ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 8.4
IJAR 2021; 7(4): 416-418
www.allresearchjournal.com
Received: 16-02-2021
Accepted: 26-03-2021

Surbhi Khanna
Assistant Professor,
Department of Computer
Science, Rajdhani College,
University of Delhi, New
Delhi, India

Aspects of advanced banking tools such as ATM security

Surbhi Khanna

Abstract

Enhancements in banking have made it easier for consumers to use their services. ATM services are one of the most important services provided by banks in terms of saving customers' time and resources. Present technologies advance quickly and are continually introducing new areas into our daily lives. This article provides a study of the research on security issues related to online banking and ATM transactions. When the number of online transactions grows, so does the need for quick and accurate user verification and authorization. According to the findings, E-banking and ATMs are very versatile modes of electronic banking. Our aim, like that of these surveys, is to test the efficiency of online banking and ATM transactions using multiple techniques such as biometric technology (thumb, iris, face recognition, etc.), two-way authentication, and three-way authentication. This article provides a brief overview of the evidence and discusses existing studies on various authentication issues in e-banking and ATM transactions.

Keywords: Online banking authentication, biometric, e-banking, verification

Introduction

Historically, banks seem to be at the frontline of using innovations to enhance their goods, services, and performance. For a lot longer, they have relied on digital and service productivity to offer a diverse range of valuation goods and services. Online banking is a convenient way in which to carry out banking tasks, such as managing bank accounts, checking an account transaction history, transferring money and paying bills. Internet banking is rapidly increasing and financial institutions are ever more alert to the challenges of developing an infrastructure to secure financial data. The security, authentication, trust and availability are, therefore, the major concerning E-banking.

The issue of security in E-banking has different dimensions from logical to physical security. Some banks allow customers for direct dial-in-access to their system over a private network while others allow network access through the internet. Counterfeiting of financial data such as credit card numbers, account usernames, password and social security numbers and hijacking banks brand names are the major problems encountered in the E- banking industry.

Objective of the study

- To study security issues related to online banking and ATM transactions.
- To get an overview of the existing studies on various authentication issues in e-banking and ATM transactions.

E-Banking System

E-Banking system constructed to provide simplified business activities at higher speed. For this purpose, e-banking uses latest computer technology to manage financial transactions more quickly and efficiently. banking applications greatly reduce the need of visiting a bank personally for completing transactions. Applications pertaining to general banking, finance and insurance come under e-banking applications. The Reserve Bank of India constituted a working group on internet banking, which divided the internet banking products in India into following 3 types based on the levels of access, granted.

Corresponding Author:
Surbhi Khanna
Assistant Professor,
Department of Computer
Science, Rajdhani College,
University of Delhi, New
Delhi, India

i) **i) Information-Only System (IOS):** There seems to be no way for an unregistered individual to gain access to the bank's web applications through the internet in this system.

ii) As the name implies, this method uses the bank's website to provide comprehensive information such as lending rates, branch locations, bank services and their functionality, loan and investment calculations, and so on. There are options for accessing different components of information forms based on the needs of the customer. For further inquiries, correspondence is done via e-mail in this section. Customers have no contact with the bank's application framework. There is no customer identifier.

iii) Electronic Data Interchange System: Digital data transfer systems are systems that could provide customer-specific data in read-only formats. Passwords are used to authenticate customers. The data was retrieved in batch process or off-line from the bank's software application. The performance measurements do not have direct internet connectivity. Account balances, transaction reports, statement of accounts, and other forms of information are some of the forms in which information is given

iv) Digital Transaction processing System: These systems are reversible and handle all transactions which include the customer and the bank. The transactions that the client has sent for online updates. These activities necessitate a high level of protection and supervision. The machine cannot go down in the middle of a transaction. As a result, a high level of control is necessary to maintain good state reallocation in the event that a device fails during a transaction. The web server and software systems are connected through a secure network. It includes automation, networking, and surveillance, as well as an inter-bank payment gateway and settlement system. Some of the popular applications coming under e-banking are discussed below :

1. **Automated Teller Machines:** An ATM is an Electronic Fund Transfer terminal that can process cash deposits, account transfers, balance inquiries, cash withdrawals, and bill payments. It could be either online or offline. The customer can use the on-line ATM to get banking services from everywhere. Off-line, the services are limited to the ATMs that have been allocated to them.
2. **Credit Cards/Debit Cards:** Under the limits set by his bank, the Credit Card holder is freedom to buy anywhere and everywhere he wishes with his Credit Card. A credit card is a reloadable card. A debit card, but at the other side, is a credit card with some stored value. When an individual uses this card, payment goes from the buyer's bank to the internet-banking house's account. The same sum of sales was debited from the buyer's account.
3. **Smart Card:** To boost protection, banks are introducing chips to existing magnetic stripe cards and introducing a new platform called smart cards. The amount of data that can be stored on smart cards is thousands of times greater than that of magnetic stripe cards. Furthermore, these cards are more stable, durable, and capable of performing multiple functions. From medical and health histories to personal banking and interests, a smart card can store a lot of personal details. Online bill payment, online fund transfer, online train passes, online stock market trading, online prepaid phone recharge, etc. that are all instances of services made possible by e- banking.

