Journal of Advances in Developmental Research (IJAIDR)
E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

Advance Secured Atm System with Two Layers Security Protection

M. Swetha Vani[1], C. Pallavi[2], G. Girija[3], H. Ravindra[4], IC Narasimha M.Tech. (Ph.D.)[5]

[1,2,3,4,5]Department of ECE, Tadipatri Engineering College, Tadipatri

Abstract:
Advanced Secured ATM System with Two Layers Security Protection is designed to improve the security and reliability of the safety of the traditional ATM transaction with the incorporation of the multi-level security authentication. Conventional ATM systems using the traditional card and PIN-based security measures are vulnerable to fraud, theft, and unauthorized access. In this context, the proposed system is designed to incorporate the two-layer security feature to overcome the drawbacks associated with the traditional security measures.In the proposed system, the first level of security is the incorporation of the traditional ATM card and PIN. As the next level, the system incorporates the two-layer security feature using the biometric security feature. In this context, the user is required to look into the camera to verify the identity. The system also uses secure data communication methods to ensure that user information is not exposed to various cyber attacks. Through the integration of conventional and innovative methods of authentication, the proposed system offers a higher level of security, thereby reducing cases of fraud, thereby building user confidence. The smart and reliable system can be implemented in real-life ATMs to enhance secure transactions.

KEYWORDS: ATM Security, Two-Layer Authentication, Biometric Authentication, Facial Recognition, PIN Verification, Secure Transactions, Fraud Prevention, Embedded Systems, Cybersecurity, Smart Banking

INTRODUCTION:

Automated Teller Machines (ATMs) have become an essential tool in modern banking, facilitating the convenient and efficient performance of financial transactions. Nevertheless, with the increasing usage of ATMs, security risks like card skimming, PIN theft, and unapproved access have significantly increased. The conventional security measures used in ATMs include card and PIN-based authentication, which can be subjected to a variety of cyber and physical attacks. This has created a pressing need to incorporate more robust security measures to ensure the security of user information and financial assets. Recent developments in technology have enabled the incorporation of Internet of Things, biometric authentication, and machine learning techniques to provide enhanced security to ATMs. Internet of Things-based systems allow real-time monitoring and communication, which can help in the early detection of any suspicious activities. Biometric authentication techniques like fingerprint and facial recognition can provide enhanced security to ATMs, as these techniques verify the identity of the users based on unique physiological characteristics. This can greatly reduce the risks of fraud, as it is extremely

difficult to steal or duplicate biometric information. Furthermore, modern technology has also incorporated intelligent models and tracking systems into ATM systems in order to enhance safety and efficiency in these systems. The implementation of GPS technology in tracking various activities related to ATMs, such as cash transport, has also strengthened the safety system in ATMs. These modern technologies clearly indicate the growing trend towards smart and secure banking systems. However, currently, various ATMs face various challenges related to implementation costs, system complexity, and lack of real-time adaptability in these systems. Therefore, there is a need to develop a secure, efficient, and cost-effective ATM system that can integrate various security features into a single system. The proposed advanced ATM system with two-layered security protection can efficiently address these challenges by incorporating traditional and biometric authentication systems in ATMs in order to enhance security, reduce fraud cases, and increase users' trust in banking systems.

Various biometric-based authentication techniques, such as fingerprint-based and face recognition-based systems, have been found to be highly reliable in terms of user authentication. Unlike other techniques, biometric-based systems are based on unique physical properties of a person, which cannot be easily replicated, hence minimizing the possibilities of unauthorized access. Face recognition-based systems are found to provide a convenient and touch-free authentication method, which makes them highly suitable for modern ATMs.Pattern recognition-based techniques have been found to be widely used in order to increase the accuracy of biometric-based systems. Apart from this, recent developments in machine learning-based techniques have helped in improving the reliability of ATM systems by predicting potential faults in the system, which otherwise would have resulted in abnormal behavior patterns.Despite these developments in improving the reliability of ATM systems, existing security solutions are found to face various issues, such as high implementation costs, system complexities, and inadaptability in real-time scenarios.

