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 1, April 2024

OTP and Fingerprint Based ATM System

Prof. Sharda Chavan Jumdre[1], Ayush Vishnu Achari[2], Atulkumar Vinodkumar Sah[3], Tanushree Gopal Saw[4], Sushmita Hublal Bind[5]
Professor, Department of Computer Engineering[1]
Students, Department of Computer Engineering[2,3,4,5]
Loknete Gopinathji Munde Institute of Engineering and Research Center, Nashik, India

Abstract: *The solutions for ATM security are the topic of this study. In addition to using ATM pins, we will also use fingerprint or One Time Password (OTP) verification. The user of this system has the option of third-party authentication either transient or long-term. Throughout the entire procedure, the banker, who is the first party, will have a database with the customer's fingerprint and cellphone number. The ATM card and PIN will be provided by the banker. Following the entry of the ATM pin, the customer will be prompted to select between fingerprint and OTP verification for the transaction. Through a GSM module that is attached to the system, the OTP will be delivered to the customer's registered mobile phone.*

Keywords: ATM, OTP, fingerprint, ATM pin, mobile number

I. INTRODUCTION

With the advent of modern technology, there is a drastic increase in fraud. One easy way is ATM fraud which includes fraudulent cash transactions so there is a need to regularly develop consumer favourable systems to deal with these frauds related to ATM transactions may be of several ways viz. Eavesdropping, Spoofing, Skimming Attack, Card Trapping, PIN Cracking, Phishing Attack, ATM Malware, ATM hacking . Several biometric authentication methods can be used to minimise such cases which includes fingerprints, face, iris before any transaction through ATM. One approach to deal with ATM frauds is face detection technology . Here the transaction is allowed if and only if the face of the user is detectable. But it has a drawback that it does not authenticate the legal user of the ATM and instead it just asks for detectable face of suspects who tend to hide their face. Another approach is the iris recognition system. It has very high accuracy in verifying an individual's identity. It works on four steps- image acquisition, segmentation, encoding and matching but work is still going on to make this technology feasible and cost effective.The third approach is Palm Vein Technology to run financial transactions. In this system, the user is required to provide his/her palm vein since these veins are unique for each individual. It is being practised in Japan. But it requires an overall update of database which is a tedious and costly process .

II OBJECTIVE & SCOPE OF PROPOSED SYSTEM

1. The primary objective of the proposed system is to enhance the security and efficiency of authentication processes within various domains such as banking, e-commerce, healthcare, government services, and more The system aims to provide a robust and reliable means of verifying the identity of users through the use of OTPs and fingerprint biometrics.
2. Multi-factor Authentication (MFA): The system will implement multi-factor authentication techniques combining OTPs and fingerprint biometrics to ensure a higher level of security compared to traditional password-based authentication methods.
3. Secure Access Control: The system will control access to sensitive information, systems, or physical spaces by requiring users to authenticate themselves using OTPs and fingerprint scans.
4. User Registration and Enrollment: The system will facilitate the registration and enrollment of users by collecting necessary information such as mobile numbers, email addresses, and biometric data for fingerprint authentication.
5. OTP Generation and Delivery: The system will generate unique OTPs for each authentication attempt and securely deliver them to registered users via SMS, email, or other secure communication channels.

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 1, April 2024

6. Fingerprint Biometric Authentication: The system will capture and store fingerprint biometric data during user enrollment and authenticate users based on their fingerprint scans during login or access attempts.
7. Integration with Existing Systems: The proposed system will be designed to seamlessly integrate with existing authentication frameworks and systems, allowing for easy adoption and deployment across various platforms and applications.
8. Logging and Audit Trail: The system will maintain comprehensive logs and audit trails of all authentication events, including user authentication attempts, successful logins, and failed authentication attempts, to ensure accountability and traceability.
9. Compliance and Regulations: The system will adhere to relevant security standards, regulations, and compliance requirements such as GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and PCI DSS (Payment Card Industry Data Security Standard).
10. Scalability and Performance: The system will be scalable to accommodate a large number of users and authentication requests while maintaining optimal performance and reliability.

