Journal of Information Systems Engineering and Management
2025, 10(52s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Mobile Banking Security Risks: An Analysis

[1]Twinkle Malhotra, [2]Dr. Sunil Kadyan

[1]*Research Scholar, Manav Rachna University,*
twinklemalhotra1998@gmail.com

[2]*Associate Professor, Manav Rachna University,*

Received: 25 Dec 2024 Revised: 15 Feb 2025 Accepted: 25 Feb 2025

1. INTRODUCTION TO MOBILE BANKING

Today, personal experience in banking involves a growing variety of services, making it easier to use one's money from various locations through the use of digital platforms. One such service provides mobile banking, which is the provision of financial services using mobile devices. At its most basic, it allows a customer to interact with a bank via mobile devices using text or through a browser. It fosters ease of access to the banking account, especially when the customer is traveling from one place to another. It offers a wide range of activities and services that a customer can do, such as fund transfers, checking deals, paying bills, reducing balances, and wire transfers. Devices used include mobile phones, smart cards, and personal digital assistants, as these are used to access financial services from mobile devices. The major part of India has been avoided, and the specifics have been incorporated either from public sources, primary survey work, or anecdotal information during conference hall deliberations in various parts of the region at different periods of time. The changes and the differences are in the adoption of various technologies and the spread of the internet and the mobile network.

Mobile banking is part of what can be seen as a larger trend towards digital banking, an evolution consisting of four stages, with each stage more advanced than the other. Initially, in the era of paper-based banking, transactions between banks and their customers were conducted through manual processes involving a paper-based exchange of information. This type of banking is still popular in developing countries. In the second stage, the systems of electronic banking, the so-called branch, departmental, retail banking, and wholesale banking ensure the automation of transactions. The third stage is online banking, which allows customers to conduct financial transactions on a secure website operated by their retail or virtual bank. The system then connects to the bank's network, and an online banking session begins or takes place. This is normally operated by a retail bank; the simplicity of trading online has opened up the possibility of banking in ways that were previously impossible, such as checking a bank account, investing in mutual funds or bank deposits, and managing accounts and transactions, all via the internet. It is now possible for the customer to have this facility from anywhere and anytime, using the internet if they just access the bank's internet banking. The latest generation, stage four, is mobile banking. Generally, mobile banking services are growing at a rate of 100 percent each year. Surveys show consumers are keen to adopt mobile banking services because of the convenience offered. The customer is seeking fast communication and tools that meet the criteria of mobile commerce.

1.1. Definition and Scope

Mobile banking refers to a system that allows customers to make financial transactions using a phone or a personal digital assistant with an internet connection. The most basic function of mobile banking is to check account details such as the current balance and transaction history. In addition to these, several banks have started offering services such as fund transfers within the same bank or to other banks, mobile recharge facilities, and payment processing due to user demand and technological capabilities. Users can deposit checks, view account activity, pay bills, transfer money, and send money to another account, send cash for recipients to pick up, or send cash to be picked up by recipients. Banking services are offered free of cost or at a minimal cost. Some mobile banking providers charge

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(52s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

end consumers in the form of data charges. Various other reasons that have led to the popularity of the mobile banking system are that most mobile phones have a short messaging service feature through which banks deliver information to their customers regarding their bank details. Furthermore, mobile banking is P2B, and rather than internet infrastructure limitations, the mobile banking system can be much preferred.

The purpose of our study is to investigate security concerns and to propose a risk management framework from the perspective of two major stakeholders, i.e., the banks and the mobile subscribers in the geographical location of Delhi NCR. Technologically, the banking sector of Delhi NCR is equipped with the latest communication channels and provides various banking services to customers, transcending geographical boundaries, virtually 24/7. Thus, this study touches upon a number of aspects from the Delhi NCR perspective, including improving the existing mobile banking infrastructure to cater to a large population, which in turn has multiple security concerns, both in operational aspects as well as in risk management.

1.2. Evolution and Adoption

Evolution and Adoption

Mobile banking is simply the latest form of banking services that use mobile communication devices. This innovation opens up many new opportunities in the business world. The software that drives mobile banking technology was introduced to the public after 2002, and by 2002, all of the major banks in America had a platform, with 4.1 billion registered customers conducting transactions valued at $498 billion annually. In 2007, research showed an increase of 154% in global mobile banking usage from the previous year. Currently, a number of large countries in terms of economics are growing fast. Now, more than 182 banks worldwide are offering mobile banking services today. In 2001, a software company released the first customizable and pluggable portal solution for banks, including the first mobile banking service. The software represented the first downloadable mobile banking service mainly using an SMS gateway.

