RESEARCH MATRIX :2321-7073
Peer Reviewed & Refereed | International Multidisciplinary Journal of applied research

ENHANCING SECURITY IN E-BANKING: THE ROLE OF CARD LESS BIOMETRIC ATMS

MS. ISHA TRIVEDI
RESEARCH SCHOLAR, ATMIYA UNIVERSITY, RAJKOT
DR.KAIRAVI RATHOD
ASSISTANT PROFESSOR,ATMIYA UNIVERSITY, RAJKOT

ABSTRACT
The introduction of biometric ATMs in India is a significant step in the banking industry. The technology allows for more secure and efficient authentication of users, which is crucial in preventing fraudulent activities. The use of biometric identification such as thumbprints, fingerprints, or iris scans ensures that only the authorized user can access their accounts, making it a safer option than the traditional card-based ATM system. Furthermore, the introduction of biometric ATMs also provides an opportunity for banks to expand their reach to rural and semi-literate populations. The talking biometric ATMs, which communicate in local languages, cater to the needs of farmers and other semi-literate individuals who may have difficulty operating traditional ATMs. Additionally, the use of mobile biometric access ATMs enables the bank to reach customers in remote areas where traditional ATMs may not be accessible.The proposed model for biometric ATMs that replaces the card system with biometric technology is a significant development that further improves the security and efficiency of banking services. By reducing the complexity of authentication and eliminating the need for plastic cards, the model offers a more environmentally friendly and cost-effective alternative to traditional ATMs.

KEYWORDS: BIOMETRIC ATMS, AUTHENTICATION, PIN, SECURITY, PLASTIC CARDS.

INTRODUCTION

Risk Mitigation:
Computers have revolutionized record keeping and made office automation cost-effective. With organizations sharing data across wide areas, LAN-based protocols are being converted into WAN-friendly protocols like TCP/IP. While this interconnectivity offers many advantages, it also introduces new risks. The computer systems that support critical services like telecommunications, power distribution, national defense, law enforcement, financial services, government services, and emergency services are at enormous risk. Security concerns arise due to the associated risk, threat, and vulnerability. Thus, it is crucial to prioritize security measures and safeguard against potential cyber-attacks that could have disastrous consequences for society as a whole.

OBJECTIVES:

1. To investigate the potential applications of biometric authentication methods in automated teller machines (ATMs).
2. To develop a module that enables easy operation of ATMs while ensuring secure authentication through networking.
3. Recommendations for the proposed model, highlighting its advantages and limitations.

LITERATURE REVIEW:
The adoption of biometric technology in banking and financial services is a growing trend that offers a range of benefits. However, convincing customers to switch from the tried-and-tested card-and-PIN system can be a challenge. Biometric technology offers a higher level of security than traditional authentication methods, and its non-repudiable nature makes it harder to imitate or duplicate. As

AvivahLitan, an analyst with Gartner Inc., notes, biometrics is the most secure form of authentication available.

Furthermore, biometric technology offers greater convenience to customers, as they no longer need to carry an ATM card or remember a PIN. In South America, where citizens are already accustomed to using fingerprints for general identification, biometric-enabled ATMs have gained traction. For example, BanCafe, Colombia's fifth-largest bank, bought 400 biometric-enabled ATMs in 2002 to provide added security for coffee growers and encourage them to open accounts without needing to carry ATM cards.

Overall, while there may be challenges in convincing customers to switch to biometric authentication, the benefits of increased security, convenience, and unique identification are compelling reasons for banks and financial institutions to continue exploring this technology.

IDENTIFICATION AUTHENTICATION

Identification is the process of establishing a user's identity, whereas authentication confirms a user's claim to a specific identity using credentials. Biometrics is a highly reliable method for authentication. Identification involves a system that recognizes a user's unique traits and determines their identity, such as using hand geometry to recognize Doctor Hunk. Authentication, on the other hand, involves a user presenting their credentials to prove their identity, such as presenting their hand for biometric recognition. Biometric authentication is feasible today and offers a reliable and secure method of confirming a user's identity.

