JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A STUDY OF CUSTOMER PERCEPTION TOWARDS SECURITY AND PRIVACY ISSUES OF ATM IN CHENNAI CITY.

Dr. S.Kala
Assistant Professor
Department of Bank Management
Anna Adarsh College for Women (Autonomous) Chennai.

Abstract

Indian financial innovation has combined client premiums, bank premiums, and nature to change banking from a traditional framework to a comprehensive one. The most common banking conveyance channel is an ATM, but password protection and identity theft are no longer adequate. Deduction charges in ATMs are the most significant determinant of security issues, according to a study on consumers' opinions of security and privacy concerns with certain public sector banks, particularly in the Chennai City.

Keywords: Digital Banking, Gender awareness, ATM security, Password protection, Identity theft.

I. Introduction

Banks are financial institutions that accept deposits and channel them into lending activities. The traditional banking system transitioned into e-banking, with the introduction of 'Any Branch Banking' and 'Core Banking Solution'. In India, the first green bank is the State Bank of India (SBI), which pioneered green banking under the leadership of Shri O.P. Bhatt. Green banking focuses on promoting environmentally sustainable practices in the banking sector, reducing carbon footprints. Technological advancements and changing consumer habits have transformed the Indian banking sector, with ATMs becoming the most popular delivery channel. ATMs revolutionized the banking experience by providing 24/7 access to cash and reducing the need for large amounts of cash.

II. Objectives of the Study

- To elaborate the ATM threats which can be segmented into card and currency fraud, logical attacks and physical attacks.
- To identify the users opinion on security and privacy issues of risk of ATM password theft.
- To assess the level of awareness on security risk in public wifi networks for digital banking on the basis of Gender.

III. Need for the Study

With the increasing reliance on Automated Teller Machines (ATMs) for financial transactions, concerns about security and privacy have become more prominent. ATMs offer convenience, but they are also vulnerable to various threats, including card skimming, malware attacks, logical fraud, and physical breaches. Customers' trust in ATMs depends on the perceived security measures implemented by banks. A lack of confidence in ATM security can lead to reduced usage and a preference for alternative banking channels. This study aims to understand customer perceptions of ATM security and privacy, assess the effectiveness of existing security measures, and identify areas for improvement to enhance user trust and safety.

IV. Review of Literature

- **Sayeed and Singh (2024)** explored the impact of security concerns on banking adoption, using qualitative and quantitative methods. It suggests that robust security measures and transparent communication strategies can boost e-banking adoption, despite technological advancements and changing consumer preferences.
- **Diptiben Ghelani and Surendra Kumar Redd (2022)** exhibited a solution to protect data against cyber threats in mobile environments, integrating machine learning, biometric recognition, and hybrid approaches into banking systems. This reduces intrusion risks and ensures secure transactions.
- **Pavithra B (2021)** highlighted the significance of digital banking for modern customers, highlighting its convenience and effectiveness. Surveying 150 users, it found a preference for smartphone-based digital banking due to its instant fund transfers and convenience.
- **Sankararaman, Suresh, and Kumar (2021)** examined the impact of cyber safety on consumers' behavior in trade and reimbursement schemes. The research involved gathering customer sentiments on cyber safety from 112 customers using convenience sampling, and analyzing the results through correlation analysis.
- **Luigi Wewege, Jeo Lee, Michael C. Thomsett, (2020)** Fintech and telecom firms are revolutionizing banking with user-centric digital services, despite facing trust and regulatory challenges. They are valuable partners for incumbent banks in digital transformations, emphasizing infrastructure capabilities, API standardization, and adherence to data protection laws.

V. Research Methodology

This research design is used to assess customer perceptions of security threats and privacy issues and the effectiveness of protective measures by using convenience sampling which was collected from 100 respondents.

VI. Security and privacy issues in ATM

The Automatic Teller Machine (ATM) was first commercially introduced in the 1960s. According to estimates by Retail Banking Research, there are 2,249,497 ATMs worldwide and expected to increase to 3,195,880 by end 2016 (Diebold). The introduction of the ATM proved to be an important technological development that enabled financial institutions to provide services to their customers in a 24X7 environment. The ATM has enhanced the convenience of customers by enabling them to access their cash wherever required from the nearest ATM. However, as the banker and the customer are not face-to-face, there is the risk of fraud, which may affect the customers and also the bank's reputation. ATM fraud is not confined to particular regions of the world. ATM threats can be segmented into three types of attacks: card and currency fraud, logical attacks and physical attacks.