Security Requirements

Security is the primary concern for all organizations. Organizations are worried about the security of their stored and transported data. E-commerce and e-banking have their own special security problems, due to the remote access granted to their important information. According to the researches in the field, a few security requirements in e-banking can be recognized as follow :

1. Confidentiality: Confidentiality means ensuring that no one other than the expected parties is able to access the information. It is the idea of possessing sensitive data restricted to a precise set of individuals or organizations. Confidentiality guarantees that the data not shared with unauthorized entities.
2. Entity authentication: It is verifying that a user actually is who he or she claims to be. In the physical world, this commonly accomplished by use of a passport, driving license or ID card. From an ecommerce perspective, it must be possible remotely verify the identity of a user, before communicating with them (him/her). In e-banking, the two parties engaged in communication are the bank and the user.
3. Data authentication: Consists of both data origin authentication and data integrity, and ensures the users that the information they have received has not been manipulated (inserted, deleted, or substituted in any way) by unauthorized parties.
4. Non-repudiation: Non-repudiation is the act of assuring the origin and/or issuance of transaction or action so no one can falsely deny its previous actions and each party is able to prove to a third party that a user performed a certain transaction.
5. Availability: Availability ensures having an uninterrupted service.
6. Auditability: Means the ability of keeping a record of all transactions.
7. Authorization: It is controlling the actions of a person or entity, based on its identity.
8. Integrity: It is ensuring that a message cannot alter in any way during transmission. There has always been a demand for integrity when two or more remote parties need to rely on a given quantity of information.

Need for Improvement

There is a need for improvement of security in ATM transactions, due to tremendous increase in the number offenders and their activities, the ATM has become insecure. ATM systems today use no more than an access card and PIN for identity verification. The Personal Verification Number (PIN) not gives good security. The Physical Hardware (token) was duplicated by others. ATM would do the pin verification and token code identification through Database server. With Token code and pin verification one has embedded the Global System for Mobile Communications (GSM) modem connected to the microcontroller engenders the 4 digit one time password, which sends to the main user physical contrivance the user (main user), enroll the mobile number every physical contrivance that enrolls is checked by the database. The 4 digit one time password (OTP) should be entered by pressing the keys on the touch screen. After entering the entire correct information customer commences the further transaction. The Physical hardware (token) features are not replicated; this proposal would go a long way to solve the problem of account safety. An improvement to conventional ATM network paradigms involves the distribution of ATM switching functions across a large number of ATM switching units, each of which may typically provide a limited number of available ports, and by establishing multiple connections between the larger numbers of ATM switching units in a partially redundant "chained" configuration analogous to various ring type topologies.

References

1. Juergen Seitz, Eberhard Stickel. Internet Banking - An Overview www.arraydev.com, JIBC.
2. Lichtenstein, Williamson. Consumer Adoption of Internet Banking. Journal of Electronic Commerce, Research 2006;7:2.
3. Barskar Deen, Ahemed, Bharti. The Algorithm Analysis of E-commerce Security Issues for Online Payment Transaction System in Banking Technology. IJCSIS 2010;8(1).
4. Gunajit Sarma, Pranav Singh. Internet Banking: Risk Analysis and Applicability of Biometric Technology for authentication. International Journal Pure Application Science Technology 2010, 67-78. ISSN 2229-6107, www.ijopaasat.in
5. Sri Shimal Das, Smt. Jhunu Debbarma. Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System ISSN-2223-4985 International Journal of Information and Communication Technology Research 2011;1(5). http://www.esjournals.org
6. Bhosale ST, Dr. Sawant BS. Security in E-banking via Cardless Biometric ATMs. International Journal of Advanced Technology and Engineering Research (IJATER), ISSN no. 2250-3536 2012;2:4.
7. Zachary Nelson, Dr. Wanyembi. Security and Privacy of Electronic Banking IJCSI 2012;9(4):3. ISSN: 1694-0814, www.IJCSI.org
8. Navneet Sharma, Vijay Singh. Role of Biometric Technology over Advanced Security and Protection in Auto Teller Machine Transaction. IJEAT, ISSN: 2249-8958 2012;1:6.
9. Prof. Selina Oko, Jane Oruh. IJCSI International Journal of Computer Science 2012;9(3). ISSN (Online): 1694-0814, www.IJCSI.org