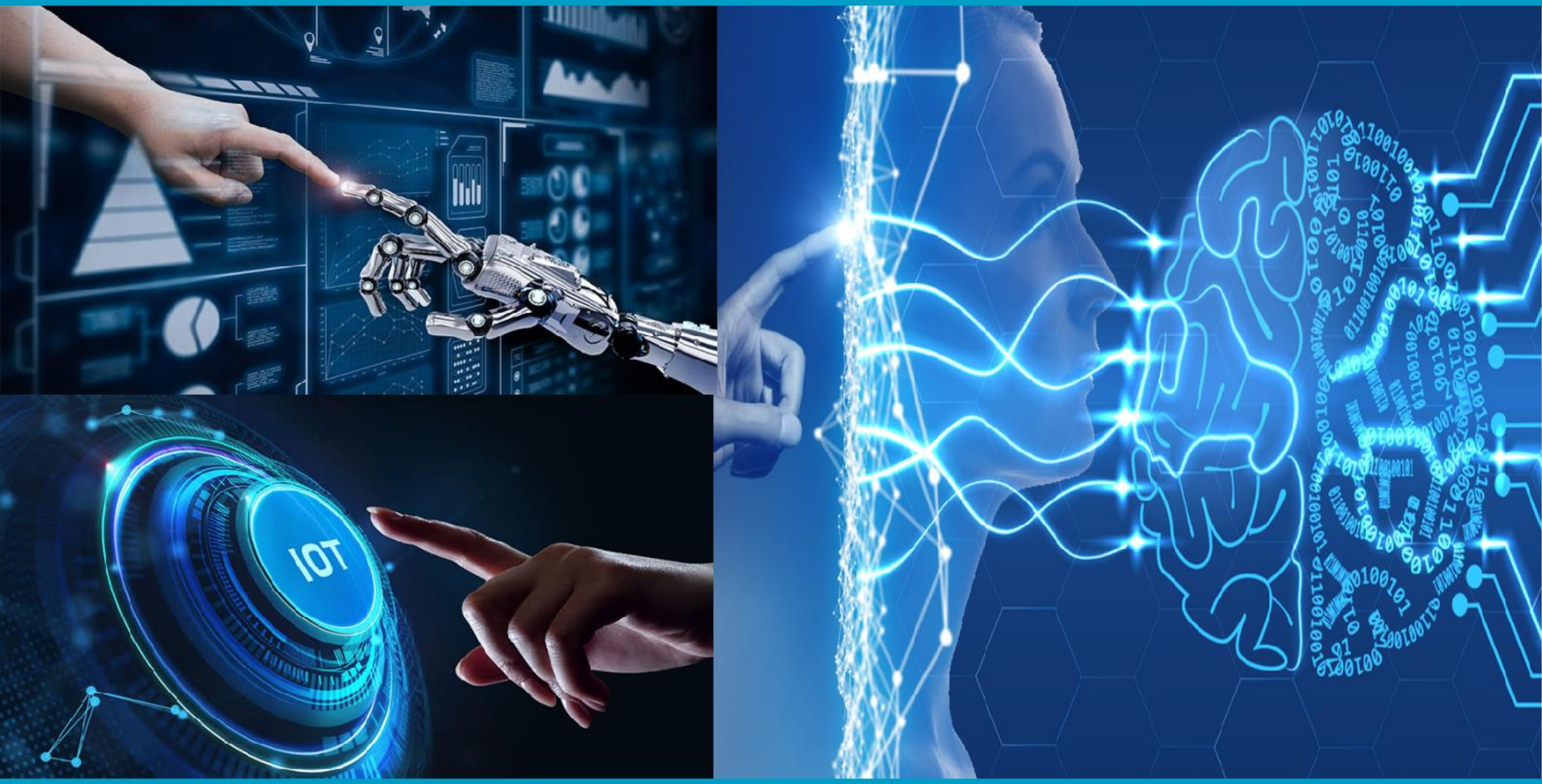
IJMRSETM

e-ISSN: 2395 - 7639



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 10, Issue 5, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.580

SMART ATM SECURITY SYSTEM

[1]Prof.Ganapathi Avabrath, [2]Arshiya U , [3]Ismat Tasleema, [4]Mufeeda Mashrufa, [5]Thasreefa

[1], Associate Professor, Dept. of Information Science and Engineering, Yenepoya Institute of Technology, Moodbidri, India.

[2,3,4,5,] Students, Dept. of Information Science and Engineering, Yenepoya Institute of Technology, Moodbidri, India

ABSTRACT: In most ATMs, cash can be withdrawn by unauthorized users merely by knowing their PIN number. We employed RF readers for authentication so that we could conduct secure transactions with the account holders' consent, and we have a database that comprises the RF identification of specific individuals with their picture. When one presents the RF tag to the RF reader, the camera is activated, captures the cardholder's image, and begins to check the database to see if the ID and their face match or not. If the account holder tries to use their ATM, the system recognizes that face and compares it to its database, sends OTP and allows consumers to take money from an ATM immediately. As someone tries to use your ATM, the system sends them an image with an OTP if their face cannot be matched with the original card account holder. Others can only use the ATM to withdraw cash after entering the OTP system.