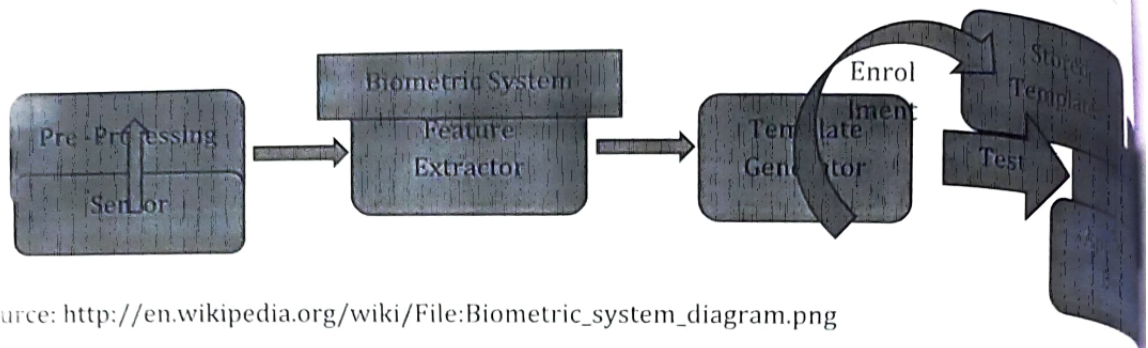
BIOMETRIC AUTHENTICATION

Biometrics refers to the use of physical characteristics of the human body to authenticate an individual's identity. There are two categories of biometric identifiers - physiological and behavioral. Physiological characteristics include fingerprint, face recognition, DNA, palm print, hand geometry, iris recognition, and scent. Behavioral characteristics include typing rhythm, gait, digital signature, and voice. Biometric authentication is considered more secure than traditional access control systems based on tokens or knowledge, as it is difficult to fake or steal a person's physical characteristics. The list of biometric authentication technologies is constantly expanding, and they are increasingly being used in various applications, such as security, access control, and payment systems.

Biometric authentication is becoming increasingly popular due to its many advantages. Biometric recognition devices are now capable of recognizing fingerprints, hand geometry, retina and iris, voice, handwriting, blood vessels in the finger, and face. One of the most significant advantages of biometric authentication is that it is nearly impossible to lose, steal, forget, lend, or forge. When combined with a password or PIN, biometric authentication can provide a foolproof way to use ATMs. Biometric authentication is receiving widespread attention from the public, and a biometric device can be considered the ultimate method of proving one's identity.

WORKING OF BIOMETRIC AUTHENTICATION

Biometric devices are electronic gadgets that use unique human characteristics for authentication purposes. These features include fingerprints, voice, facial recognition, or iris patterns. Biometric devices can range from simple handprint detectors to complex identification patterns in the retina. When a user wants to access a secured area, they are required to provide a sample of their biometric characteristics, which are then matched with the ones stored in the user database. If the two samples match, the user is authenticated and allowed access. Biometric devices provide a high level of security as it is almost impossible to replicate or forge these physical characteristics, making it an ideal solution for security-sensitive areas.