- **CARD AND CURRENCY FRAUD**

Card and currency fraud may take place through both direct attacks to steal cash from the ATM and indirect attacks to steal a consumer‘s identity (in the form of consumer card data and PIN theft). The purpose of indirect attacks is to fraudulently use the consumer data to create counterfeit cards and obtain money from the consumer‘s account through fraudulent redemption. Brief description of card and currency frauds is given below:

- **SKIMMING**

These days, ATM card skimming is the most common and well known attack against ATMs. Card skimmers are devices used by fraudsters to capture cardholder data from the magnetic stripe on the back of an ATM card. These sophisticated devices, which are smaller than a deck of cards and resembling a hand-held credit card scanner, are often installed inside or over top of an ATM‘s originally installed card reader. When the consumer inserts his card into the card reader, the skimmer captures the card information before it passes into the ATMs card reader to initiate the transaction. When removed from the ATM, a skimmer allows the download of personal data belonging to everyone who used the ATM. Following are three kinds of card skimming attacks that can occur

- **External card skimming:** placing a device over the card reader slot (motorized or dip) to capture consumer data from the magnetic stripe on the card during a transaction. This is the most common form of card skimming.
- **Internal card skimming:** gaining access to the top hat of the ATM to modify the card reader or replace the original card reader with an already modified one for the purpose of obtaining consumer card data during a transaction.
- **Vestibule card skimming:** in locations where the ATM is located within a vestibule, skimmers are placed on the vestibule door card access reader to capture cardholder data from the magnetic stripe where the card is read so an unwary consumer inserts their card into the vestibule instead of on the ATM.

Fraudsters usually combine skimming attacks with other fraudulent devices such as covert cameras or keypad overlays that capture the consumer‘s PIN as it is being entered on the keypad during a transaction. Sometimes, fraudsters even install signs on ATMs instructing cardholders to ―swipe here first before continuing with transactions. Another fraudulent method is to portray the additional card reader as a card cleaner designed to extend the life and improve the performance of ATM magnetic stripes.

- **CARD TRAPPING/FISHING**

Card trapping and fishing attempt to steal consumers ‘cards itself rather than information on it. It takes place when a card is inserted into the card reader during a transaction. The purpose of this type of attack is to steal the card and use it at a later time to make fraudulent withdrawals from the consumers ‘accounts. Card trapping is conducted by placing a device over or inside the card reader slot to capture the consumer‘s card. These can be devices such as plates over the card reader, thin metallic strips covered in a plastic transparent film, wires, probes and hooks. These devices are designed to prevent the card from being returned to the consumer at the end of a transaction. These attacks are sometimes combined with other fraudulent devices such as cameras or keypad overlays to capture the consumer‘s PIN as it is being entered on the keypad during a transaction.

- **CURRENCY TRAPPING/FISHING**

Currency trapping and fishing is an attempt by perpetrators to capture currency that is dispensed by the ATM during a transaction. Trapping takes place when a false dispenser front is placed over the shutter of the dispenser with adhesive or tape on the inside to trap the notes before they are dispensed. Currency Fishing takes place by using the methods which are similar to those used to fish for cards. Wires, probes and hooks that are difficult for the consumer to see are used to prevent cash from being dispensed or deposits from being made. When the unwary consumer leaves the ATM, the perpetrator returns and uses the fishing device to retrieve the currency or deposit envelope.

- **LOGICAL/DATA ATTACKS**

Logical attacks target ATM software, operating systems and communications systems. Logical attacks can be some of the most damaging in terms of the quantity of consumer data compromised. The migration from proprietary operating systems to Microsoft Windows® technology has led to greater connectivity and interconnectivity of ATMs. Vast networks—including ATMs, branch systems, phone systems and other infrastructure connected via the Internet—are targets of logical security threats. Logical attackers include vandals who author viruses intended to exploit an ATM operating system and hackers who install malware to violate the confidentiality, integrity or authenticity of transaction-related data.

- **MALWARE AND HACKING**

With any computer system, the purpose of installing malicious software (malware) is to violate the confidentiality, integrity and/or authenticity of data on that computer system. These are designed to collect cardholders' data and/or dispense cash, malware and hacking can occur both locally or remotely. Local attacks operate by accessing the top hat and downloading the malware using a USB drive or attaching a USB sniffing device to intercept communication between the card reader and the ATM computer. Remote attacks on an ATM network occur at some point in the communication with the host or at the backend infrastructure. Typically, these sophisticated attacks are carried out by well-funded criminal organizations. Malware threats are of particular concern as they are on the rise and constantly evolving in an attempt to stay ahead of security measures.

- **PHYSICAL ATTACKS**

Physical attacks on an ATM include any type of assault that physically damages the components of the ATM in an attempt to obtain cash. While the entire ATM can be a target for a physical attack, specific components of the ATM are often targeted. Specific components, which may be targeted are Safe, Top Hat, Presenter and Depositor. Ramming, Pulling and Lifting are used to remove the entire ATM.

VII. Data Analysis and Interpretation

TABLE 1: AGE OF THE RESPONDENTS

Age group	No of respondents	Percentage
18- 25	58	58 %
26- 35	20	20 %
36- 50	18	18 %
Above 50	4	4 %
Total	**100**	**100 %**

Source:Primary Data

The table shows that the majority of respondents (58%) are aged 18-25, indicating higher engagement from younger individuals. The 26-35 and 36-50 age groups represent 20% and 18%, respectively, while only 4% are above 50.This suggests that younger individuals are more involved in the study.

