Automated Fee Payment Systems in ATM Enhancing Security & Efficiency Through OTP Verification

Soham Deshmukh[1] *Vidula Sardesai* [2] *Prachi Dharawane* [3]
Atharva Nanaware[4]

Zeal College Of Engineering & Research , Pune (Mechanical Department) [1]
Zeal College Of Engineering & Research , Pune (Robotics & Automation) [2 3 4]

Abstract

This paper explores the integration of automated fee payment systems in ATMs, focusing on the use of One-Time Password (OTP) verification to enhance transaction security and efficiency. The system allows users to authenticate their identity through an ID card, enter a unique Zero Payment Reference Number (ZPRN), and deposit the required fee. The ATM then sends an OTP to the user's registered mobile number, which the user must enter to complete the transaction. This method prevents unauthorized transactions, even if the ID card and ZPRN are compromised. The paper examines the design and implementation of these systems, their advantages, and challenges. It highlights how OTP verification increases security and user confidence, making ATMs a more reliable option for complex financial transactions. Additionally, it discusses the potential for future enhancements such as biometric authentication and blockchain technology to further improve ATM security and efficiency. Despite challenges like technical issues and the need for user education, the benefits of automated fee payment systems with OTP verification make them a significant advancement in financial technology.

Introduction:

The rapid advancement of financial technology in recent years has led to significant changes in how people and institutions handle money transactions. One notable innovation in this domain is the introduction of automated fee payment systems in ATMs, offering a more convenient and efficient alternative to traditional methods. These systems incorporate modern technology into ATM services, making fee payments easier and more secure. The use of One-Time Password (OTP) verification is a key component, in enhancing transaction security.

The process commences with the user inserting their ID card into the ATM, which then verifies their identity and links to their account. Subsequently, the user inputs their unique ZPRN (Zero Payment Reference Number), associated with the specific fee to be paid. After verification, the system calculates the total fee, often a substantial amount, such as 1.25 lakh (125,000). The user then deposits the required fee, and the system updates the remaining balance.

Upon completing the deposit, the system generates an OTP, sent to the user's registered mobile number. This step is critical for authenticating the transaction and ensuring only authorized individuals can finalize it. The user must enter the OTP at the ATM to complete the fee deposit. Upon successful verification, a transaction receipt is issued, confirming the payment.

The incorporation of OTP verification in automated fee payment systems addresses crucial concerns in financial transactions, particularly security and user confidence. OTPs, being unique and time-sensitive, effectively prevent fraud. Requiring this additional step ensures that unauthorized transactions cannot occur even if someone's ID card

and ZPRN are stolen, as the OTP is still needed.

This paper aims to delve into the specifics of automated fee payment systems in ATMs, focusing on the role of OTP verification in enhancing transaction security and efficiency. It will analyze the design and implementation of these systems, evaluate their benefits and challenges, and explore future trends and innovations that could further enhance their functionality. By examining these aspects, the paper aims to offer valuable insights into how automated fee payment systems can revolutionize financial transactions.

Literature Survey:

Automated fee payment systems are a major technological advancement in the financial sector, offering users a secure and efficient way to manage their financial obligations. Initially, ATMs were designed for basic banking tasks like cash withdrawals and account inquiries. However, ATMs have evolved to handle more complex functions like fee payments, bill payments, and other financial services. This survey examines the development of ATM functionalities, the role of OTP (One-Time Password) verification in enhancing security, and how these systems impact efficiency and user experience.

Early ATMs were primarily used for cash dispensing and checking account balances. Technological advancements have expanded their capabilities to include more complex transactions, such as paying fees. DeYoung, Lang, and Nolle (2007) noted that integrating additional services into ATMs has made them more useful, reducing the need for customers to visit bank branches and thereby increasing convenience and efficiency.

Security has always been a critical concern for ATM transactions. Traditional ATM security relied heavily on PIN-based authentication, which, while relatively secure, was still vulnerable to fraud methods like skimming and shoulder surfing. Introducing OTP verification has significantly reduced these risks. OTPs are dynamic, time-sensitive codes that provide an extra layer of security. Even if a user's primary credentials are compromised, unauthorized transactions cannot be completed with OTPs. Dunphy and Petitcolas (2018) highlighted that OTPs effectively prevent unauthorized access, making ATM transactions safer.

OTPs are now a standard security measure in many financial systems because of their effectiveness. Research by Pashalidis and Mitchell (2003) shows that OTPs significantly reduce the chances of successful fraudulent transactions. In the context of ATMs, OTP verification ensures that only the account owner can authorize fee payments, enhancing security.

