Archives available at journals.mriindia.com

International Journal on Research and Development - A Management Review

ISSN: 2319 - 5479

Volume 15 Issue 01, 2026

Securtisation of Data and Best Practices Privacy in Banking Sector

[1]Dr. E. Saravanan, [2]S. Mohana Priya, [3]V. Muthulakshmi

[1]Research Supervisor & Guide, Assistant Professor,
PG & Research Department of Commerce
Dharmamurthi Rao Bahadhur Calavala Cunnan Chetty's Hindu College
(Affiliated to the University of Madras), Chennai - 72
[2,3] Ph.D (Full-Time) Research Scholar,
PG & Research Department of Commerce
Dharmamurthi Rao Bahadhur Calavala Cunnan Chetty's Hindu College
(Affiliated to the University of Madras), Chennai - 72
Email: [1]Prof.esaravanan@gmail.com, [2]mohanapriyas291288@gmail.com, [3]muthufamily2@gmail.com

Peer Review Information

Submission: 10 Feb 2026

Revision: 22 Feb 2026

Acceptance: 03 March 2026

Keywords

Security, Customer, Banking Sector, Data Privacy.

Abstract

The protection of customer information and financial data is of paramount importance to banks to maintain trust and confidence in their services. This research paper delves into the dynamic landscape of data privacy and security within the banking industry, examining the multifaceted challenges encountered by banks. It further investigates the proactive measures, best practices, challenges in data privacy and strategic approaches implemented to fortify the protection of sensitive information. By analyzing the current landscape, regulatory frameworks, and emerging technologies, this paper aims to provide insights into effective data protection and challenges for banks.

Introduction

Data privacy and security in the banking sector refers to the measures and practices implemented to protect customer information and safeguarding the confidentiality, integrity, and accessibility of financial data of paramount importance. Data privacy is the protection of personal data from those who should not have access to it and the ability of individuals to determine who can access their personal information.

Objectives

The purpose of the study is challenges in data privacy and security for banks.

To study best practices in data privacy in protection of customers

Review of Literature

Patsiotis (2012) examined internet banking adoption and resistance behaviour in Greece in order to develop profiles of adopters and non-adopters of the service. The study identified three segments, where the description of their profiles was based on customer perceptions of the service and general usage data. Across these segments adopters and non-adopters were found to have different characteristics. With regard to demographics, only income was found to be associated with segment membership.

Thakur and Srivastava (2013) investigated the factors influencing the adoption intention of mobile commerce. For the study purpose research model was developed based on constructs from the technology acceptance model and innovation resistance theory. Perceived usefulness, perceived ease of use and

social influence were found to be significant dimensions of technology adoption readiness to use mobile commerce while facilitating conditions were not found to be significant. The results also indicated perceived credibility risk defined by security risk and privacy risk was significantly associated with behavioural intention in negative relation, which indicated that security and privacy concerns are important in deterring customers from using mobile commerce.

Maditinos et al., (2013) developed an extended technology acceptance model (TAM) model as a tool for examining the factors that have a significant impact on customers' online banking acceptance. The typical TAM constructs were enhanced with the variables of perceived risk and quality of the internet connection. The proposed conceptual framework of the study (extended TAM), was tested on a sample of Greek internet users. The findings of the study provided overall support for the extended TAM model and confirmed its robustness in predicting customers' intention of adoption of internet banking. More specifically, results underlined the important impact of perceived usefulness, security risk and performance risk on the intention to use internet banking. On the contrary, the impact of perceived ease of use and quality of the internet connection seemed to have only an indirect effect on internet banking adoption.

Challenges in Data Privacy and Security for Banks:

Cyber-security Threats: Banks face a wide range of cyber threats, including malware, phishing attacks, ransomware, and advanced persistent threats (APTs). Constant vigilance and robust security measures are necessary to mitigate these threats.

Insider Threats: Employees with access to sensitive data pose a significant risk to data privacy and security. To mitigate insider threats, banks must enforce stringent access controls, implement comprehensive monitoring mechanisms, and conduct employee awareness programs.This includes robust user authentication measures, role-based access controls, and regular review and updating of access permissions.

Third-Party Risks: Banks often rely on third-party vendors, suppliers, and service providers, increasing the risk of data breaches and privacy incidents. Thorough due diligence, vendor risk assessments, and contractual agreements are crucial for managing third-party risks effectively.

Regulatory and Compliance Challenges: The banking sector faces complex data protection regulations and must adapt to evolving regulatory requirements. Compliance monitoring, reporting, and ensuring alignment with regulatory guidelines pose significant challenges for banks.