III. FEATURES OF PROJECT

- Enhanced Security Protocols
- Integration with Biometric Authentication
- Widespread Adoption in IoT
- Mobile Device Security
- Healthcare and Government Services
- Blockchain and Cryptocurrency
- Continuous Authentication
- Usability Improvements
- AI and Machine Learning Integration
- Standardization and Interoperability

IV. LITERATURE REVIEW

1. Security Enhancement: OTP systems provide dynamic passwords for each login session, significantly reducing the risk of password theft and unauthorized access compared to static passwords.
2. User Convenience: Fingerprint authentication offers a seamless user experience by eliminating the need to remember and input passwords, leading to higher user acceptance and satisfaction.
3. Vulnerabilities: OTP systems are susceptible to phishing attacks, interception of OTP delivery channels, and man-in-the-middle attacks, while fingerprint authentication systems may face challenges such as spoofing attacks.
4. Mobile Integration: Mobile-based OTP solutions leverage smartphones to generate and deliver OTPs, offering enhanced security and convenience for users accessing online services.
5. Biometric Uniqueness: Fingerprint authentication relies on the unique patterns present in an individual's fingerprints, providing a highly reliable method for identity verification.
6. Authentication Accuracy: Advancements in fingerprint recognition technology have led to higher accuracy rates, ensuring reliable authentication in various applications.
7. Hybrid Approaches: Combining OTP and fingerprint authentication systems can offer synergistic benefits, enhancing security while maintaining user convenience.
8. Anti-Spoofing Measures: Developing robust anti-spoofing techniques is crucial for ensuring the integrity and security of fingerprint authentication systems against spoofing attacks.
9. Regulatory Compliance: OTP and fingerprint authentication systems must comply with data protection regulations and industry standards to safeguard user privacy and security.
10. Future Directions: Future research should focus on addressing the vulnerabilities of OTP and fingerprint authentication systems, exploring innovative approaches to enhance security and usability in the evolving threat landscape.

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 1, April 2024

V. REPRESENTATION OF THE METHODOLOGY

One-Time Password (OTP) authentication is a widely used method for enhancing security in various systems and applications. The methodology behind OTP authentication involves several key steps to ensure secure access to sensitive information and resources. First and foremost, OTPs are generated using cryptographic algorithms such as Time-based One-Time Password (TOTP) or HMAC-based One-Time Password (HOTP). These algorithms generate unique, unpredictable strings of characters that serve as temporary passwords for authentication purposes. The generation process involves combining a secret key with a timestamp or counter to produce the OTP. Once generated, the OTP needs to be securely delivered to the user. This can be done through various channels such as SMS, email, or generated by a dedicated hardware token. The secure delivery of OTPs is crucial to prevent interception or unauthorized access by malicious actors. Upon receiving the OTP, the user enters it into the system for authentication.

On the other hand, fingerprint authentication systems, exemplified by technologies like ATUM, rely on biometric data to verify a user's identity. The methodology behind fingerprint authentication begins with the enrollment process, where a user's fingerprint is captured and securely stored in the system's database. This process involves scanning the user's fingerprint using a dedicated fingerprint scanner device and extracting its unique features. These features are then converted into a template or digital representation that serves as a reference for future authentication attempts. During authentication, the user's fingerprint is scanned again, and its features are extracted once more.