Automated fee payment systems in ATMs also improve transaction efficiency. Automation reduces processing times and minimizes human error, making the payment process faster and more convenient. According to a study by Dahlberg, Guo, and Ondrus (2015), these systems are particularly beneficial in areas with limited banking infrastructure, where ATMs often serve as the primary access point for financial services.

User experience is crucial for the adoption of automated fee payment systems. Studies indicate that the convenience and ease of use of ATMs are major factors driving user satisfaction. Howcroft, Hamilton, and Hewer (2002) found that users value the ability to perform multiple transactions, including fee payments, at ATMs. While OTP verification adds an extra security step, it does not significantly impact the user experience because people are generally familiar with OTPs from online banking.

Despite the benefits, implementing automated fee payment systems in ATMs comes with challenges. Ensuring reliable network connectivity and maintaining ATM security are significant technical issues. Additionally, it is crucial to educate users about these systems and gain their trust in the security measures. Future research should focus on addressing these challenges and exploring emerging technologies like biometric authentication and blockchain to further improve the security and efficiency of ATM transactions. Liu and Silverman (2001) suggest that such technologies could enhance both security and user experience in the future. Overall, automated fee payment systems offer significant benefits by enhancing the capabilities of ATMs, improving security with OTP verification, and increasing transaction efficiency. User satisfaction and convenience are key to their adoption, despite the challenges in implementation and security.

Components:

1. User Interface Components:

- Card Reader: Reads data from the user's ID card (magnetic stripe or chip) to authenticate their identity.
- Keypad: Allows users to enter their ZPRN number, OTP, and other required information.
- Display Screen: Provides instructions and feedback to the user throughout the transaction process.

2. Security Components:

- One-Time Password (OTP) Generator: Generates a unique OTP for each transaction.
- OTP Delivery System: Sends the OTP to the user's registered mobile number via SMS or email.
-Encryption Modules: Encrypt sensitive data during transmission for security.

3. Software Components:

- Transaction Management Software: Manages fee calculation, verification, and account balance updates.
- Authentication Software: Verifies user identity through ID card and ZPRN.
- OTP Verification Software: Validates entered OTP against generated OTP.

4. Hardware Components:

- Cash Handling Mechanism: Facilitates cash deposit and counting. - Receipt Printer: Prints transaction receipts.
- ATM Enclosure: Protects internal components.

5. Network Components:

- Communication Interface: Connects ATM to bank's network for transaction processing and OTP delivery.
- Database Connectivity: Accesses and updates user data and transaction records.

6. Power Supply Components:

- Uninterruptible Power Supply (UPS): Ensures ATM operation during power outages.
- Power Management System: Regulates power distribution.

7. Monitoring and Maintenance Components:

- Diagnostic Tools: Monitor ATM status and detect faults.
- Remote Management System: Allows remote ATM management and troubleshooting.

***Security Component**

- OTP Generator: Creates time-sensitive passwords for transactions. - OTP Delivery System: Sends OTP via SMS for secure user authentication.
- Encryption Modules: Protect sensitive data during transmission.

***Software Components**

- Transaction Management Software: Manages transactions and updates account balance.
- Authentication Software: Verifies user's identity using ID card and ZPRN. - OTP Verification Software: Validates user-entered OTP against generated OTP.

***Hardware Components**

- Cash Handling Mechanism: Ensures accurate cash acceptance and verification.
- Receipt Printer: Generates detailed transaction receipts for users. - ATM Enclosure: Protects internal components and withstands tampering.

***Network Components**

- Communication Interface: Connects ATM to the bank's network for real-time data exchange.
- Database Connectivity: Allows ATM to access and update user data and transaction records.

***Power Supply Components**

- Uninterruptible Power Supply (UPS): Ensures continuous operation during power outages.
- Power Management System: Regulates power distribution and monitors power consumption.

***Monitoring and Maintenance Components** - Diagnostic Tools: Monitor ATM status and detect faults in real-time.
- Remote Management System: Allows remote monitoring and troubleshooting.

Integration Overview:

1. User Authentication:

- User inserts ID card for verification.
- Enters ZPRN number for database validation.

2. Fee Payment:

- Screen displays total fee.
- User deposits fee using cash handling mechanism.

3. OTP Generation and Verification:

- System generates OTP and sends it to the user's mobile. - User enters OTP on keypad.
- OTP software validates OTP.