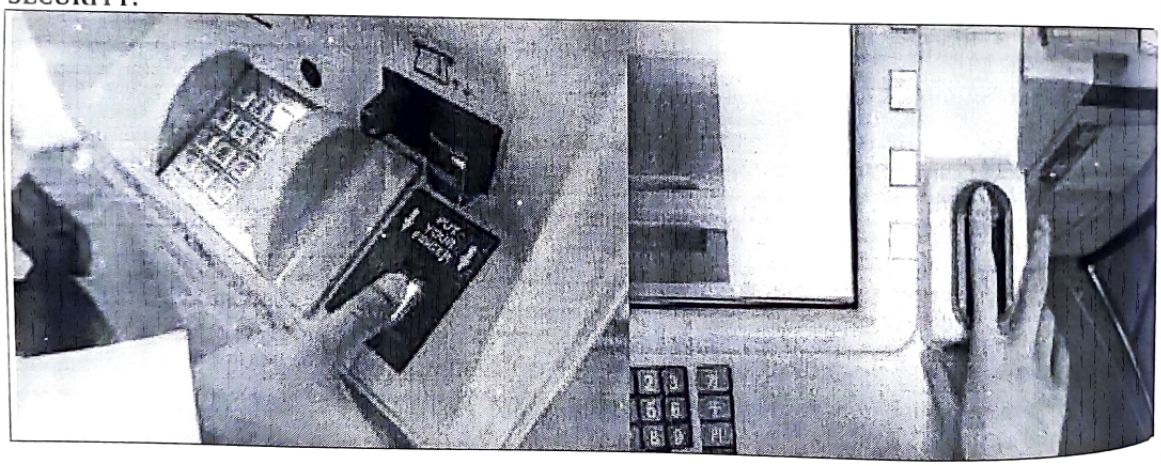


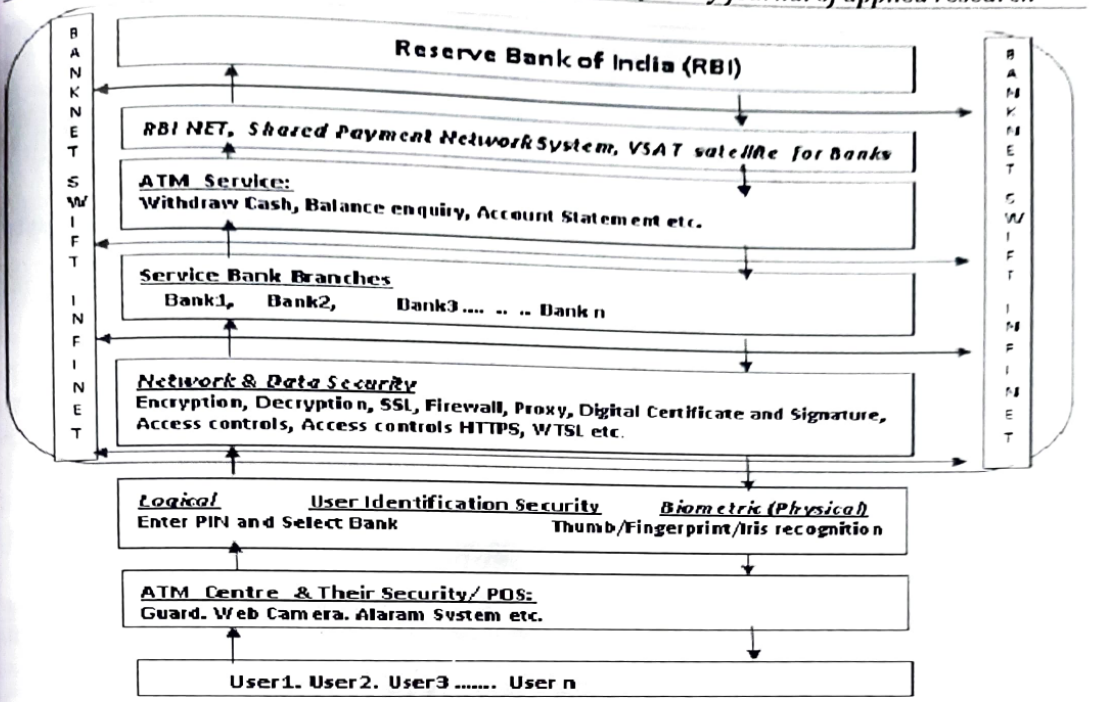
Source: http://en.wikipedia.org/wiki/File:Biometric_system_diagram.png

TECHNICAL SPECIFICATION

During the authentication process, it is common for there to be slight variations in matching biometric characteristics. This is because physical features of the user may change over time due to factors such as age, injury, or environmental conditions. For example, fingerprints may have cuts, other marks, or be positioned differently on the reader during each authentication attempt. Therefore, an exact match of the sample is not always necessary, and an approximate match can be acceptable. To address this, multiple samples of the user's biometric data are collected during the registration process. These samples are combined, and their average is stored in the user database. This way, during actual authentication, the different possibilities of the user's samples can be mapped to this average sample, allowing for a more accurate and reliable authentication process.

CONCEPTUAL MODEL FOR ATM BANKING WITH KNOWLEDGE BASED AND BIOMETRIC SECURITY:





WORKING:

A biometrics authentication process typically involves the creation of a user's biometric sample, such as a fingerprint, and its storage in a user database. During authentication, the user provides a sample of the same nature with a Personal Identification Number (PIN) and selected bank branch in a cafe center. The system generates a virtual account identification (V-ID) code and sends it encrypted to the server. The user's sample is decrypted and compared to the one stored in the database. If the two samples match, the user is considered authenticated and can proceed with transactions. If not, the user is considered invalid, and the session terminates. The process enhances security and reduces the risk of identity theft.

DRAWBACKS OF EXISTING CARD BASED ATMS

1. Having a card with a PIN code gives ownership of the account, without requiring additional identification of the account holder.
2. The current system operates with cards, causing longer processing times to be required.
3. Losing/stolen cards increase the risk of card misuse.
4. Replacing lost/stolen cards takes time and can be expensive for the bank.
5. Cards can become inoperable after several years or transactions, requiring the bank to provide a costly and time-consuming replacement.
6. Overuse of plastic cards harms the environment.
7. Managing and using multiple cards can be challenging for the account holder.

REQUIREMENT AND WORKING CONDITIONS:

1. For secure authentication, ATM centers need biometric devices and PIN pads to accept PINs.
2. Authentication needed for each transaction.
3. To maintain security, accounts should be blocked for the day if a user fails identification more than four times.
4. If an account is blocked more than four times in three months, the user must regenerate their authentication at their home bank.

ADVANTAGES OF CARD LESS ATMS

1. Ensures secure access with robust identification.
2. Biometric technology replaces cards by identifying physiological features of individuals.
3. By adopting alternative payment methods, expenses associated with ATM card management can be eliminated.
4. Suitable for Indian rural population.
5. An account holder can nominate an individual with valid identification to operate the same account.
6. Senior citizens benefit from not having to carry or maintain a card due to difficulty.
7. Eliminating card-related complaints such as theft, reissuing, and maintenance reduces cost, time, and effort for banks.
8. Convenient account access for service users.
9. Biometric authentication ensures account security against unauthorized access.
10. Biometric authentication ensures account security against unauthorized access.