Statistics clearly show an increase in worldwide mobile banking usage over time. Rapid advances in technology have led to the widespread adoption and use of mobile phones, smartphones, and other mobile devices. These technological advances have also allowed mobile devices to develop to where they are today. Gone are the days when mobile devices were carried about as a status symbol. Today's mobile devices are more compact and robust, with more storage space and additional processing power. According to research, the digital climate is now evolving to the point where mobile phones and tablets are the main tools for searching the internet. This is happening around the world today. The number of mobile internet users worldwide increased by 17% from 2 billion in 2015 to 2.3 billion in 2016 and by 20.3% to 2.8 billion in 2017. Many factors can be ascribed to the increase in the number of people using mobile phones worldwide. More people can afford to buy a mobile phone, and others consider it a great asset in making life simpler. The rapid penetration of the internet also plays a critical role in the increased use of mobile phones. Furthermore, with more companies implementing work-from-home policies, the need for employees to stay connected is more important because business transactions are gradually moving from paper to mobile, thereby contributing to the increased use of mobile phones. With growing interest from consumers, more bank entities began to offer the new mobile banking services to their customers.

2. IMPORTANCE OF SECURITY IN MOBILE BANKING

Mobile banking security can be approached using the 'C' of the CIA triad, which stands for confidentiality. The data at rest and in transit of a user should be encrypted with industry-recognizable encryption standards. Integrity is the next on the list, and it ensures that the transactions are going through or not interrupted by a third party. It is necessary in mobile banking systems to alert the user when a transaction is attempted on their behalf. Data pertaining to user accounts should be readily

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(52s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

available, and this is made possible through the 'A' in the CIA triad, availability. The availability of the services makes a customer return again and again to the mobile banking services, but with an equal proportion of security importance. The data should be available to an authorized user and also protected from unauthorized access.

Numerous rules, guidelines, and statutes prescribe how the transaction and the credentials should be protected. Strong data encryption, multifactor authentication, and other customer data privacy measures are required. In India, guidelines have been issued and also regularly updated for the users of mobile banking. It is a criminal offense to fail to set up the minimum standards in mobile banking. This means that not only users but also developers are equally responsible. In a few words, by reducing security risks and increasing security, mobile banking is resilient in the face of regulatory compliance because a balanced and strong level of security in the embedded system is expected. Importantly, laws directly influence mobile banking as a service, such as configuration, architecture, smooth processing, technological usage, and targeted groups of users. The consequences of non-compliance or failure to prove compliance with these regulations are far-reaching to the embedded system. In the banking system, non-compliance can lead to large-scale financial damages and eventually harm to the common man, as they have shown their unflinching trust in banking, as evidenced by the rapid increase in the mobile banking user population. Efforts would also be taken in the research to understand the shift of security risks in account-based banking to user-based banking.

2.1. Confidentiality, Integrity, and Availability (CIA) Triad

2.1. Confidentiality, Integrity, and Availability (CIA) Triad

Every security policy is built around the cornerstones of confidentiality, integrity, and availability. Company data is shifting from central servers to distant data centers, making on-the-fly analysis and transaction completion achievable. These are the significance of the new CIA. These aspects are used to secure the data and verify the enterprise. Confidentiality implies that the protected or sensitive data are concealed from an unauthorized individual, so it will be undetected if intercepted. Confidentiality in mobile banking is preserved utilizing encryption algorithms, user identification and validation, and authentication along with firewalls and other Internet protection techniques. An accessibility management structure is essential for the integrity and confidentiality of mobile banking.

Data integrity implies that the data are reliable and proper during their issuance. In mobile banking, data integrity can also be accomplished utilizing electronic signatures, which can be built with the utilization of digital signatures and certificates. Data availability implies that the banks must allow consumers to obtain information each time they want in order to handle every service request. The transmission system, internet, and communication networks are needed for mobile banking to be operable. At any level, a shortage in these devices is equal to a permanent disruption of the device, which could bring about a state of economic loss. Confidentiality, integrity, and availability are the three mainstays of protection not only for bank systems but also for details. Each pillar is equally significant to banking and the whole economy. The requirement for each item is established in this paper, which has improved with the development of telecommunications and increased the instances and complexity of safety flaws. An improvement in the number of these flaws can be expected in the near future. This research and learner book are now in Melbourne, Australia, and have concentrated on approaches to managing risks and crises. Bank and safety managers wander throughout the world. Traditionally, safety management plans have prioritized availability, thus neglecting the CIA dimensions. Safekeeping is more the conglomeration of three elements, which are essential for handling hazards. These aspects can portray the existence of altering menaces, be they old or new. Balancing these three factors is crucial to risk management.

Ensuring information security is characterized by emphasizing the need to maintain confidentiality, integrity, and data availability, which ensures customer trust in the bank's services. One of the

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(52s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

important elements that needs to be seen as one of the important reference frameworks, with the existence of supporting elements, will be able to form an effective protocol in information risk management in the scope of understanding threats and vulnerabilities. The principles above indicate that maintaining security is the top priority. The aims of achieving conformity with the organization's legal requirements include maintaining business activities. The research objectives are being pursued to assess the conceptual contributions and practical consequences.

