International Journal of Advance and Innovative Research
Volume 12, Issue 2 (XVII): April - June 2025
ISSN 2394 - 7780

BREACHES IN THE DIGITAL FORT: A STUDY ON CUSTOMER DATA LEAKS AND CYBERSECURITY IN INDIA

[1]Sonakshi Julka and [2]Wilson Rao
[1]Student and [2]Assistant Professor, MSc. Big Data Analytics Department, Jai Hind College, Mumbai

ABSTRACT
Cybercrime is rapidly escalating in India, presenting unique challenges for developing economies like India that are undergoing digital transformation. This paper tries to explore the growing issue of cybercrime and cybersecurity in India, where cyberattacks are reportedly increasing, and different organizations face the average attacks per week of 3,201. Successive waves of the digital revolution have prompted unparalleled growth in online services, and this is nothing but massive data accumulation at various levels across various industries from finance to e-commerce. Apart from this, this phenomenal growth period has thrown open critical weaknesses in India's cybersecurity infrastructure to serious breaches and mass leakage of sensitive customer data. We try to outline in this paper the most notable lapses on cybersecurity over the recent past and the breaches of vulnerability across various sectors, such as the massive Aadhaar data breach, security failures within the banking industry, vulnerabilities in e-commerce, and telecom data leaks. Through these high-profile cases, we identify common patterns involving security flaws, evaluate the falling domino effect of such breaches on the individuals and organizations involved, and thus assess the efficacy of the mitigation measures currently in use. This research also identifies a very critical need for stronger cybersecurity measures and frameworks of regulatory measures to protect personal data in an increasingly more digitalized economy. We assess the impact of security breaches on consumers, coordination challenges of cyber defenses, and challenges in imposing suitable regulatory oversight. Finally, we look at the Indian government's and the private sector's responses by coming out with initiatives such as the Personal Data Protection Bill that will ensure better data security and privacy standards. We propose actionable solutions and recommendations that would further enhance cybersecurity policies already in place and further strengthen the protection of consumer data. Rapid technological development requires that India address the vulnerabilities thus created in a forward-looking manner so as to preserve consumer's faith in security in this digital ecosystem.

Keywords: *Data breach, Data leak, cybercrime, cybersecurity, Cybercrime in India, Aadhaar data breach, Cyberattacks, Customer data protection, Personal Data Protection Bill cybersecurity gaps.*

I. INTRODUCTION
India has become the pace-setter in its digital transformation. However, the untimely rapid digital transformation has led to the adoption of cybercrime at equal speeds as well. Here lies the critical gaps in the cybersecurity framework of India. With the organizations witnessing an average of 3,201 cyberattacks every week, securing personal and organizational data is really becoming a daunting task. As all sectors be it finance, e-commerce, or telecommunication are moving online, many millions of the country's citizen's information channeled to inadequately secured platforms. Such an attack that symbolized and highlighted Aadhaar data leakage makes the consumer vulnerable and brings their trust into question with regard to digital services. These cyber failures come at a cost that goes beyond mere losses but lowers public confidence. Such efforts, therefore, as in the Personal Data Protection Bill, indicate that they are headed in the right direction regarding proper data governance; however, current measures are still not at par with the complexity of modern cyber threats. This paper investigates recurring security issues in industries, assesses the impact on the consumers and the organizations involved, and evaluates the effectiveness of the current mitigation strategies used. This analysis aims to present typical patterns in security flaws and provide applicable solutions to be implemented for the improvement of India's cybersecurity landscape.

ISSN 2394 - 7780

Fig 1: Data leak, Data breach, cybercrime

II. OVERVIEW OF CYBERSECURITY IN INDIA

A. Current Landscape

This digital transformation that India has witnessed, with the adoption of online services across various sectors, needed robust cybersecurity infrastructure. With growth so quick in India, security measures put into place lagged behind and exposed the customer vulnerabilities in terms of data protection. These are areas such as finance and healthcare, where personal information is ammassed on a large scale; and ecommerce, which is one of the most vulnerable sectors in this regard. (Mehta, V., & Dhillon, G. S. 2019, Mukherjee, A., & Mohapatra, P. 2017) For instance, there is an example of the growth in online banking leading to allowing cyber-crooks to exploit a software vulnerability or steal financial records of individual consumers.

B. Regulatory Framework

Even though it would raise a legal framework to manage crimes related to the information technology area, there were severe limitations. The prime focus of the IT Act revolves around cybercrime punishment without seriously working for the protection of consumer data. Recently, the Personal Data Protection Bill had been introduced to upgrade the regulations (Sharma, D., & Singhal, S. 2022) dealing with data privacy. It aimed to vest data protection rights in the citizen, compel organizations to improve data security measures, and demonstrate compliance. However, the implementation of all these rules remains challenging in this Indian digital scattered landscape.