LITERATURE SURVEY:

[1] D. Thirumoorthy et al. proposed an IoT-based ATM safety system that enhances security through real-time monitoring and alert mechanisms. The system uses sensors and communication modules to detect unauthorized access and suspicious activities, enabling quick response and improved protection of ATM machines.[2] A. S et al. developed an IoT-based system for securing ATM machines against physical and cyber threats. Their approach includes continuous monitoring and alert generation when tampering or abnormal activities are detected, thereby increasing system reliability and safety.[3] D. Anveshini et al. presented a fingerprint authentication system based on pattern recognition techniques. This method improves user verification accuracy and provides a secure alternative to traditional PIN-based systems by using unique biometric features.[4] I. P. Nkrumah et al. introduced a machine learning-based predictive model to detect ATM system defects. The model helps in identifying faults in advance, reducing system downtime and improving overall performance and maintenance efficiency.[5] B. Gopinath et al. proposed a system integrating IoT and GPS technologies to enhance the security of ATM cash refilling vans. The system provides real-time location tracking and monitoring, ensuring safe transportation and reducing the risk of theft. [6] F. G. Praticò et al. discussed the use of self-powered sensors for road pavements. Their work focuses on integrating energy harvesting technologies into pavements to power sensors without external energy sources, enabling continuous monitoring of road conditions and improving infrastructure sustainability.[7] T. Lin et al. presented the modeling and field testing of an electromagnetic energy harvester for rail tracks with anchorless mounting. Their study demonstrated efficient energy generation

from rail vibrations, making it suitable for powering monitoring systems in railway applications.[8] M. Balato et al. proposed a Maximum Power Point Tracking (MPPT) technique for wireless sensor nodes powered by electromagnetic vibration harvesters. Their system ensures efficient energy utilization, especially in freight wagon applications where vibration energy is abundant.[9] H. Rashidzadeh et al. explored energy harvesting for IoT sensors using MEMS technology. Their research highlights the potential of micro-scale energy harvesting systems to power low-energy IoT devices, improving system autonomy and reducing dependence on batteries.[10] T. Lin et al. developed an efficient electromagnetic energy harvester specifically for railroad transportation systems. Their work emphasizes improved design and performance for capturing vibration energy in dynamic environments.[11] P. Venugopal et al. introduced the concept of self-healing highways integrated with wireless electric vehicle charging and sustainable energy harvesting technologies. Their study focuses on future smart infrastructure that combines energy generation, storage, and utilization for improved transportation systems.

METHODS

1. Requirement Analysis

First, the security problems in existing ATM systems are studied. The need for two-layer security is identified to prevent fraud and unauthorized access.

2. System Design

The complete ATM system structure is designed, including user, ATM machine, server, and security modules.

3. User Registration

User details such as card number, mobile number, and biometric/OTP information are stored securely in the database.

4. First Layer Authentication

The user inserts the ATM card and enters the PIN. The system verifies these details with the bank server.

5. Second Layer Authentication

After PIN verification, a second security check is performed using OTP sent to the registered mobile number or biometric verification.

6. Transaction Processing

Only after successful verification of both security layers, the user is allowed to perform transactions like cash withdrawal or balance inquiry.

7. Security Monitoring

The system continuously monitors activities. Any wrong attempts or suspicious actions are detected and alerts are generated.

8. Testing and Implementation...

Finally, the system is tested for accuracy and security, and then implemented for real-time ATM usage.

PROPOSED SYSTEM –

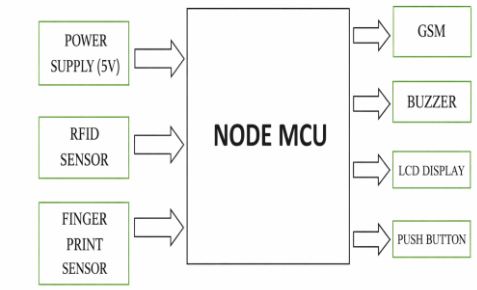
The Dual Secure ATM The proposed system, Dual Secure ATM, introduces an advanced two-layer security mechanism to ensure safe and reliable ATM transactions. The system integrates both biometric verification (such as fingerprint or facial recognition) and PIN authentication to provide double-layer protection against unauthorized access .In the first layer, the user must enter a valid ATM card number

and PIN. Once verified, the second layer of authentication uses biometric data to confirm the user's identity. Only when both layers are successfully verified, the user is granted access to banking services. This dual authentication process greatly reduces the chances of ATM fraud, card theft, and unauthorized transactions. The system ensures enhanced security, user convenience, and trust in digital banking operations. The Biometric Verification Module acts as the second layer of security. In this stage, the user's fingerprint or facial data is captured and compared with the biometric details stored in the database. Only if the biometric data matches successfully will the user be allowed to access the ATM services. This two-step verification ensures that even if someone obtains the user's card and PIN, they cannot perform transactions without the correct biometric identity.