2.2. Regulatory Compliance

Regulatory compliance refers to the body of laws and regulations that describe a legal and ethical code of conduct to be followed by top executives. By the very nature of their business, banks and financial institutions are essentially open to risks. Security for online and mobile banking is an integral part of an enterprise-wide integrated approach to providing secure, robust, compliant, and reliable internet-based services. The security of the mobile banking system primarily refers to the technical information security surrounding the use of mobile devices. The security of transactions relates to the secrecy and integrity of exchanged messages as part of negotiations around establishing, managing, and effecting transactions. Although regulatory control or standardization may not be exact, the people in charge of these organizations must be aware of the current situation of regulation. All intermediaries and companies are required to maintain reasonable security practices in accordance with the international standard.

A huge number of international and national legal and regulatory instruments are applicable to mobile banking. These span consumer and competition laws, privacy and data protection laws, telecommunications laws, and telemarketing laws. The severity of possible sanctions under non-compliance can be quite high, ranging from administrative fines through judgments such as court-imposed injunctions, investment of profits gained by illegal conduct back to public funds, other relief including cease-and-desist orders, and disgorgement, where the violation resulted in unjust enrichment. There can be class actions other than administrative and judicial cases as per customer protection laws. The nature of this legislation is essentially disclosure-based; to the extent that technology does explicitly need to be mentioned in order to fulfill such provisions, it is in ways that could, in the view of those consumer protection advocates, engender consumer trust and strengthen security. More importantly, it says that regulatory compliance contains significant information regarding expected security practice implementation actions and understanding, signifying the interdependence of technology and regulation in security measures.

3. TYPES OF SECURITY THREATS IN MOBILE BANKING

Mobile banking is a system that allows customers to perform transactions or access information without the need to visit a bank physically. Though it has a host of advantages, mobile banking is susceptible to a host of threats because most modern phones are 'little' computers that run on complex operating systems; thus, they share similar risks with any other device that is connected to a network. This section explores these threats in greater detail as a step in understanding the multitude of risks that a mobile banking ecosystem must cope with. Typically, the traditional risk of banking is amplified in each of these operations, and added to this is the disposable nature of mobile devices that are easily lost, stolen, or misplaced. Some of the most common types of mobile banking threats come in the form of malware and SMS phishing attacks. One increasingly common type of attack among these is the Man-in-the-Middle attack. Man-in-the-Middle attacks are where the attacker intercepts communications between the genuine user and the financial institution by gaining access to the same connection and alters data in exchange either in real-time or even in 'stealth' mode without either end realizing. Given various banking regulations and security standards are operational, these attacks pose additional directives for enforcement. Man-in-the-Middle attacks represent a technology-based threat; the sophistication generally requires that the user download multiple software tools and acquire considerable expertise in systems and protocols. Furthermore, Man-in-the-Middle attacks permit the perpetrator to extend their

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(52s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

sphere of control to banking servers and banks' information, thus combining fraud and high-profile privacy concerns that could result in identity theft or breaches.

3.1. Malware and Phishing Attacks

Malware and phishing attacks are the most prevalent threats in mobile banking. The widespread use of portable computing devices like smartphones creates an opportunity for malware to infiltrate the system. Some malware writes its registry entries, which help it achieve persistence in the system. However, modern antivirus and anti-malware solutions provide safeguards against malware, but some malware can go undetected. Some malware can steal login credentials and other sensitive details stored in the smartphone, such as usernames and passwords of mobile banking applications, or even credit card information. This would allow an attacker to gain unauthorized access to bank account information. Stolen login credentials can also help an attacker initiate transactions to perform financial fraud.

If a keylogger is installed on a device, everything a user types, including sensitive credentials or PIN, can be captured by an attacker. A Trojan horse can compromise a mobile banking account when a user carries out a transaction using the mobile banking application. A Trojanized mobile banking app can make hidden transactions without the knowledge of the mobile banking user. As a result, security has become a fundamental consideration when pursuing mobile banking. Phishing has emerged as one of the most dangerous strategies for breaching a bank account in mobile banking. Social engineering, such as user habits, is the art of deceiving people into revealing sensitive information. It is a common cybercrime practice. These kinds of assaults are carried out through phone calls, emails, badges, SMS, and social networking platforms. The process of psychological manipulation and the techniques of fraud trigger people to make security-related mistakes. Training users about social engineering tricks can also be an effective preventive measure.