C. Regulatory Framework

Whereas the Information Technology Act gave legal competency for cyber-related offenses to be handled, it is somewhat more riddled with very serious pitfalls. The IT Act dealt primarily with penalizing cybercrimes, and hardly any attention was paid for proactively taking care of protecting consumer data. The Personal Data Protection Bill was recently drafted to fortify data privacy regulation. This bill has empowered citizens with rights of data protection, obliged organizations to enhance data security, and necessitated conformance. However, implementing such pieces of legislation across the highly fractured digital platform in India is no mean feat.

III. CASE STUDIES ON MAJOR DATA BREACHES IN INDIA

1.BigBasket Data Leak

In October 2020, hackers compromised an online grocery delivery service, BigBasket, exposing over 20 million customer details. Hackers stole email addresses, phone numbers, delivery addresses, and hashed passwords. Hackers seem to have put up the stolen data on the dark web for sale and can sell it to identity thieves. It again brought under focus the need for stronger data encryption and cybersecurity measures in the e-commerce sector, where a huge amount of sensitive information is kept about its customers.

2. Mobikwik Data Breach

In March 2021, digital wallet provider Mobikwik suffered a data breach that affected nearly 100 million users. The exposed data included names, email addresses, phone numbers, bank account details, and partial credit card numbers. Cybersecurity researchers discovered a 9GB database with Mobikwik's user information on the dark web. Mobikwik initially denied the breach but later faced significant public backlash. This case drew attention to the importance of proactive breach detection and the implementation of multifactor authentication for sensitive accounts.

ISSN 2394 - 7780

3. Domino's India Data Leak
In May 2021, Domino's India operated by the company Jubilant Food Works reported a data breach that leaked data of 180 million orders. It compromised customer name, phone number and delivery address information. Details of internal company files and an employee's information were also breached. The data later surfaced for sale on the dark web. This case points out the vulnerabilities in protecting customer information in the food and hospitality industry, along with the importance of adequate data storage practices.

4. Aadhaar-Linked Health Records Leak
In January 2022, a health sector breach exposed sensitive medical records of individuals linked to their Aadhaar information. This included various health databases integrated with India's National Digital Health Mission, or NDHM. Exposed data include their health history, treatments, and other personal information. This has once again added concern over security protocols for Aadhaar-linked records as well as dangers of centralized storage combined with personal health data integration.

5. Unacademy Data Breach
In mid-2022, Unacademy, a popular e-learning platform in India, suffered a data breach that compromised data of over 22 million users. Leaked information included email addresses, names, and usernames, and was reportedly sold on the dark web. Although no payment information was leaked, the incident illustrated the growing threats to online education platforms, especially as e-learning gained traction during the COVID-19 pandemic.

6. HDFC Bank Data Exposure
In early 2023, a security researcher disclosed a data exposure incident at HDFC Bank that displayed some comprehensive information about clients due to unsecured servers. Names, account numbers, and transactions carried out of the customers were compromised. The breach was promptly addressed, but it did spark some questions about internal cybersecurity practices and the data protection protocols existing within Indian banking institutions.

7. Aadhaar Data Breach
One of the most significant data breaches in India involved the Aadhaar database, which exposed the personal information of millions of Indian citizens. Unauthorized access to this data led to widespread privacy concerns, highlighting severe flaws in data protection strategies and the need for advanced security protocols. The breach exposed the vulnerability of centralized databases and the potential consequences when sensitive citizen data is compromised.

8. Air India Data Breach
Air India reportedly suffered a data breach in May 2021, which compromised about 4.5 million passengers. The stolen information included passenger names, passport details, contact data, and credit card details. The vulnerability was in the systems of SITA, a global IT provider for the aviation sector. Third party data management risks were finally brought to the forefront, and with robust data sharing agreements and cybersecurity standards in partnerships, Air India answered back with issues like password reset and credit card reissuance.

9. Justdial Data Leak
An investigation in July 2021 found out there was a data breach involving Justdial, a free local search and business directory service, where personal information of more than 100 million users leaked out into the open. The data exposed contained names, phone numbers, email addresses, gender and details of user queries. The hackers managed to steal the data because the endpoints in the API of the mobile application of Justdial were insecure. This, in the course of time, led to a responsibility in making people aware of the need to secure API endpoints as well as encrypting customer data in the sector of search and business services.