4. Transaction Completion:

- Successful OTP verification finalizes the transaction.
- Receipt printer generates a receipt.
- Transaction details are updated in the bank's database.

Working:

1. ID Card Insertion:

- User inserts their ID card into the ATM card slot.
- ATM reads the card's magnetic strip or chip to authenticate the user's identity and link to their account.

2. Enter ZPRN Number:

- Users enter their unique ZPRN (Zero Payment Reference Number) using the ATM keypad.
- ATM verifies the ZPRN number against the database to identify the specific fee payment details.

3. Display Total Fee:

- The ATM system calculates and displays the total fee to be paid, typically a substantial amount like 125,000.
-The user confirms the amount to proceed with the transaction.

4. Deposit Fee:

- User deposits the required fee into the ATM.
- ATM counts and verifies the deposited amount, updating the remaining balance if necessary.

5. Check Remaining Fee or Confirm Completion: - System checks if the total fee has been completely paid. - If there is any remaining balance, the system notifies the user. - If the full amount is paid, the system moves to the next step.

6. Generate and Send OTP:

- ATM system generates a One-Time Password (OTP).
- OTP is sent to the user's registered mobile number via SMS.

7. Enter OTP:

- Users receive the OTP on their mobile phones.

The user enters the OTP into the ATM to verify the transaction.

8. OTP Verification:

- The ATM system verifies the entered OTP against the one sent to the user's mobile number.
- If the OTP is correct, the transaction is authenticated.

9. Transaction Completion:

- Upon successful OTP verification, the ATM system confirms the fee payment.
- Transaction details are updated in the system's database.

10. Print Receipt:

- ATM prints a receipt confirming the successful fee payment. - Receipt includes transaction details such

Code [Python]

```
import random

class ATM:
    def __init__(self, user_data):
        self.user_data = user_data
        self.current_user = None

    def insert_id_card(self, user_id):
        if user_id in self.user_data:
            self.current_user = self.user_data[user_id]
            print(f"ID Card inserted for user: {self.current_user['name']}")
            return True
        else:
            print("Invalid ID card.")
            return False

    def enter_zprn_no(self, zprn_no):
        if self.current_user and zprn_no == self.current_user['zprn_no']: print("ZPRN No. entered successfully.")
            return True
        else:
            print("Invalid ZPRN No.")
            return False

    def deposit_fee(self, amount):
        if self.current_user:
            total_fee = 125000
            self.current_user['deposited'] += amount
            remaining_fee = total_fee - self.current_user['deposited']
```

```
            if remaining_fee <= 0:
                print(f"Deposited {amount} successfully. Fee deposit complete.") self.current_user['fee_status']
                = "complete"
            else:
print(f"Deposited {amount} successfully. Remaining fee:
{remaining_fee}")
                self.current_user['fee_status'] = "incomplete"
            return True
        else:
            print("No user authenticated.")
            return False

    def get_otp(self):
        if self.current_user:
            otp = random.randint(100000, 999999)
            self.current_user['otp'] = otp
            print(f"OTP sent to registered number: {otp}")
            return otp
        else:
            print("No user authenticated.")
            return None

    def confirm_fee_deposit(self, entered_otp):
        if self.current_user and entered_otp == self.current_user.get('otp'): if self.current_user['fee_status']
            == "complete":
                print("Fee deposited successfully.")
                return True
            else:
                print("Fee deposit is not yet complete.")
                return False
        else:
            print("Invalid OTP.")
            return False

    def get_receipt(self):
        if self.current_user:
            print("Receipt:")
            print(f"User: {self.current_user['name']}")
            print(f"Deposited Amount: {self.current_user['deposited']}")
            print(f"Fee Status: {self.current_user['fee_status']}")
```

```
            return True
        else:
            print("No user authenticated.")
            return False

# Sample user data
user_data = {
    "123456": {"name": "Soham Prashant Deshmukh", "zprn_no": "122E10434", "deposited": 0, "otp": None, "fee_status": "incomplete"},
    "654321": {"name": "Vidula Sudhir Sardesai", "zprn_no": "XYZ789", "deposited": 0, "otp": None, "fee_status": "incomplete"}
}

# Initialize ATM instance with user data
atm = ATM(user_data)
# Simulate the process for user with ID card "123456" print("----- ATM Fee Payment Process -----")
if atm.insert_id_card("123456"):
    if atm.enter_zprn_no("122E10434"):
        if atm.deposit_fee(50000): # Example deposit amount otp = atm.get_otp()
            if otp is not None:
                if atm.confirm_fee_deposit(otp):
                    atm.get_receipt()
```

Compile Result

----- ATM Fee Payment Process -----

ID Card inserted for user: Soham Prashant Deshmukh ZPRN No. entered successfully.
Deposited 50000 successfully. Remaining fee: 75000 OTP sent to registered number: 707944
Fee deposit is not yet complete.