Phishing attacks, if not handled effectively, can lead to significant financial and privacy risks for organizations and individuals. The significant financial risk is mediated by users' unwillingness to proceed with transactions that require them to enter personal details like their banking information and credit card number. When customers lose confidence in the security of their financial details, they may be hesitant to exploit electronic facilities due to threats. The Internet provides a simple way to build virtual businesses and share details. The greatest challenge in the digitized environment is the protection of online interactions. Smartphones are used by a wide variety of systems with various activities that allow attackers an easy way to find access to the systems. Major crimes have been reported due to significant security challenges for cyber consequences such as hacking, spoofing, data breaches, and other serious crimes that have financial and reputational influence on any individual or entity. For activities like money laundering, financial fraud, matrimony scams, identity theft, and unauthorized financial transactions, banking system compromise has been reported.

3.2. Man-in-the-Middle (MitM) Attacks

Man-in-the-Middle (MitM) Attacks In a MitM attack, the attacker compromises the integrity of the communication between the user and the financial institution. This threat to communication integrity can result in significant financial and customer data loss. In a typical MitM attack, an unauthorized party intercepts a communication. By probing endpoint systems, i.e., probing ports and services of client or server computers, the attacker identifies a vulnerability in one of the systems. The attacker then leverages the vulnerability to inject a machine that can alter the communication. For example, in the case of unencrypted communication, the Man-in-the-Middle would have the ability to read, delete, or alter the data at his discretion. Such an attack can be used to carry out theft, such as theft of privacy, sensitive information, and funds. Generally, it is carried out over unsecured public Wi-Fi in a public place such as a café or during travel on trains or airplanes. Losses have been reported due to compromised mobile banking sessions by snooping over insecure Wi-Fi connections. The key reason

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(52s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

behind this attack is the general tendency of customers accessing their enterprise portals via Wi-Fi in enterprises. Therefore, it makes sense for an attacker to be in that same network or try to implement something like an ARP poisoning attack or a man-in-the-middle attack to intercept network traffic. The consequences of such a breach can be very severe, including locking out customers from their accounts, deleting transaction history, adding ghost employees to company payrolls, and modifying financial statements. End-to-end encryption of data can protect against it; it obviates the need for securing connections by providing multi-tier authentication. A random key is generated on the device that encrypts the data. The data is not decrypted again until it reaches the target device. Thus, if intercepted, the attacker does not gain anything because an encrypted stream is useless. Educating people about the risks of using Wi-Fi in a public place during financial transactions is critical as threats evolve every day. It is important that consumers remain vigilant. Mobile banking is on the rise; vigilance needs to be a priority.

4. RISK MANAGEMENT FRAMEWORKS IN MOBILE BANKING

Risk management can be understood as taking rational measures to minimize the probability of a threat materializing, as well as the extent of its adverse impact. In the mobile banking industry, such rational measures can take the form of structured frameworks developed for the sole purpose of guiding directors, CEOs, CTOs, and CISOs in recognizing and identifying security risks, profiling these risks, managing and mitigating these threats, and ensuring compliance in the context of an ever-evolving statutory and regulatory regime. Risk management is a structured approach to identifying, assessing, and making explicit management and operational decisions about the risks to the confidentiality of sensitive customer financial information, the vulnerability window exploited by threat agents, and then the integrity and availability of financial transactions between banks and their customers. At the operational level, this involves looking into customer data and the delivery of BV products to SME and household clients. The risk management framework manages these risks as part of the banks' and, eventually, also BV's risk management strategy according to the strategic objectives stated in the Aspiration Document.

Several omni-risk management approaches and frameworks help us understand how to ensure such compliance. These approaches and frameworks have also been designed to aid in the consistent evaluation of governance and risk management; risk assessment, attack prevention measures, risk mitigation, and risk management outcomes; as well as continual improvement of BV’s risk governance capabilities. An Information Security Management System (ISMS) encompasses technical, human, and physical aspects in the B-C-B BV delivery channel while safeguarding both customer and bank information, and ensuring the level of service agreed upon between the customer and bank is realized. Movement towards the internet and even mobile banking also results in transactions being conducted remotely without a face-to-face meeting between the customer and bank clerk. The framework uses industry best practices, standards, and guidelines to manage cybersecurity risks. The framework provides a common language to address and manage cybersecurity risk in a cost-effective way, based on business needs, without placing additional regulatory requirements on businesses. While not prescriptive, the framework is a set of challenges, priorities, and specific action items. It is broad-ranging and gives organizations quite a bit of flexibility in picking and choosing activities that best fit their particular needs, culture, and industry requirements.

4.1. ISO/IEC 27001:2013

The International Organization for Standardization and the International Electrotechnical Commission provide requirements to organize information security in organizations. Its procedures allow organizations to manage their data security appraisal system. Based on the principles of these standards, organizations can develop Information Safety Management Systems. This international standard will help organizations manage and secure sensitive information using a systematic approach

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(52s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

to threats, vulnerabilities, and risks. Adopting this standard can help any organization prevent various threats and protect their banking sector even in a vulnerable cyber environment.