10. Indian Railways Data Leak
This was the case when, in February 2023, it was revealed that a data leak from Indian Railways exposed millions of passengers' names, phone numbers, email addresses, and travel details. The breach, which has been caused by the vulnerabilities within the website of Indian Railways, does not only compromise personal information but also travel schedules, thereby exposing privacy and security risks among people affected. The aftermath of the incident highlighted the need for proper security implementations in the online services managed by the government and put more importance on the increasingly growing peril to public infrastructure through cyberattacks.

ISSN 2394 - 7780

IV. CYBERSECURITY CHALLENGES AND IMPACT

A. Key Cybersecurity Challenges in India

1. Technical Vulnerabilities

One of the major issues in the cybersecurity landscape of India is technical vulnerabilities in digital infrastructures. It's a matter of great concern that there are very few advanced security systems available within the small and medium-sized enterprises in India, thus making them vulnerable to sophisticated cyberattacks. Some common reasons for exposure can be obsolete software, unpatched systems, and weak encryption protocols with respect to risks like ransomware, phishing, and Distributed Denial of Service (DDoS) attacks. Moreover, when heritage systems are integrated with newer technologies, compatibility issues arise that cybercriminals can take advantage of.

2. Inadequate Regulatory Framework and Enforcement

While India has made strides in developing cybersecurity regulations, the enforcement of these laws remains inconsistent. The Information Technology (IT) Act, 2000, provides a legal framework for addressing cybercrimes, but it is often criticized for being outdated and not comprehensive enough to cover emerging threats. The proposed Personal Data Protection Bill aims to strengthen data privacy and protection, but its implementation is still in progress. Furthermore, the lack of uniform enforcement across different states and sectors leads to gaps in cybersecurity practices, making it challenging to maintain a cohesive defense against cyber threats.

3. Increasing Sophistication of Cyber Threats

Cyber threats in India have increased in sophistication level; with attackers now applying advanced techniques such as AI and ML in breaching the security systems. These technologies enable cybercriminals to automate attacks, avoid detection, and exploit vulnerabilities more efficiently. The rise in targeted attacks, including APTs, is a tremendous challenge since they are designed to remain masked for extended periods; thereby causing vast damage before being identified.

Fig 2: Cybersecurity, Cybersecurity in India

4. Insufficient Investment in Cybersecurity

Many Indian organizations, especially in the public sector, allocate limited budgets for cybersecurity initiatives.This underinvestment leads to inadequate security measures, insufficient monitoring, and delayed responses to incidents. Without substantial financial commitment, organizations struggle to adopt cutting-edge security technologies and hire qualified professionals, leaving them vulnerable to cyberattacks.

B. Impact of Cybersecurity Breaches in India

1. Economic Consequences

Cybercrime attacks have serious economic implications on businesses, and the general economy at large. The losses in this regard would be enormous resulting from various financial consequences of data breach, ransomware, and fraud. Some data indicate that the cost of a data breach for organizations in India reached an average of $2.18 million in 2023, up 28% on a yearly basis from data collected in 2020. The cost in this context includes direct financial loss, the lawyers' fee and regulatory penalties, and costs incurred during incident response and recovery. Cyberattacks can also impact the business operations, causing a loss in revenue and reduced productivity.

2. Erosion of Consumer Trust

Data breaches erode consumer trust, which is essential for the sustained growth of digital services. When customer’s personal and financial information is compromised their confidence in using online platforms diminishes. This loss of trust can result in decreased customer loyalty, reduced user engagement, and

ISSN 2394 - 7780

a decline in overall market participation. Rebuilding consumer trust after a breach is a lengthy and costly process, often requiring extensive public relations efforts and enhanced security measures.

3. Legal and Regulatory Repercussions

Cybersecurity attacks may also attract legal and regulatory penalties. To violate the provisions related to data protection laws and cybersecurity regulations can result in huge fines, lawsuits, and penalties. Once the Personal Data Protection Bill comes into effect, more stringent compliance standards will be imposed, and if companies don't respect those standards, huge legal penalties will be incurred. Diversion cost apart from monetary expenses due to lawsuits, there are diversion costs involved with diversion of resources from the core business activities for compliance matters and legal defenses.

4. National Security Risks

Cybersecurity breaches can pose national security risks, particularly when they target critical infrastructure sectors such as banking, telecommunications, healthcare, and government services. Attacks on these sectors can disrupt essential services, compromise sensitive information, and undermine national security. The interconnectedness of digital systems means that a breach in one sector can have cascading effects across multiple domains, amplifying the overall impact on the country's stability and security.