In summary, OTP and fingerprint authentication systems employ distinct methodologies to enhance security and verify the identity of users accessing sensitive information and resources. OTP authentication relies on the generation of one-time passwords using cryptographic algorithms and their secure delivery to users through various channels. Fingerprint authentication, on the other hand, utilizes biometric data captured during enrollment to verify a user's identity based on the unique features of their fingerprint. Both methods offer additional security layers beyond traditional password-based systems, mitigating the risk of unauthorized access and enhancing the overall security posture of the system

VI. PROPOSED SYSTEM ARCITECTURE

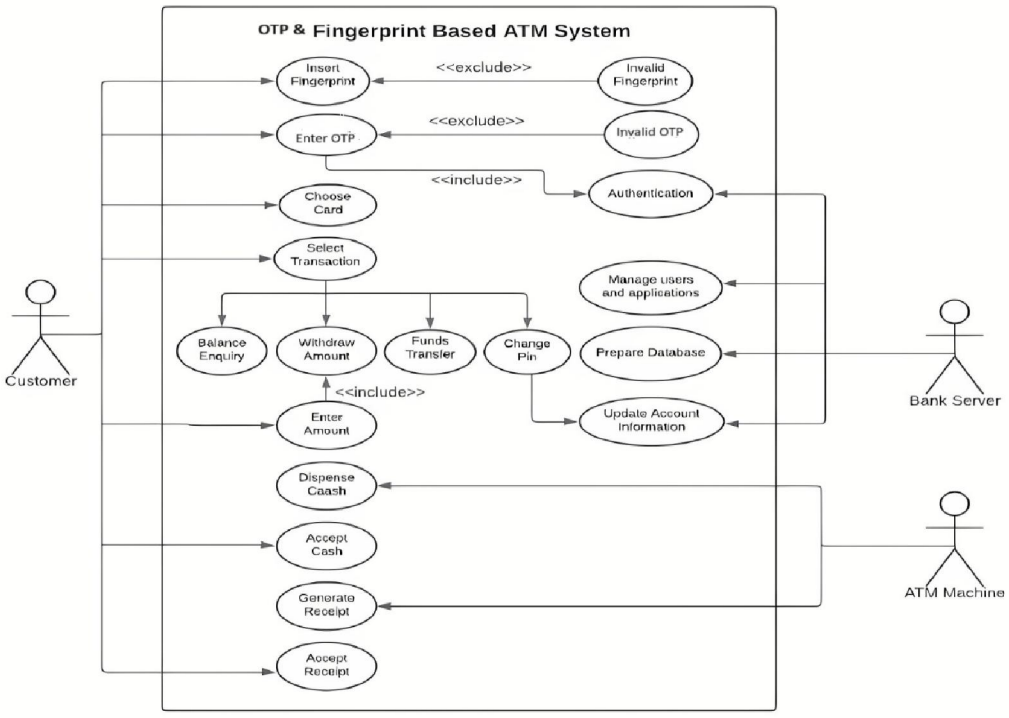

Figure: Proposed System Architecture

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 1, April 2024

VII. ADVANTAGES

1. Enhanced Security: OTP and fingerprint authentication add an extra layer of security to ATM transactions. OTP ensures that a unique password is generated for each transaction, which significantly reduces the risk of unauthorized access. Fingerprint authentication relies on biometric data, making it extremely difficult for fraudsters to replicate or bypass.
2. Reduced Fraud: By utilizing OTP and fingerprint authentication, the chances of fraud, such as card skimming or shoulder surfing, are minimized. Biometric authentication ensures that only the authorized user can access their account and conduct transactions.
3. Convenience: Users don't need to remember multiple PINs or carry physical tokens such as ATM cards. OTPs are typically sent to the user's registered mobile number, and fingerprint authentication eliminates the need for remembering passwords or carrying physical cards.
4. Fast and Efficient: OTPs are generated instantly and sent to the user's mobile device, allowing for quick authentication. Fingerprint scanning is also quick and seamless, reducing transaction time at ATMs.
5. Accessibility: Fingerprint authentication can be particularly beneficial for users with disabilities or those who have difficulty remembering PINs. It offers a more accessible and user-friendly option for ATM transactions.
6. Reduced Maintenance: With OTP and fingerprint authentication, there's less reliance on physical ATM cards, which can be prone to wear and tear or loss. This reduces the need for card replacements and associated maintenance costs.
7. Deterrent to Theft: The use of biometric data such as fingerprints makes it less attractive for thieves to steal physical items like ATM cards. Even if a card is stolen, without the associated fingerprint, it remains useless to the thief.