ADVANTAGES

- Enhanced security
- User identity confirmation
- Fraud prevention
- Real-time alerts

System Architecture



SOFTWARE AND HARDWARE REQUIREMENTS –
HARDWARE REQUIREMENTS

1. Nodemcu
2. Fingerprint sensor
3. LCD display
4. Buzzer
5. Relay
6. Power supply
7. GSM module
8. RF ID sensor

SOFTWARE REQURIMENTS

1. Arduino IDE

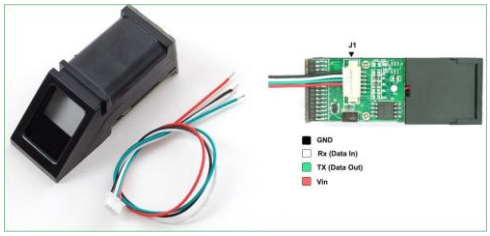
2. Database

NODEMCU

NodeMCU is a low-cost development kit for IoT devices based on the ESP8266 Wi-Fi module. The device is connected to the internet via wireless connectivity. The device can be easily programmed using the Arduino IDE. The device also supports different input and output interfaces for connection purposes. Due to its small size and high efficiency, NodeMCU is used for smart and automation devices.

FINGERPRINT SENSOR

A biometric reader that identifies users based on unique finger ridge patterns. Most hobbyist modules (like the AS608) use optical scanning and store up to 127 unique templates.



LCD DISPLAY

A Real Time screen (common sizes include 16x2) that shows real-time information such as "Access Denied" or system time. It often uses an I2C module to reduce the number of wires needed for connection.

BUZZER

An audio output device that produces a beep or alarm tone. Active buzzers are popular because they only require a simple 5V signal to sound, whereas passive buzzers require a more frequency than Active .

RELAY

An electromagnetic switch that allows a low-power circuit (like a 5V Arduino) to control high-power devices, such as a 220V light bulb or a 12V solenoid door lock.

POWER SUPPLY

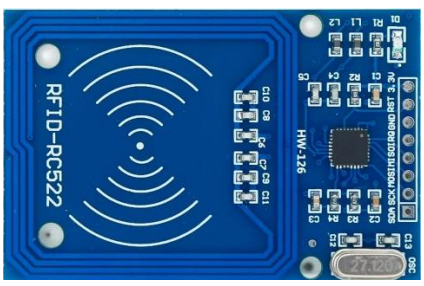
The energy source for the entire circuit. While a microcontroller may run on 5V, like GSM modules may require a stable 5V 2A or higher supply to handle current up and downs.

GSM MODULE

A cellular communicator that uses a SIM card to send SMS alerts or make calls to your phone during security events.

RFID SENSOR

A reader that detects ID cards or tags through radio frequency. Users can simply tap a card near the sensor to unlock a door or log attendance.



SOFTWARE REQUIREMENTS

Arduino IDE: The primary software tool for programming the NodeMCU is the Arduino Integrated Development Environment (IDE) for this project. The Arduino IDE is a simple and user-friendly tool for writing and editing code for the microcontroller. The primary advantage of using the Arduino IDE is that it supports C/C++ based programming and provides a wide array of built-in functions and libraries. This makes it very simple and efficient for programming the microcontroller and interfacing it with different components such as sensors, displays, and communication modules. In this project, the Arduino IDE is used for developing and implementing the code for controlling the RFID sensor, fingerprint sensor, GSM module, and LCD display. The IDE also supports real-time debugging and serial monitoring of the code and is very helpful for testing and troubleshooting the project. The IDE also supports the use of external libraries for different modules, which helps in enhancing the functionality of the project. The open-source nature of the IDE and its cross-platform compatibility make it a very reliable tool for programming microcontrollers.