V. CURRENT AND PROPOSED SOLUTIONS

Fig 3: Cybersecurity, Solutions to prevent data leaks

1. Advanced Technological Measures

Artificial intelligence (AI) and machine learning (ML) offer innovative ways to enhance cybersecurity (Ramesh, S., & Prakash, A. 2023) by detecting anomalies, predicting potential threats, and automating response actions. Techniques such as behavioral analytics, where AI identifies unusual user behavior, could provide early alerts for potential breaches. Blockchain technology also presents a decentralized solution for storing and verifying data, reducing the risks of centralized breaches.

2. Strengthening Regulatory Frameworks

The Personal Data Protection Bill in its current version really restricts data collection and storage, as well as processing, and empowers the citizen with control over his or her personal data. For this to be fully effective, these regulations need to be implemented very strictly and, if possible, similar to international standards, such as the General Data Protection Regulation of the European Union. Additional compliance measures and regular audits will further ensure that companies adhere to data protection protocols.

3. Best Practices for Organizations

Best practices include holding regular security audits, implementing multi-factor authentication, and offering training for employees to improve organizational security. Securing data encrypts software updates and the use of best coding practices; these are effective ways to prevent data breaches. Organizations are able to respond to breaches, recover quickly, and have less damage with good incident response planning.

ISSN 2394 - 7780

VI. FUTURE DIRECTIONS AND RECOMMENDATIONS

1.Emerging Technologies

Quantum computing, edge computing, and secure cloud infrastructure present new opportunities for advancing cybersecurity in India. Quantum computing, while still in its infancy, promises unparalleled data processing capabilities that could help defend against future cyber threats. Additionally, edge computing enables data processing closer to the data source, improving security in real-time applications.

2. Policy Recommendations

Policymakers need to bring in clear guidelines and stringent penalties in case of noncompliance to fortify the cybersecurity base in India. At the same time, there is a need for greater transparency in dealing with data. Improvement of national cybersecurity infrastructure needs collective contributions from both government as well as private sectors of the economy. Moreover, creating consumer awareness campaigns can empower citizens to protect their data and report potential breaches.

3. Public Awareness and Education

With this effort and growing dependence on the digital world, an educated public about cybersecurity has become a necessity. Programs educating consumers on their rights when it comes to data privacy and practices of consuming data online can be a significant step forward in making consumers less vulnerable to cyber threats. Schools and universities are equally important in trying to build a solid foundation for the future workforce with cybersecurity training within school curriculums.

VII. CONCLUSION

India's specific cybersecurity needs require a proactive and concerted approach towards the protection of personal data in an increasingly digital economy. With focus on current high-profile data breaches by critically reviewing current measures, suggesting solutions to exemplify the greater need for more robust security frameworks, this paper highlights this need as being imperative for India's cybersecurity infrastructure to be regarded as a priority with regards to more advanced technology, legislation, and the fostering of security awareness through varied steps that can maintain public trust in digital services.

ACKNOWLEDGMENTS

I am profoundly grateful to my mentor, wilson rao sir, for his invaluable guidance and unwavering support throughout the course of this research paper. His vast knowledge and insightful feedback have greatly deepened my understanding of the subject. I truly appreciate the time he invested in reviewing my work and offering thoughtful advice, which has significantly elevated the quality of this study.

REFERENCES

[1] **Bose, S., & Verma, M.** (2024). Data breach costs in India: An analysis of financial impacts from 2020 to 2024. Journal of Financial Cybersecurity, 2(1), 50-68. doi:10.1016/j.fcyber.2024.01.004

[2] **Mehta, V., & Dhillon, G. S.** (2019). Current cybersecurity challenges and solutions in e-commerce. Journal of Cybersecurity and Privacy, 3(2), 123-138. doi:10.3390/jcp3020011

[3] **Mukherjee, A., & Mohapatra, P.** (2017). Cybersecurity issues in modern day e-commerce. Computers & Security, 78, 241-259. doi:10.1016/j.cose.2017.04.005

[4] **Ramesh, S., & Prakash, A.** (2023). The rise of phishing attacks in India: Trends and mitigation strategies. Journal of Cybersecurity Trends, 5(3), 145-160. doi:10.1016/j.cybertrends.2023.03.002

[5] **Sharma, D., & Singhal, S.** (2022). Data protection laws and the rise of privacy frameworks in India: A review of the Personal Data Protection Bill. Indian Journal of Law and Technology, 14(1), 15- 29.

[6] **Singh, K., & Choudhary, R.** (2021). A case study of Aadhaar data breach and implications on data security. International Journal of Cyber Criminology, 12(2), 65-78. doi:10.1177/0974627921123429

[7] **Subramaniam, B., & Gupta, P.** (2018). "Cybersecurity in Indian banking: A roadmap to enhance data protection and privacy." International Journal of Information Management, 42, 46- 56. doi:10.1016/j.ijinfomgt.2018.04.004