The framework can be adopted in managing sensitive mobile banking systems using controls. This audit approach minimizes the magnitude of risks associated with security attacks and automates recurring risk assessments. An external agency's evaluation on updated adherence to standards would allow a banking organization to be a reliable source in the production of stable and trustworthy mobile banking systems. Employee training should emphasize recognizing the importance of information security standards in customer privacy concerns and system safety. It provides insight into how organizational operations and regulations may cause mobile banking threats. It also discusses the requirements, scope, and objectives of adopted methods in the control of mobile banking within the rules. Internal audits face information security requirements to protect an in-scope area of banking, banks, or financial institutions. These methods decrease the risk of policy failure events. The exact allocation of duties decreases the hazardous material flow. If any system failure arises, they should requalify in the future in order to address compliance issues. The extent of problems, processes, operations, services provided, and services offered by the organization that were in or out of the scope of the template is discussed. Personnel with special needs are trained before the system goes live. Meetings are regularly held with the respected stakeholders to provide them with progress on the system development lifecycle. Therefore, keeping in view the rapid increase in banking activities and mobile banking transactions and increasing security threats due to the internet, it is very important for banks and financial institutions to have excellent security mechanisms in place, so that no security breach occurs. This standard basically revolves around the management of any organization’s information assets, ensuring their effective protection. Increased adoption of this standard in banks will not only benefit the banks in maintaining secure solutions, but it will also be beneficial for the customers of the bank to carry on secured and safe banking transactions, whether they are using mobile banking or any other electronic channel for bank account transactions.

4.2. NIST Cybersecurity Framework

With the growing occurrence of cyberattacks on industry sectors like power, finance, information technology, and communication, it is necessary to have a guide that can be used to manage cybersecurity risks. The development of the Cybersecurity Framework started with extensive involvement from a diverse group of organizations providing various services and developing themselves. The framework is intended to be used by organizations to manage and mitigate cybersecurity risk based on inherently recognized business requirements without placing requirements on the use of specific technologies, industry sectors, or services, leveraging existing practices. The framework for improvement is based on the implementation of the risk management framework as well as the plan-do-check-act management system. These elements are enhanced with the seven high-level outcome categories derived from different industry standards and best practice documents.

The Cybersecurity Framework's foundational model of identify, protect, detect, respond, and recover provides a set of core, high-level cybersecurity functions of the activities that must be achieved for an organization to fundamentally and effectively address threats and vulnerabilities that could result in physical and reputational harm or financial loss. Implementation of the framework is inherently flexible, scalable, and adaptive to the environments and needs of organizations with differing attack and event dependencies, differing missions, business objectives, and resources. When implemented, the framework for improvement and approach should improve the resilience of organizations against cyberattacks, reducing the occurrences of such incidents. The framework can be used by any organization, large or small, including diverse public and private sector entities, from multinational firms representing large industrial and critical infrastructure to small business enterprises. Some of the benefits that could be achieved include improving or increasing the preservation of the institution's stability and reputation by elaborating and developing risk management practices and processes. This

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(52s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

includes translating risk into economic and financial terms, enhancing situational awareness, measurement infrastructure, and standards. The framework, by design, is intended to assimilate and leverage existing security practices and enable an organization's risk management practices for improved standards and reusability. Failure to enhance existing security management processes, but instead allowing them to continue diverging, is expected to increase cybersecurity vulnerabilities. The framework integrates and synthesizes existing security standards, guidelines, and practices, prioritizing them for common-sense use by practitioners. It is flexible, allowing access, reference, and use by organizations of all sizes. Organizations most reliant on operationalizing cybersecurity standards can find essential support by adopting the framework. Systemically, adversarial behavior can be deterred through systematic risk-based management processes. Identifying, analyzing, treating, and communicating risks signify an effective risk management approach. Contingency planning helps provide training, testing, and continuous improvement of plans to ensure proper steps are taken to prevent, protect against, mitigate the effects of, respond to, and recover in the event of any potential risk.

5. SECURITY TECHNOLOGIES AND SOLUTIONS

To secure the customer's integrity and confidentiality, banks are implementing various security technologies. As a result, the banks' IT systems are safeguarded from unauthorized access. The various security solutions provided by the banks have been found to help the banks overcome identified challenges. The security solutions, including end-to-end encryption and multi-factor authentication, are effectively reducing the chances of a security breach impacting customer satisfaction. The banks are using end-to-end encryption as a critical technology for securing the communication channel. Multi-factor authentication is used by banks for mapping fraud and easing customer worries. It improves communication, protecting consumers and banks by authenticating the user's right to access and use banking solutions while blocking out illegal users. It has saved the bank from unauthorized access and users' accounts from fraudulent activities.