[Process completed - press Enter]

Advantages

1. Enhanced Security:

- OTP Verification: Provides an extra layer of security, reducing the risk of unauthorized transactions even if card details are compromised. - Encryption: Ensures data privacy and security during transmission.

2. Convenience:

- 24/7 Availability: Users can pay fees at any time without the need to visit a bank branch.

-Reduced Waiting Time: Automated systems minimize the time required for transactions compared to manual processing.

3. Efficiency:

- Streamlined Processes: Automates the fee payment process, reducing errors and speeding up transactions.
- Instant Updates: Real-time transaction processing and instant updates to the user's account.

4. Cost Savings:

- Operational Costs: Reduces the need for human tellers and administrative staff, lowering operational costs for banks.
- Infrastructure Utilization: Maximizes the use of existing ATM infrastructure for additional services.

5. Accessibility:

- Wider Reach: ATMs are often more widely available than bank branches, especially in remote areas.
- User-Friendly Interface: Intuitive user interfaces make it easy for customers to complete transactions.

Disadvantages

1. Technical Issues:

- System Downtime: ATMs can be prone to technical issues and maintenance downtime, disrupting services.
- Network Dependency: Reliant on stable internet connections for OTP delivery and transaction processing.

2. Security Concerns:

-Hacking and Malware: ATMs can be targets for hacking, skimming, and malware attacks.

- Physical Security: ATMs are susceptible to physical attacks and vandalism.

3. User Limitations:

- Technological Barriers: Some users, especially elderly or less tech-savvy individuals, may find it difficult to use automated systems. - Mobile Number Requirement: OTP verification requires a registered mobile number, which may not be available to all users.

4. Initial Setup Costs:

- Implementation Costs: High initial costs for setting up the hardware, software, and security measures.
- Maintenance Costs: Ongoing maintenance and updates can be expensive.

5. Limited Support:

- No Human Interaction: Lack of immediate human assistance for troubleshooting or resolving complex issues.
- Language and Accessibility Issues: Automated systems may not cater to all languages and accessibility needs, potentially alienating some users.

Conclusion

The implementation of automated fee payment systems in ATMs, enhanced by OTP (One-Time Password) verification, marks a significant advancement in financial technology. These systems not only streamline the fee payment process but also significantly enhance security. By requiring a unique, time-sensitive OTP for each transaction, the risk of unauthorized access and fraud is greatly minimized, providing users with a higher level of confidence in the safety of their financial transactions.

The automated nature of these systems also leads to increased efficiency, reducing the need for manual intervention and decreasing transaction times. This is particularly beneficial in regions with limited banking infrastructure, where ATMs are primary access points for financial services. Despite some challenges, such as technical issues and the need for reliable network connectivity, the benefits of these systems outweigh the drawbacks.

Future developments, such as integrating biometric authentication and leveraging blockchain technology, hold the potential to further enhance the security and efficiency of ATM transactions. Overall, automated fee payment systems with OTP verification represent a crucial step forward in modernizing financial services, offering a secure, efficient, and user-friendly solution for fee payments.

References

1. Dahlberg, T., Guo, J., & Ondrus, J. (2015). A critical review of mobile payment research. Electronic Commerce Research and Applications, 14(5), 265-284.

2. DeYoung, R., Lang, W. W., & Nolle, D. L. (2007). How the Internet affects output and performance at community banks. Journal of Banking & Finance, 31(4), 1033-1060.

3. Dunphy, P., & Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. IEEE Security & Privacy, 16(4), 20-29.

4. Gates, B. (2006). Security in ATM networks. Security and Privacy in the Age of Ubiquitous Computing, 19(1), 8-14.

5. Howcroft, B., Hamilton, R., & Hewer, P. (2002). Consumer attitude and the usage and adoption of home-based banking in the United Kingdom. International Journal of Bank Marketing, 20(3), 111-121.

6. Liu, S., & Silverman, M. (2001). A practical guide to biometric security technology. IT Professional, 3(1), 27-32.

7. Pashalidis, A., & Mitchell, C. J. (2003). Single sign-on using trusted devices. IEEE Transactions on Consumer Electronics, 49(4), 1058-1063.