LIMITATIONS

1. This method requires more ATM instruments and is more expensive to implement.
2. Biometric ensures exclusive account access to the account holder.
3. Multiple authentications make the initial stage time-consuming, requiring fast and efficient technology for system management.
4. If a user fails to provide correct identification in four attempts, their account will be blocked; after four blocks in three months, re-identification is required at their home bank.

SUGGESTIONS

1. Banks need dedicated, skilled technical staff to support and ensure user satisfaction with this system.
2. Banks should provide a demo room for showcasing new technologies to customers and staff, along with video conferencing for remote communication.
3. Promote e-banking among service users.
4. Banks can generate revenue and improve customer relationships by charging nominal fees for e-banking training services provided to account holders.
5. Banks should provide support to e-banking users for any issues or difficulties they face.

PROBLEMS WITH BIOMETRIC

1. Biometric techniques, such as hand geometry, fingerprint, and face recognition, are still relatively new and some find them intrusive. Although not entirely enveloping, people have concerns about the process of peering into a laser beam or placing their finger into a slot for identification purposes.
2. Biometric recognition devices can be expensive, but as their popularity increases, their cost is likely to decrease.
3. Biometric readers sample data and establish a threshold for accepting matches. They measure key points, compare with a template and account for normal variability. This involves hundreds of measurements, making it necessary to carefully establish acceptable thresholds.
4. Equipment improvements notwithstanding, false readings/recognition still exist.
5. Speed limits recognition accuracy.

FUTURE ATMS

ATMs currently rely on card systems and PINs, but there is growing demand for biometric authentication for better security. However, security experts have pointed out the potential for fingerprints to be lifted and replicated. The most secure biometric technology currently involves iris scanning, which uses over 2,000 unique measurement points. Developers believe that iris scan identification will become more widespread in the coming decades. Banks may also launch solar-powered and biometric with PIN-based ATMs in rural areas in the future.

CONCLUSION

The proposed conceptual model is designed for ATM and Point of Sales (POS) transactions using biometric authentication (such as fingerprint and iris recognition), PIN codes, and selection of bank branch to create a virtual account (V-ID) for identification and authentication. This cardless e-banking

technique reduces the risks associated with cards and simplifies the authentication process for Internet, mobile, and POS transactions. With its unique method of authentication, this system reduces the costs, time, and efforts of both banks and service users. By reducing the need for handling physical cards, it streamlines the process and provides enhanced security for users. Overall, this model represents a significant step towards a more efficient, secure, and user-friendly banking experience.

REFERENCES:

Biometric ATMs for rural India, ChirasrotaJena,Weekly Insight for Technology Professionals, 12, March 2007, www. Expresscomputeronline.com, Access date 16-Dec-2011

Handbook of Biometrics. Springer. pp. 1–22. ISBN 978-0- 387-71040-2. http://www.springer.com/computer/image+processing/book/97 8-1-4419-4375-0, access on 10-Dec-2011, 5.00pm

InternationalReferences: http://www.rediff.com/money/2005/oct/11atm.htm, Access on 16-Dec- 2011, 11.00 am

Jain, A., Hong, L., &Pankanti, S. (2000). "Biometric Identification", Communications of the ACM, 43(2), p. 91-98.

Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics", pp. 45-60

Krause Micki, Tipton Harold F., Handbook of Information Security Management (Imprint: Auerbach Publications) (Publisher: CRC Press LLC), ISBN: 0849399475, http://www.ccert.edu.cn/education/cissp/hism/ewtoc.html, data access on 13-Dec-2011, 3.50 pm

Laudon Kenneth, Traver Carol Guercio, E-Commerce (2005), Second Edition , pp. 237-239, Pearson Education (Singapore), Pvt. Ltd.

ONeil Erin, Back to the future at your local ATM, http://banking.about.com/od/securityandsafety/a/biometricatms .htm, access on 16-Dec-2011 at 11.45 am

Pfleeger Charles P., Pfleeger Shari Lacorence, Shah Deven N. (2009), Security in Computing, "User Authentication", pp. 257-258, IVth Edition, Pearson Publication.

S.C. Bihari, e-Banking, "When Convenience Banking can Become Inconvenience", pp. 52-55, First Edition, Skylark Publication, New Delhi

S.C. Bihari, e-Banking, "When Convenience Banking can Become Inconvenience", pp. 85-91, First Edition, Skylark Publication, New Delhi

http://www.indianexpress.com/news/district-gets-its-first- solar-biometric-atm/767886/, access on date 15-Dec-2011.