End-to-End Encryption means encrypting data in transit such that the primary data itself is not visible to third parties in any way; only the encrypted form of the data is transferred. The objective of end-to-end encryption is to ensure the confidentiality and integrity of mobile banking transaction data as it is actively being transmitted. It is currently recognized as a valuable and efficient means of reducing unauthorized access to confidential customer data in transit on an open, unprotected wireless network and mitigating the delivery of malware. Multi-Factor Authentication is a method of computer access control in which a customer is granted access only after providing two or more proofs of their identity by presenting their identity, then a token, and providing information that only the user knows. Input knowledge may include a personal identification number or a password and may also involve the answer to a "secret question." The objective of multi-factor authentication is to ensure the identity of a mobile banking user, ensuring its confidentiality and integrity. The bank asks the customer to go through more than one authorized access potential, ensuring that the right to access banking services, access accounts, and perform financial transactions rests with the authorized person, not the imposter. To avoid fraudulent access to customer funds, banks routinely examine the authentication status of relevant consumers through internal technology and other external databases. Providing multi-factor authentication is a move to increase the difficulty of fraudulent access. If a hacker wants to obtain unauthorized access to a financial enterprise, they must first know the user ID-password pair and then possess a requisite protocol tool that will deliver the "second factor." In the case of a stolen or hacked "first factor," the hacker is expected to find their way past the "second factor," which is tough, if not impossible. While multi-factor authentication is not guaranteed to prevent fraud in any case, it undoubtedly serves as an excellent deterrent. It serves as a buffer against hackers and falsifiers attempting to enter a system or steal account login information. With multi-factor authentication in place, hacking accounts becomes a more complex and time-consuming process.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(52s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5.1. End-to-End Encryption

End-to-end encryption is the encryption of data so that it is only readable by the sender and the recipient, safeguarding it from potential eavesdroppers. Even if anyone manages to access the data in transit, it cannot be read without the associated decryption key. It is crucial for the confidentiality of data being exchanged, as it ensures that not even the medium facilitating the communication is able to interpret the data being carried. It is critical in mobile banking, where data travels all over the internet. End-to-end encryption is of utmost significance, as it safeguards the information from unauthorized access, alteration, or theft by untrusted intermediaries. End-to-end encryption thus adds a layer of confidentiality between the app user and the banking institution.

Data breaches have been in the news for the past few years. In a bid to keep the databases of customer information secure from data breaches, companies are adopting the end-to-end encryption approach. For our application, we can follow the same approach and use end-to-end encryption to encrypt sensitive information shared within the app. However, one of the biggest challenges that can arise in our scenario is managing the keys securely. In end-to-end encryption, the keys for encryption and decryption will be on the user devices. Here are a few best practices for implementing end-to-end encryption: key management, key exchange mechanism, cipher suite and session establishment, secure error handling, and so on. Although end-to-end encryption is said to be the silver bullet for sensitive information protection, there are potential trade-offs too. Performance, computations, memory, and user experience could be the primary challenges when we implement end-to-end encryption. Also, implementing end-to-end encryption in the new application is recommended rather than adding it later in third-party institutions.

5.2. Multi-Factor Authentication (MFA)

5.2. Multi-Factor Authentication (MFA)

Overview MFA is an additional security mechanism that enforces security measures with the use of multiple components to ensure that the user is who they claim to be. One of the most common forms of MFA is to send a one-time password when someone tries to register with a service or log in to a service. Biometric verification, hardware tokens, software tokens, smart cards, etc., are other forms of MFA. Biometric verification, used at ATMs that now support fingerprint authentication instead of an ATM PIN, makes transactions more secure and helps reduce theft when an unauthorized person gets the ATM card. The one-time password is another mechanism in which the one-time password is generated and sent to customers, without which the transaction cannot be completed. From the mere use of passwords for software security about one or two decades ago, it's a world of difference now. Any transaction on a web server or mobile device...

6. CASE STUDIES AND INCIDENTS IN MOBILE BANKING SECURITY

Hu, Chinnappan, and Bolic introduced cases of cybersecurity incidents in the digital environments specifically targeting mobile banking, depicting the manifesto of the active changes in the security arena. A brief overview of the incidents is as follows: The State Bank of India, the Union Bank of India, the HDFC Bank, the National Cash Register Corporation, and the Australian Government Services reported that their customer details, including driver's licenses, passport details, bank account information, and much more, were among the stolen items. The data included were up to date at the time of the theft. In continuation, the Union Bank of India reported that a portion of the stolen data logged was related to their bank. Similarly, the HDFC Bank also had 9.6 GB of data breached.

Specific incidents reported were: On August 29, 2021, the NCR Corporation suffered a data breach in Las Vegas. The personal information of some of their clients was stolen, including customer names, addresses, emails, and bank account numbers. The case study raises an important concern over how, in today's digital world, algorithms work without fail or legal support from the justice system, while

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(52s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

criminals leverage the same platforms to identify their wrongdoings by combining public registry information with criminal activity to defraud financially secure entities. It is also interesting when the case is read in conjunction with analysis, as it brings up concerns about its validity, reliability, relevance, resources, rigor, and replicability, as suggested for the accepted work of academic research. This also depicts the vital role of investigations in an individual's life, as professionals must keep pace with current changes in the field in order to report accurately. It also raises the debate over the disproportion versus proportion of crime uncertainty and the need for resources to be helpful in times of societal need within a reasonable time.