Best Practices for Data Privacy and Security in Banks

- Data Classification and Risk Assessment: Banks should classify their data based on sensitivity and conduct regular risk assessments to identify vulnerabilities and prioritize protection measures.
- Access Controls and Authentication: Strong access controls, role-based access privileges, and multi-factor authentication are essential to prevent unauthorized access to sensitive data.
- Encryption and Data Masking: Encryption techniques, both in transit and at rest, should be implemented to protect data confidentiality. Data masking techniques, such as tokenization and anonymization, can further safeguard sensitive information.
- Incident Response and Management: By establishing incident response plans, banks can quickly identify and contain security breaches, mitigate potential damages, and initiate appropriate remediation measures. These plans outline the roles and responsibilities of key personnel, provide guidelines for communication and coordination, and specify the necessary steps to restore normal operations while preserving the integrity of customer data. Prompt detection, containment, notification, and recovery are critical elements of incident response.
- Employee Awareness and Training: Banks should provide comprehensive training programs to employees, emphasizing the importance of data privacy, security best practices, and the risks associated with negligent or malicious actions.
- Regulatory Frameworks and Standards: Compliance with relevant data protection regulations, such as GDPR and PCI DSS, is essential for banks. Regulatory frameworks provide guidelines and requirements for protecting customer data and ensuring privacy. Banks need to stay up-to-date with regulatory changes and incorporate them into their data privacy and security strategies.

Conclusion

Data privacy and security are paramount for banks to maintain customer trust, comply with regulations, and protect against financial and reputational risks. By adopting best practices, leveraging emerging technologies, and staying vigilant, banks can mitigate data privacy and security challenges effectively. In today's digital age, data privacy and security have emerged as critical concerns for the banking sector. The importance of safeguarding customer information, financial data, and maintaining trust cannot be overstated. Banks face various challenges in ensuring data privacy and security, including cyber-security threats, insider risks, third-party vulnerabilities, and compliance complexities. However, by implementing best practices and leveraging emerging technologies, banks can effectively mitigate these challenges and protect sensitive data. Data privacy and security in the banking sector require a comprehensive approach that encompasses regulatory compliance, robust technological measures, and employee awareness and training programs. Banks must adhere to relevant data protection regulations, such as GDPR and PCI DSS, and continuously monitor and adapt to changing compliance requirements. Implementing strategies such as data classification, access controls, encryption, incident response plans, and employee training significantly contribute to mitigating risks. Furthermore, emerging technologies such as artificial intelligence, block chain, and biometric authentication offer promising avenues for enhancing data privacy and security in banks. Leveraging these technologies can improve fraud detection, transaction integrity, and user authentication processes, augmenting existing security measures. Successful case studies, such as JPMorgan Chase, HSBC Holdings, and Deutsche Bank, demonstrate the effectiveness of comprehensive data privacy and security measures. These organizations prioritize data protection through encryption, access controls, continuous monitoring, and employee awareness programs. Looking to the future, banks must stay ahead of the evolving threat landscape by continuously enhancing their security measures, fostering collaboration, and engaging in information sharing initiatives with industry peers and regulatory bodies. Continuous monitoring and auditing are vital to detect and respond to security incidents promptly. Additionally, exploring stronger customer authentication methods, such as biometrics or token-based authentication, can further bolster data protection efforts.

Bibliography

PWC (2012), Carving a new path through innovation, CII Banking Tech Summit report. Available at https://www.pwc.com/in/en/assets/pdfs/consulting/financialservices/Carving_a_New_Path_Through_Innovation_June_28_2012.pdf , Accessed on 9th September, 2012.

Rajneesh De and Padmanabhan, Chitra, (2002), ―Internet Opens New Vistas for Indian Banking‖, Express Computer, 16th September, available at http://www.expresscomputeronline.com/20021202/banks1.shtml. Accessed on 9 th September, 2012.

RBI (2012), Report on Trend and Progress of banking in India. RBI‘s Report of Internet banking (2001) available at http://rbidocs.rbi.org.in/rdocs/notification/PDFs/21569.pdf.

Thakur, Rakhi and Srivastava, Mala (2013), ‗Customer usage intention of mobile commerce in India: an empirical study‘, Journal of Indian Business Research Vol. 5 No. 1, pp. 52-72.

Maditinos, Dimitrios, Dimitrios, Chatzoudes and LazarosSarigiannidis (2013), ‗An examination of the critical factors affecting consumer acceptance of online banking: A focus on the dimensions of risk‘, Journal of Systems and Information Technology, Vol. 15 No. 1, pp. 97-116.