IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2025

DOI: 10.17148/IJIREEICE.2025.13487

A STUDY ON ANALYSIS OF CYBERSECURITY THREATS IN BIG BASKET

Mrs. R. Anitha[1], D. Udhaya[2]

Assistant Professor, Department of Computer Science, Dr.N.G.P Arts and Science College, India[1]

Student, Department of Commerce with Information Technology, Dr.N.G.P Arts and Science College, India[2]

ABSTRACT: This study provides an in-depth analysis of the cybersecurity threats faced by Big Basket, a leading online grocery delivery service in India. As e-commerce continues to grow rapidly, it presents lucrative opportunities for businesses but also attracts a diverse range of cyber threats. These threats include data breaches, phishing attacks, ransomware, and insider threats, each posing significant risks to customer data and organizational integrity. Given Big Basket's handling of sensitive consumer information, understanding and mitigating these risks is crucial for maintaining customer trust and ensuring business continuity. The research aims to identify specific vulnerabilities in Big Basket's cybersecurity framework, assess the effectiveness of current security measures, and evaluate the level of awareness and preparedness among employees and customers regarding these threats. Utilizing a descriptive research design, the study collects qualitative and quantitative data from various stakeholders, analysing their perceptions regarding cybersecurity risks. The findings reveal that while a considerable number of users have not experienced a security breach, there is a persistent concern regarding issues such as payment fraud and data leaks. This indicates a pressing need for improved cybersecurity measures. The study highlights the importance of enhancing user education and implementing advanced security protocols like encryption and two-factor authentication. By fostering a culture of cybersecurity awareness and vigilance, Big Basket can bolster its defence's against potential cyber attacks, thus ensuring a safer online shopping experience for its customers.

Keywords: Cybersecurity, E-commerce, Big Basket, Data Breaches, Phishing, Ransomware, Consumer Trust, Security Measures, Vulnerabilities, Awareness**.**

I.INTRODUCTION

In the era of digital transformation, e-commerce platforms have fundamentally altered the retail landscape, providing consumers with unparalleled convenience and a plethora of choices. Big Basket, one of India's leading online grocery delivery services, exemplifies this evolution by meeting the demands of millions of customers seeking easy access to essential goods. However, the rapid growth of such platforms is accompanied by an increasing array of cybersecurity threats that can undermine customer trust and operational integrity.Big Basket is particularly vulnerable to issues such as data breaches, phishing attacks, and ransomware, each posing unique risks to sensitive consumer data and financial information. As the platform expands its operations and customer base, it is imperative to identify potential vulnerabilities within its cybersecurity framework and evaluate the effectiveness of existing security measures. This study aims to analyse the current cybersecurity landscape surrounding Big Basket, focusing on the various threats it faces, the sources of these threats, and the impact on both consumers and the organization. By exploring recent incidents and industry best practices, this research seeks to provide actionable insights and recommendations to fortify Big Basket's cybersecurity posture, ensuring a secure and trustworthy shopping experience for its users.

II.OBJECTIVES OF THE STUDY

1. To Identify Cybersecurity Threats
2. To Evaluate Existing Security Measures
3. To Understand Threat Sources
4. To Customer Data Protection
5. To Future Treads in Cybersecurity

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2025

DOI: 10.17148/IJIREEICE.2025.13487

III.METODOLOGY OF THE STUDY

Research Design:
This study will adopt a descriptive research design to explore and analyze the cybersecurity threats faced by Big Basket.

Population and Sample size:
Population: The target population for this study includes that the customers who use the platform big basket within the family members, friends, colleagues, an also within my college.
Sample Size: A sample of 103 respondents will be selected for this analysis
Sampling method:
A **convenience sampling** method will be used to select participants who are readily available and willing to participate in the study.
Data collection method:
Questionnaire: A structured questionnaire will be developed to collect quantitative data from customers regarding their experiences with cybersecurity threats, awareness of security measures, and perceived risks while using Big Basket
Data analysis techniques:
The survey data will be analyzed using simple percentage to summarize user responses and identify trends in user experiences.
Ethical consideration:
Participants will be informed about the purpose of the study, and their consent will be obtained before data collection

IV.LIMITATIONS OF THE STUDY

- The study may be limited by the sample size and the use of convenience sampling, which may not fully represent the entire population of Big Basket users.
- The reliance on self-reported data may introduce bias, as participants may not accurately recall their experiences or perceptions

V.OVERVIEW OF THE COMPANY

Big Basket, founded in 2011, has emerged as India's largest online grocery delivery platform, revolutionizing the way consumers shop for essentials. Headquartered in Bengaluru, Big Basket offers a vast assortment of over 20,000 products, including fresh fruits and vegetables, staples, dairy, household supplies, personal care products, and beverages, catering to diverse customer needs. With services available in multiple cities, it provides various delivery options such as express delivery within 90 minutes, same-day delivery, and subscription-based daily essentials through "BB Daily." The platform is powered by advanced technologies like artificial intelligence and machine learning for inventory management, demand forecasting, and supply chain optimization, ensuring seamless operations and minimal stockouts. In 2021, Big Basket was acquired by the Tata Group, further solidifying its position in India's growing e-commerce ecosystem by integrating it into the Tata Digital ecosystem. Big Basket also offers private-label brands like Fresho, BB Royal, and Happy Chef, delivering high-quality products at competitive prices. Its customer- friendly mobile app and website enhance user experience with features like real-time tracking, personalized recommendations, and multiple payment options. While the platform has maintained market leadership, it has faced challenges, including the need to scale operations for perishables and a significant data breach in 2020, which exposed customer information and underscored the need for robust cybersecurity measures.