VIII. APPLICATION AREAS

1. User Enrollment: When a customer opens an account or applies for an ATM card, their fingerprint and contact details (phone number or email) are registered with the bank.
2. ATM Card Issuance: Each ATM card issued by the bank is linked to the user's account and their fingerprint data.
3. ATM Transaction Process:
4. Insertion of Card: When a user inserts their ATM card, the system prompts for fingerprint authentication before proceeding with any transactions.
5. Fingerprint Authentication: The ATM machine scans the user's fingerprint and compares it with the registered fingerprint stored in the bank's database. If the fingerprint matches, the user is prompted to enter their PIN.
6. OTP Generation and Delivery: After successful fingerprint authentication, the system generates a one-time password (OTP) and sends it to the user's registered mobile number or email address.
7. OTP Verification: The user enters the OTP received on their registered device. The system verifies the OTP entered by the user.
8. Transaction Authorization: Upon successful verification of both fingerprint and OTP, the user gains access to perform transactions such as cash withdrawals, balance inquiries, fund transfers, etc.
9. Transaction Completion and Receipt: After completing the transaction, the ATM machine issues a receipt to the user for their records.
10. Security Measures:
11. Encryption: All communication between the ATM machine and the bank's servers should be encrypted to prevent interception and tampering.
12. Data Protection: User fingerprint data and OTPs should be securely stored and transmitted using industry-standard encryption protocols to prevent unauthorized access.
13. Multi-factor Authentication: Combining fingerprint authentication with OTP adds an extra layer of security, making it harder for unauthorized individuals to access the user's account.

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 1, April 2024

IX. HARDWARE REQUIREMENTS

1. CPU Quad Core (not counting hyper-threading) 2.4Ghz, Intel VT or AMDV (Intel i3 or better)
2. Memory 4 GB
3. The ability to install more memory is desirable. Disk 512 GB SSD or better
4. Graphics Accelerated, Gaming Support Nvidia is preferred over AMD 1920 by 1080 resolution is recommended (at least on an external port) At least 1280 by 1024 resolution
5. HDMI output recommended (perhaps with an adapter)
6. Mouse An external mouse (USB or Bluetooth) is desirable.
7. USB USB 3.0 desirable for an external disk Other USB ports may be needed for: mouse, printer, mic-in, and headphones-out, depending on how these are connected.
8. External monitor A 23" or larger HDMI monitor is recommended, with reasonable resolution.
9. Laptop or Desktop Windows 11 or macOS 12.4 or above. Linux is also acceptable if a mainstream distribution (e.g. Ubuntu).

X SOFTWARE REQUIREMENTS

1. Operating System: Windows XP and later versions
2. Front End: HTML,CSS
3. Programming Language: NODE JS
4. Dataset: MongoDB
5. Additional Technologies: JavaScript and Bootstrap for enhancing the user experience with dynamic page elements, responsive design, and interactive features.

XI TEST DATA REQUIREMENTS

Unit Testing:

Unit testing in the context of our college forum project involves verifying the functionality of individual modules such as campaign, lead, contact, etc. Each submodule undergoes independent testing to ensure its proper operation. Input field validations are rigorously examined to detect any errors or inconsistencies within the module. By utilizing detailed design descriptions, we identify and test important control paths to ensure errors are identified within the module's boundaries.

Integration Testing:

Following unit testing, integration testing is performed to assess how individual units are integrated and function together within our college forum system. This phase ensures that no data is lost across interfaces, one module does not adversely affect another, and functions are executed correctly. Each submodule is thoroughly tested while integrating with others to ensure seamless functionality across the entire system.

