IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

A Review on Enhanced Security in ATM Transaction Using Fingerprint Authentication

Dr. Reshma Banu[1], Jawad Haris Khan[2], Mohammed Adnan Khan[3], Syed Ansar[4], Chandan B[5]
Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4,5]
Vidya Vikas Institution of Engineering and Technology, Mysore, India

Abstract: *The proliferation of automated teller machine (ATM) usage in modern banking has necessitated robust security measures to safeguard transactions against various threats. Traditional methods of authentication, primarily reliant on Personal Identification Numbers (PINS) and magnetic stripe cards, are increasingly vulnerable to fraudulent activities such as card skimming and PIN theft. In response, biometrical authentication, particularly fingerprint recognition, has emerged as a promising solution to enhance ATM security. The fundamental concept revolves around the biometric phenomenon known as "authentication". Within this project, we present an approach to fingerprint comparison centered on Minutiae Matching Algorithm. In an era where digital transactions are increasingly prevalent, ensuring the security of Automated Teller Machine (ATM) transactions remains paramount.*

Keywords: Minutiae Matching Algorithm, Biometrics, Fingerprint Authentication.

I. INTRODUCTION

Among the various methods employed for user authentication fingerprint recognition has emerged as a promising biometric technique due to its uniqueness and reliability. Fingerprint authentication has emerged as a promising solution to address the vulnerabilities associated with conventional ATM security methods. Fingerprint biometrics offer several advantages, including uniqueness, permanence, and the convenience of not requiring users to remember passwords or carry physical tokens.

This survey paper aims to comprehensively explore the landscape of enhanced security in ATM transactions through fingerprint authentication using the Minutiae Matching Algorithm. Through an exhaustive review of existing literature, we will delve into the underlying principles of fingerprint recognition, elucidate the intricacies of the Minutiae Matching Algorithm, and examine its efficacy in bolstering security measures within ATM environments. Minutiae Matching is a widely adopted approach in fingerprint recognition that involves identifying and comparing the minutiae points such as ridge endings and bifurcations, between the stored template and the live fingerprint image.

II. RELATED WORK

Fingerprint Identification Process

Many Fingerprint Scanning devices rely on intricate Minutiae. However, a challenge of image matching lies in its sensitivity to the accuracy of the finger during verification, coupled with the substantial template generation. To authenticate fingerprints, a device must first capture the fingerprint and then subject it to an algorithm for matching. This study delves into the precise intricacies of detection algorithms to elucidate the essential requirements of fingerprint images for recognition purposes. The advancement of biometric methods, particularly the remarkable evolution of recording devices, has paved the way for the widespread integration of fingerprinting across various applications in recent years. Minutiae details stand as the predominant factors in quitting the algorithm performance biometric data is distinct and separate from personal information.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

Introducing A Replacement For Conventional Identification Methods

In response to the shortcomings of established recognition techniques, the developer has developed The developer has devised a new ATM client identification system aimed at thwarting theft and unauthorized access to personal data

This system incorporates an upgraded algorithm for fingerprint image enhancement and utilizes advanced microprocessor technology to bolster the security of both bank accounts and ATM machines. Miao et al have highlighted the pivotal role of Gabor philters in generating Gabor features, thereby enhancing various image types. Currently, fingerprint and voice recognition systems possess relatively smaller footprints compared to eye-based systems, which dominate the landscape. However, the efficacy of fingerprint mechanisms can be compromised by poor-quality fingerprint images, resulting in unaccounted features and diminished performance. Therefore, it is imperative for fingerprint identification systems to assist the quality and suitability of captured fingerprint images meticulously.

Enchanting Biometric Payment Systems

Improving the mechanism for fingerprint matching relies on leveraging spectral details attributes incorporating two feature reduction algorithms: Line Discrete Fourier transform feature reductions and Column Principle Component Analysis. Ensuring the security of biometric templates is paramount as they cannot be reverse-engineered to access personal data thus mitigating the risk of theft and unauthorized access. Fingerprint information typically encompasses impressions on the last joint of the thumb and fingers, with fingerprint cards often capturing portions of the lower finger areas. As contemporary technologies in cash processing evolve biometric payment mechanisms have garnered increased attention as a viable solution to combat identity theft. Their applicability spans historical present and conceptual realms showcasing their enduring relevance and potential impact.