6.1. Data Breaches and Customer Data Theft

6.1. Data Breaches

Data is the new oil; customer data is the mobile banking commodity; thus, there is a growing trend of data breaches reported from a variety of industries. Several techniques such as mobile threat risk, remotely controlled rogue applications, and distributed phishing cover pages designed by criminals describe how a criminal can change the backdoor for unlawful access in mobile networks. In addition to this, the literature primarily consists of analytical work carried out at a global level which focuses on the strategic framework, avenues, and techniques for mobile banking. A recent variety of phishing and fraudulent websites study findings, and value reproduction for similar companies have been undertaken to characterize the negative impact of website infectiveness on ongoing group attacks, including the website assessment methodology used for both man-in-the-middle and server compression technologies. We have been discussing mobile banking and mobile wallet applications that contain passwords and cryptographic rights. This reflects that there are very high assets that are at risk on mobile due to some kind of incident, containing more options as a part of the service. Security concerns and risk management in mobile banking from a perspective are not only about storing data on mobile but also about transferring crucial rights.

What were the largest data breaches and cyber-attacks in recent times that shook the markets and customer-serving organizations? The literature describes data breaches as occurrences when unauthorized individuals access sensitive login credentials, financial information, customer data, or other confidential data. Such activities can drive away customers and erode their trust, based on findings that showed the spread of the detrimental effects of breaches and turnover of mobile customers, with an estimation of a significant financial impact after the incident. The hacked identities resulted in a direct loss and revealed a cost for good accounts or service remediation. The compromise revealed the data for a long time and incurred notification costs due to the time of investigation. Cyber-attacks in other countries in developed areas indicate that concerns about data risk are victims of cybercrime. It is quite likely that this year a significant portion of the population is likely to have been affected. Attackers often use server information and channels to appropriate data, strike, modify personal information, and therefore also change system accounts, including records with banks. When considering attack channels, ransomware is highlighted as a major affecting factor in our lives. Immediate attention to data breaches improves the response and also minimizes the damage. The incident is depicted as a beautiful picture of the face-to-face experience and indicates that after acquaintance with the client, a bank can better prepare and reduce the monetary value of the fundamentals. Prosecutors learn from attacks on backdoors that deeper insight is important during future attacks and a more inclusive framework for IT infrastructure, software, and all types of partners. Currently, the bank relies on the standard of uncovering results. Nowadays, as the world grows faster and captures technological advancements, evolved offenders and good residues are currently capturing the global market. We should take preventive steps and understand the need for reduced perseverance.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(52s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

7. CHALLENGES AND FUTURE DIRECTIONS

The ever-evolving and highly complex nature of security for mobile banking is not without its challenges. The rapid technological advances usually outpace the already existing security measures. Mobile banking solutions have incorporated highly advanced security measures; however, the customer's ease and comfort in use have a direct impact on acceptance. Currently, most solutions demand a trade-off between security and usability, driven by the competition to add more features that provide greater usability. This can further lead to security vulnerabilities. On the other hand, as customers start to adopt newer technologies and their protection mechanisms, the expectation for high-level security by any bank or financial institution has also increased. Therefore, it is important to balance providing a highly secure system that does not deter customers from using it. Another challenge is the continuously evolving threat trends and techniques to meet the security levels of users while trying to remain ahead of the threats.

Threats are becoming more sophisticated and continue to pose a grave risk to banks and their customers' mobile banking systems. The banks, i.e., software developers and the banking infrastructure, need to adopt the latest available technical solutions, continually upgrade the security matrix, and expand awareness engagements to protect themselves and their customers. However, there can be different banks and institutions that may not have the knowledge or may be incapable of adopting the latest available security solutions widely used in financial institutions, especially in a diverse country where the digital divide exists. The future of mobile banking security is undoubtedly an evolving risk domain and should be addressed with a well-planned risk management approach rather than an ongoing existing network infrastructure security. In conclusion, all the stakeholders of this mobile banking ecosystem must understand trust as a virtual asset in fighting against mobile banking security risks in the long-term context. In addressing these challenges, it is also recommended to adopt artificial intelligence and machine learning to detect and mitigate vulnerabilities in new mobile banking applications. In addition to technological advancements, the future of mobile banking security should focus on creating more trust among the community they serve.

7.1. Balancing Security and Usability

The relationship between security and a well-thought-out end-user experience is very important. Users depend on banking applications for daily, real-time, high-stakes banking operations. Although an application could be designed using high-end security and asking for security controls at every level, it is not feasible due to end-user frustration. End users need applications to work with ease without a very low level of security checks and balances, which can be accepted by them. It acts as a door standing in the middle of security and usability. Security can be designed at the expense of usability, but it would not provide significant results due to very low end-user acceptability.