XII SYSTEM TESTING FOR THE CURRENT SYSTEM

System testing for the college forum project involves evaluating the entire system after integrating all its main modules. The goal is to ensure that the system functions correctly and meets the desired specifications. Here's an overview of the testing approaches used:

1. Functional Testing: This testing phase focuses on verifying if the system functions according to its requirements. It involves testing features like thread creation, commenting, liking, and user profile management to ensure they work as intended.
2. Performance Testing: Performance testing assesses how well the system performs under different load conditions. It checks if the forum can handle concurrent user interactions, such as posting threads and comments, without significant slowdowns or errors.
3. Security Testing: Security testing evaluates the system's ability to protect user data and prevent unauthorized access. It involves testing authentication mechanisms, data encryption, and access controls to ensure user privacy and security.

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 1, April 2024

4. Compatibility Testing: This testing ensures that the forum functions correctly across different devices and web browsers. It verifies that users can access and use the forum seamlessly regardless of their operating system or browser choice.
5. Usability Testing: Usability testing assesses the user interface and overall user experience of the forum. It checks if navigation is intuitive, features are easy to use, and if the forum meets the needs of its intended users students, teachers, and alumni.
6. Regression Testing: Regression testing ensures that recent code changes or updates have not introduced new bugs or issues into the system. It verifies that existing functionality still works as expected after modifications.
7. Acceptance Testing: Acceptance testing involves validating the system's compliance with user requirements and expectations. It ensures that the forum meets the needs of its stakeholders and performs its intended functions effectively.
8. Recovery Testing: This testing evaluates the system's ability to recover from failures or disasters gracefully. It checks if the forum can maintain data integrity and resume normal operations after unexpected events.
9. Stress Testing: Stress testing examines how the system behaves under extreme load conditions. It assesses its resilience and performance limits by subjecting it to high user traffic or resource demands.
10. Exploratory Testing: Exploratory testing involves exploring the system to uncover any undocumented features or unexpected behavior. It helps identify potential issues that may not have been addressed in other testing phases.

XIII CONCLUSION

In conclusion, the implementation of OTP (One-Time Password) and fingerprint-based ATM systems represents a significant advancement in banking technology, offering enhanced security and convenience for users. By integrating biometric authentication methods with cutting-edge technologies such as blockchain, AI, and IoT, these systems pave the way for a future of secure, efficient, and user-friendly financial transactions. However, it is crucial to address concerns surrounding biometric data privacy and regulation while continuously updating cybersecurity measures to stay ahead of emerging threats. With a focus on scalability, interoperability, and improving the overall user experience, OTP and fingerprint-based ATM systems hold great promise in shaping the future of banking and financial services.

REFERENCES

[1]. Sergey Tulyakov, Faisal Farooq, Praveer Mansukhani, Venu Govindaraju, “Symmetric Hash functions for Secure Finger print biometric systems”.
[2]. Y.Donis, L. Reyzin and A.Smith, “Fuzzy Extractors”In security with Noisy Data: Private Biometrics, Secure key Storage and Anti-Counterfeiting, P.Tuyls, B.Skoric and T.Kevenaar, Eds., chpt5,pp.79-77, Springer-Verlag, 20012.
[3]. Direct Indirect Human Computer Interaction Based Biometrics International Journal of Emerging Engineering Research and Technology Volume 3, Issue 3, March 2015.
[4]. A.A.E. Ahmed, I. Traore, “A new biometric technology based on mouse dynamics, IEEE Transactions on dependable and Secure Computing” 4 (3) (2007) 165–179.
[5]. Deshpande, S. Chikkerur, V. Govindaraju, Accent classification in speech, Fourth IEEE Workshop on Automatic Identification Advanced Technologies, 17–18 October, 2014, pp. 139– 143.
[6]. F. Bannister and R. Connolly, “New Problems for Old? Defining e-Governance”, proceedings of the 44th Hawaii International Conference on System Sciences, (2012).