Felicitating Electronic Money Transfers

Examples of digital currency include deposits electronic cash transfers direct deposits, payment processing, and electronic currencies. Digital currency serves as a means of collecting and transferring traditional currency through digital channels, distinguishing it from standard currency while maintaining exchangeability. Electronic cash transfers via ATMs represent a form of digital currency transaction facilitated by a certificate of indebtedness machines linked to electronic or remote systems, ensuring security through server-based protection measures. Additionally, digital security encompasses various tools methods, and procedures employed to safeguard data assets within systems. Data is recognized as a critical asset and is subject to protective measures designed to mitigate risks and ensure the integrity of transactions relative to their value.

III. EXPECTED OUTCOME

The assessment of the ATM system's security involves comparing its components or verifying the PIN code. The final result of the system relies on the alignment of fingerprint patterns. Beyond the customary methods of accurately capturing and validating client fingerprints provided by the administrator, the implementation of ATM security via fingerprint recognition encompasses these techniques. Significantly bolstered, the protective function ensures the state- fast verification of the client's identity. Constructed entirely on fingerprint technology, the system offers security, reliability, and user-friendliness. This technology stands as the most advantageous option for digital or electronic financial transactions.

IV. CONCLUSION

The integration of fingerprint authentication employee miniature matching algorithms represents a significant enhancement in security for atm transactions. Through these technologies, ATM systems are fortified against unauthorized access and fraudulent activities. The utilization of minutiae matching ensures a high level of accuracy in verifying the identity of users, thereby reducing the risk of identity theft and unauthorized transactions. Furthermore, the reliance in biometric authentication adds an additional layer of security that is both

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, May 2024

reliable and user-friendly. Overall, the adoption of fingerprint authentication with minutiae matching algorithms serves as a robust safeguard for ATM transactions, providing enhanced security and peace of mind for both financial institutions and customers a like.

REFERENCES

[1]. K.V.Gunalan,R.A. Sashidhar,R.Srimathi, S.Revathi & Nithya Venkatesan, Enhanced ATM Security Using Facial Recognition, Fingerprint Authentication and WEB Application, 2023

[2] Yoganandar Chandrasekaran, Chandra Reka Ramachandiram, Kuruvikulam Chandrasekaran Arun, Adoption of future banking using biometric technology in automated teller machine (ATM), 2022. S

[3]. D Anveshini, V Revathi, A. Eswari, P. Mounika, K. Meghana, D apana, pattern recognition based fingerprint authentication for ATM system, 2022.

[4]. Shaikh Mohd Faiz, Shaikh Nadeem, Motiwala Quasai, Dr. Shabina Sayed, Fingerprint Based ATM system, 2022.

[5]. T Sangeetha, M Kumaraguru, S Akshay, M Kanishka, Biometric Based Fingerprint Verification System for ATM machines, 2021.

[6]. Christiawan, Bayu Aji Sahar, Azel Fayyad Rahardian, Elvayandri Muchtar, Fimingershield ATM-Security System using Fingerprint Authentication, 2020.

[7]. URANG Awajionyi A. and Ojekudo Nathaniel A, Securing Automated Teller Machine Transaction Using Biometric Fingerprint, 2020.

[8]. Pushpa Choudhry, Ashish Tripathi, Arun Kumar Singh & Prem Chand Vashist, Implementation of Integrated Security System by Using Biometric Function in ATM Machine, 2020.

[9]. M Navin Kumar, S Raghul, K Nirmal Prasad, p Naveen Kumar, biometrically Secured ATM Vigilance System, 2021.

[10]. Abhinav Muley, Vivek Kute, Prospective solution to bank card system, using fingerprint, 2020