S., & Jawale, S. (2024). Driver management for transportation. The Journal of Computational Science and Engineering, 2(3).