RESULT:

The Smart Attendance System with the help of RFID was successfully designed and implemented. The RFID reader was able to detect the unique ID on the cards placed in front of the reader. Once the verification is successful, the attendance is recorded along with the correct date and time with the help of the RTC module. The Arduino Uno processor was able to process the information effectively, displaying relevant information such as the user ID and attendance status on the LCD screen. The system was able to provide a quick response time with minimal errors compared to the traditional system. The system also provided the benefits of secure handling of information, ensuring that unauthorized entries were not made.Thus, the system was found to be cost-effective, easy to use, and efficient in terms of real-time monitoring. The results prove that the system can be effectively implemented with the help of the proposed system.

CONCLUSION

The Smart Attendance System using RFID technology has proven to be an efficient solution for automating attendance management. The use of RFID technology in combination with Arduino Uno, RTC module, and LCD display has ensured accurate attendance management with minimal human intervention. The system has been found to be efficient in eliminating errors, reducing paperwork, and improving the monitoring of attendance data. The Smart Attendance System has been found to be simple, cost-effective, and applicable in different fields. The Smart Attendance System has successfully shown the efficiency of embedded systems in improving security, accuracy, and efficiency in attendance management.

FUTURE SCOPE

The Smart Attendance System can be further enhanced by incorporating additional features such as biometric attendance for improving security. The system can also be integrated with cloud technology for improving accessibility. The Smart Attendance System can also be enhanced by incorporating features such as the use of mobile applications for improving efficiency. The Smart Attendance System can also be enhanced by incorporating features such as the use of GPS technology for improving efficiency. The Smart Attendance System can also be enhanced by incorporating features such as the use of artificial intelligence for improving efficiency.

Reference

1. M. Gholikhani, H. Roshani, S. Dessouky, and A. T. Papagiannakis, "A critical review of roadway energy harvesting technologies," Appl. Energy, vol. 261, pp. 1–17, 2020.
2. F. G. Praticò, F. G. Della Corte, and M. Merenda, "Self-powered sensors for road pavements," in Functional Pavement Design - Proceedings of the 4th Chinese-European Workshop on Functional Pavement Design, CEW 2016, 2016, pp. 1365–1374.
3. T. Lin, Y. Pan, S. Chen, and L. Zuo, "Modeling and field testing of an electromagnetic energy harvester for rail tracks with anchorless mounting," Appl. Energy, 2018.
4. M. Balato, L. Costanzo, and M. Vitelli, "MPPT in wireless sensor nodes supply systems based on electromagnetic vibration harvesters for freight wagons applications," IEEE Trans. Ind. Electron., 2017.
5. H. Rashidzadeh, P. S. Kasargod, T. M. Supon, R. Rashidzadeh, and M. Ahmadi, "Energy harvesting for IoT sensors utilizing MEMS technology," in Canadian Conference on Electrical and Computer Engineering, 2016.
6. T. Lin, J. J. Wang, and L. Zuo, "Efficient electromagnetic energy harvester for railroad transportation," Mechatronics, 2018.
7. P. Venugopal et al., "Roadway to self-healing highways with integrated wireless electric vehicle charging and sustainable energy harvesting technologies," Appl. Energy, vol. 212, pp. 1226–1239, 2018.
8. M. Merenda, F. G. Praticò, R. Fedele, R. Carotenuto, and F. G. D. Corte, "A real-time decision platform for the management of structures and infrastructures," Electronics (Switzerland), vol. 8, no. 10. 2019.
9. M. Merenda, D. Iero, R. Carotenuto, and F. G. D. Corte, "Simple and low-cost photovoltaic module emulator," Electron., vol. 8, no. 12, pp. 1–15, 2019.
10. R. Fedele, F. G. Praticò, R. Carotenuto, and F. G. D. Corte, "Structural health monitoring of pavement assets through acoustic signature," in Bearing Capacity of Roads, Railways and Airfields - Proceedings of the 10th International Conference on the Bearing Capacity of Roads, Railways and Airfields, BCRRA 2017, 2017, pp. 869–875.
11. R. Fedele, F. G. Praticò, R. Carotenuto, and F. G. Della Corte, "Energy savings in transportation: Setting up an innovative SHM method," Math. Model. Eng. Probl., vol. 5, no. 4, pp. 323–330, 2018.