Thus, an approach to security at the expense of usability is not advisable. Mailing certificates, as a high-end security check, is a major pain for end users and has low adaptability. At a very minimum, end users shall react very little, and this results in the objective not being achieved to ensure secure communication. The aim shall be to provide a high level of usability and a low level of security threats. It also has an impact on customer risk management, as many security features might fail due to a high level of risk from environmental changes or the factors of theft and loss of user credentials. A user-friendly interface would always have the adaptability to overcome such instances. As users tend to change their mobiles, both prepaid and postpaid, the user PIN protection secures the application from mobile theft.

The purpose of security measures is to mitigate risk. It results in the loss of assets and affects profits. It also impacts customer satisfaction. Users shall end up satisfied if the bank enables them to verify its authenticity conveniently and securely. A customer shall feel happy if the website or the mobile banking interface has a secure transaction. In order to strike the right balance, a user-friendly interface would

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(52s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

result in a good experience while using and manipulating your mobile interface, no matter what the end objective is. It increases user engagement. An application that is free of hassles is a user-focused application, leading to repeated interactions and making the user trust the bank, supporting positive brand promotion. The negative impact shall be an easy way for fraud, which makes the application less usable and susceptible to phishing and hacking. In case of misuse, the customer account can always be restored with a history of a one-time password. However, phishing may lead to manifold customers being misled and reduce customer trust.

8. SECURITY AWARENESS AND EDUCATION INITIATIVES

Awareness and education of mobile banking users is important for reducing the risks and vulnerabilities of mobile banking. It should be the endeavor of management of mobile banking service providers to develop a security-conscious culture in the bank. The primary strategy in combating new security threats is to invest in user education. User education is a project worth investing in when it comes to counteracting phishing occurrences on the internet. It not only empowers users to avoid phishing attacks, but will also have a positive effect against other scams. It is a strategic goal for financial institutions, as well as other relevant authorities, to teach customers how to pay special attention to an abnormal website, email, or web content, as these may be attempts at identity theft or spreading malware.

Various security awareness and training programs for the orientation of management teams and security officers to credit union security measures, educational workshops, and marketing campaigns aimed at educating credit union staff, credit union members, and the general public were deliberately organized by the above institutions. Education about the safe use of the internet and safe online banking was the central message. The participating institutions emphasize collaboration with the relevant authorities. The approach is to implement a program that will help improve the users' knowledge and understanding of the normal and acceptable use of information, the risks to data, and the measures taken to protect it. A user base with a satisfactory level of awareness is of crucial importance to security practices that hope to succeed. Raising awareness of users will mitigate many of the risks and reduce the occurrences of security breaches; it will have a direct bearing on security practices. Additional management plans and procedures detail the aims of the organization’s security education and awareness strategies for staff. The primary aim of the strategy is to maintain and enhance customer confidence by increasing staff awareness and understanding of potential threats, as well as the means to minimize the risks posed. By training the user, the organization can reduce the incidence of willful or malicious security incidents.

9. CONCLUSION AND RECOMMENDATIONS

Cybersecurity in specialized as well as emerging technologies such as mobile banking is critical to consider in this technical era. It is revealed that most banking customers are concerned about mobile banking security. The investigation shows that regulatory changes and various network attacks are currently in operation. Furthermore, it was found that banks have already experienced data loss with mobile banking services, and this kind of event happens in banks once a year. Mitigating this breach involves implementing effective security tools and technologies associated with mobile banking. Banking institutions also need to ensure that they are following essential security standards.

This draws attention to banking institutions to increase their commitment to the best risk management frameworks in the specific domain of mobile banking. This is achieved by rendering general data applicable to all stakeholders. Higher awareness of this will instill more commitment to the general framework, and this too adds to new best banking practices and knowledge trends in mobile banking. The analysis also concluded a need to establish a coalition where projects and initiatives comprise knowledge related to various safety issues and the preparation of industry leaders and fellowships presented to assist with their efforts. It is intended to further stimulate potential analysis to meet the

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(52s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

new future hazards. A mix of safety measures embedded in proprietary devices and software, together with typical measures strongly suitable for desktop and notebook banking, is essential. The built-in safety settings are, however, unique and highly secure for mobile banking devices. This process encrypts device data in an unencrypted encryption procedure and allows the encoded data to run securely between project servers. The report emphasized the need for a wide-ranging approval and top-level direction within the financial body, taking its service to a higher safety standard, particularly in the time-distinct, ever-consistent, and ever-favorable new response capacity to address the harsh cyber dangers. Furthermore, unauthorized focusing, in particular, is a unique plot component that should be assessed in their effort to look at top markets and business risks. The role of user knowledge in the battle with mobile banking insecurity should also be referred to on a long-term basis.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.