TABLE 2: Security and Privacy issues while using ATMs (Risk of ATM Password Theft)

Response	Count & Percentage					Total
	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	
Risk of ATM Password Theft	43 (43)	26 (26)	14 (14)	12 (12)	4 (4)	**100**
Risk of ATM Card Cloning (Duplication)	48 (48)	21 (21)	17 (17)	11 (11)	2 (2)	**100**
Risk of ATM Dispensing Less Cash Than Requested	44 (44)	24 (24)	18 (18)	9 (9)	4 (4)	**100**
Unauthorized Cash Transfer Without ATM Card	45 (45)	25 (25)	13 (13)	13 (13)	3 (3)	**100**
Unauthorized Balance Deduction Without Transaction	38 (38)	22 (22)	18 (18)	12 (12)	9 (9)	**100**
Risk of Bank Sharing Card Information with Third Parties	39 (39)	32 (32)	14 (14)	9 (9)	5 (5)	**100**
Risk of Password Exposure While Entering PIN	36 (36)	25 (25)	18 (18)	13 (13)	7 (7)	**100**
Risk of ATM Card Getting Stuck and Not Returned	19 (19)	45 (45)	17 (17)	11 (11)	7 (7)	**100**

Source:Primary Data

This table highlights respondents' concerns regarding ATM security risks. The risk of ATM card cloning (48%) and password theft (43%) are the most concerning, followed by unauthorized cash transfers (45%) and ATM dispensing less cash (44%). Unauthorized balance deductions (38%) and bank sharing card information (39%) also raise moderate concerns. The risk of password exposure while entering PIN (36%) is acknowledged but not as alarming. However, 45% of respondents disagree that ATM card retention issues are a major problem. Overall, card cloning, password theft, and unauthorized transactions are the most significant security concerns among respondents.

Level of awareness on security risk in public wifi network for digital banking on the basis of Gender

Null Hypothesis (H_0): There is no significant relationship between Gender and Level of Awareness on Security Risks in Public Wi-Fi Usage.

Alternate Hypothesis (H_1): There is a significant relationship between Gender and Level of Awareness on Security Risks in Public Wi-Fi Usage.

Descriptive Statistics (Cross Tabulation)

GENDER / Level of awareness on security risk in public wifi network for digital banking	Agree	Disagree	Neutral	Strongly Agree	Strongly disagree
Female	19 (24.36%)	12 (15.38%)	31 (39.74%)	7 (8.97%)	9 (11.54%)
Male	6 (24.0%)	6 (24.0%)	11 (44.0%)	1 (4.0%)	1 (4.0%)

Chi-square Test Results

Test	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2.601	4	0.627

Interpretation

The Pearson Chi-Square value is 2.601 with a p-value of 0.627. Since the p-value is greater than 0.05, we fail to reject the null hypothesis. This means that there is no statistically significant relationship between Gender and Awareness of Security Risks in public Wi-Fi usage.

VIII. Findings

- 58% are aged 18-25, indicating higher engagement from younger individuals. The 26-35 and 36-50 age groups represent 20% and 18%, respectively, while only 4% are above 50.
- The risk of ATM card cloning (48%) and password theft (43%) are the most concerning, followed by unauthorized cash transfers (45%) and ATM dispensing less cash (44%). Unauthorized balance deductions (38%) and bank sharing card information (39%) also raise moderate concerns. The risk of password exposure while entering PIN (36%) is acknowledged but not as alarming. However, 45% of respondents disagree that ATM card retention issues are a major problem.
- No significant association between gender and awareness of security risks in public Wi-Fi usage ($p = 0.627$)

IX. Suggestions

- Implement awareness programs focusing on cybersecurity risks in public Wi-Fi usage, targeting all demographics rather than specific genders.
- Incorporate cybersecurity education into school curriculam and workplace training to enhance overall awareness.
- Encourage individuals to adopt safe online practices, such as using VPNs and avoiding sensitive transactions on public networks.
- Conduct further research considering factors like education, digital literacy, and prior cybersecurity experiences to better understand awareness levels.
- Expand the study with a larger and more diverse sample to identify key influences on security awareness beyond gender.

X. Conclusion

This study reveals that younger individuals, particularly females, are more engaged with digital banking, highlighting the growing reliance on technology for financial transactions. Mobile banking apps are the most preferred service, emphasizing the need for continuous innovation in app development and user experience. However, security concerns such as card cloning, unauthorized transactions, and privacy risks continue to impact user confidence, necessitating standardized security measures across all platforms. This research underscores the importance of consumer awareness programs to educate users on security best practices and fraud prevention. Lower-income users require targeted initiatives focusing on affordability, accessibility, and security to enhance trust and encourage broader adoption. By addressing these challenges, banks can create a more secure and inclusive digital banking environment.

XI. References

1. Diebold I. (2002). ATM fraud and security: White Paper, New York.
2. Donnell Yuks K. (2003), New System of banking; Drawill Publications, New York. 2003.
3. European Central Bank. (2015). Report on Card Fraud. https://www.ecb.europa.eu
4. Kingpin, F. (2018). Skimming and ATM Fraud: Understanding the Threat Landscape. SANS Institute.
5. “Enhanced ATM Security System using Biometrics,” Int. J. Comput. Sci. Issues, 2012.