VI.DATA INTERPRETATION AND ANALYSIS

SIMPLE PERCENTAGE ANALYSIS

Percentage analysis is used in making comparison between two or more series of data. Percentage is used to describe relationship. Percentage can also be used to compare the relative terms, the distribution of two or more series of data.

$$\text{Percentage of respondents} = \frac{\text{Number of respondents}}{\text{Total number of people answered}} \times 100$$

Square analysis:
Chi-square analysis is a statistical test used to compare observed results to expected results in research methodology. It's most appropriate when the data is from a random sample and the variable of interest is categorical.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2025

DOI: 10.17148/IJIREEICE.2025.13487

The chi-square test determines if a difference between the observed and expected data is due to chance or a relationship between the variables being studied. The formula of Chi-square analysis is as follows,

$$x_c^2 = \frac{\Sigma\,(O_i - E_i)^2}{E_i}$$

C = Degrees of freedom
O = Observed Value
E = Expected Value

VII.FINDINGS

The study's findings indicate a high level of awareness among consumers regarding cybersecurity threats, with 75% recognizing the risks associated with data breaches, which were identified as the most significant concern. Payment security was perceived as particularly vulnerable, with 60% of respondents worried about fraud. Despite existing security measures, only 30% of users utilized two-factor authentication, highlighting a gap in the adoption of protective features. Additionally, respondents who actively sought information about cybersecurity were more likely to implement their own security practices. This suggests a need for Big Basket to enhance training and awareness initiatives to educate users on protecting their data, alongside a call for regular updates to security protocols to address the evolving nature of cyber threats effectively.

VIII.SUGGESTIONS

- Promote the use of two-factor authentication by showing users how it adds an extra layer of security to their accounts.
- Make it simple for users to report security problems and consider offering rewards for those who do
- Send regular emails or messages to users about security updates and tips to keep their accounts safe
- Create a dashboard where users can easily check their account security and see any alerts or updates
- Conduct regular surveys to gather user feedback on their security concerns and experiences, using this information to make improvements
- Partner with cybersecurity experts to perform regular audits and enhance the platform's security features
- Stay updated on the latest cybersecurity trends and threats, adapting strategies and user education accordingly to ensure ongoing protection

IX. CONCLUSION

The study highlights that cybersecurity is a prime feature on e-commerce sites like that of Big Basket, with users' transactions and data at risk from cybercrime. While a majority of respondents have not suffered a breach in security, concerns regarding fraud payments, spamming through email as well as data breaches are persistent. The study highlights that more stringent measures in terms of security, awareness, as well as regular updates are essential in order to maintain customers' confidence at a high level as well as shopping secure. In terms of preventive measures, utilization of new technologies as well as emphasis on awareness at a consumer level can boost its cybersecurity platform as well as secure its operation as well as users. Cybercrime is a prime challenge on e-commerce sites like that of Big Basket, which handle a high amount of consumer data. The study discovers that though a majority are comfortable with the platform, concerns regarding fraud payments, spamming through email as well as data breaches are persistent. Fifty-six percent (56.3%) of respondents are updated with cybersecurity risks through social media, though a minority take preventive measures in terms of having two-factor authentications. One of the key observations is that payment processing is seen as the riskiest area in Big Basket's operation, hence more secure encryption and secure transaction methods are a requirement. The study also indicates that platform security is inextricably tied with confidence from customers, which also means that a single event can have a lasting impact on both Big Basket's reputation as well as users' loyalty.

REFERENCES

[1]. https://www.twingate.com/blog/tips/bigbasket-data-breach
[2]. https://www.linkedin.com/pulse/big-basket-data-breach-world-cyber-security-forum

DOI: 10.17148/IJIREEICE.2025.13487

[3]. https://timesofindia.indiatimes.com/gadgets-news/grocery-app-bigbasket-hacked-data- of-2-crore-users-leaked-what-you-should-do-to-stay-safe/articleshow/79126384.cms
[4]. https://m.economictimes.com/tech/startups/bigbasket-faces-potential-data-breach-details-of-2- crore-users-put-on-sale-on-dark-web/articleshow/79109124.cms
[5]. https://securityaffairs.com/110543/data-breach/bigbasket-details-dark-web.html/attachment/bigbasket-data-leak/
[6]. https://www.indiatoday.in/technology/news/story/bigbasket-user-data-allegedly-leaked- on-dark-web-including-email-ids-numbers-addresses-of-over-two-crore