KEYWORDS: ATM, Card Verification, Face Recognition, OTP Sending, OTP Verification.

I. INTRODUCTION

The Internet of Things is a rapidly growing and well-known phenomenon in today's technological world. IOT projects have been implemented in both the public and private sectors of our society. Automated teller machines (ATMs) are well-known machines that people commonly use to conduct banking operations or personal and business financial transactions. No one is able to withdraw money from an account without the account holder's knowledge while employing RF components and the SMTP protocol. The system only permits the usage of that specific ATM card when the OTP has been entered into the system with the account holder's knowledge. A significant portion of our population has access to ATM machines and debit cards that accept debit and credit cards.

Additionally, crime and unauthorized use of the cards started to pose a severe threat to both the population and the financial industry. Since the other user of the card is not authorized to use it, this project focuses on how to block an ATM. Face detection is done using a face Haar cascade, face recognition is done using a user at an ATM, and an OTP is sent to the authorized user so that they can enter it in order to withdraw cash from the machine. If the OTP that the user installed at the ATM is inaccurate, a notification message is instantly issued to the authorized user. The Arduino UNO is a popular component of the Face discovery Haar camera used for precise user images to A smart ATM security system using IoT and cloud Capture faces in this IoT project. RFID is utilized as an ATM card. Python-written code that sends the user an alert message and OTP via normal email.

II. LITERATURE SURVEY

[1] Biometric Based Smart ATM Using RFID:

Biometric Based Smart ATM Using RFID is a modern technology that combines biometric authentication and RFID technology to enhance the security of Automated Teller Machines (ATMs). This technology uses a combination of fingerprints and RFID cards to identify ATM users and provide them with secure access to their accounts. The biometric authentication system involves the use of fingerprint sensors to scan and verify the user’s fingerprints before granting access to their banking information. The RFID technology allows the user to wave or tap their RFID- enabled card close to the ATM's reader, which then identifies the user and authorizes the transaction. The advantages of this technology include enhanced security, increased convenience, and faster processing times. It eliminates the need for physical cards and passwords, reducing the risk of card skimming, identity theft, and other fraudulent activities.

[2] Enhanced Security Feature of ATM's Through Facial Recognition

The major objective of this article is to improve the user experience by combining the facial recognition feature with the already used conventional technique. In this system, Face-id is used as a key in the current approach. The fact that each person's face ID is unique and that only them can use it confers certain benefits. The machine learning and image processing algorithms (Eigenface algorithm) are employed to implement the face-id scan. The user's face is compared to a face in the database using the Eigenface technique in this case. The face recognizer, which is incorporated into OpenCV, is trained using machine learning. Compared to the eigenface Algorithm, the Adaboost face recognition algorithm has a success rate of 80%. This system's primary drawback is that the cameras must undergo routine maintenance. With this system, twins can be an exception. Photos can occasionally be used to get around security. Future applications for this technique include the employment of robust, high-quality cameras. Twins and photo bypassing are conditions that can be treated with 3-d cameras.

[3] Enhanced Security Mechanism for Atm Machines:

The primary idea behind the technology is that after an ATM card is inserted and authenticated, an image of the cardholder is taken with the use of the ATM's webcam and compared to the actual images that have already been kept in the database. If the captured image matches the recorded photos, proving he is the authorized user, he moves on to the next step where he may enter the password to complete the transaction. When the saved image and the image that was captured don't match, it shows that the user isn't authorized and restricts his access. The system might also inform the card's genuine owner of the misuse. Account holders must adjust their faces to the system in order for it to save and use their faces in the future. Once the individual's photograph connected with the card is obtained from the database, more processing can be done on the suggested system itself without affecting a server's actual capability. The disadvantage of the suggested approach is that when we grow those networks, the cost of the neural networks may be considerable. This can be prevented by offering If the cost is reduced and face recognition may be employed as an additional feature, further biometric characteristics or security layer approaches may be applied. As a result, we draw the conclusion that this project's execution will make it simple for people to use ATMs, rely on their security, and steer clear of fraudulent transactions.

[4] ATM Security System Using Arduino:

The fundamental tenet of the system is that the user must first enter their ATM card into the reader. Here, an RFID TAG has been utilized as an example. When using an ATM, each user is required to put their RFID TAG into the RFID. A distinguishing finger impression scanner will then be used to ask the user to look at the distinctive mark. Next, it will be looked at how the RFID and the distinguishing mark work together. In the unlikely event that both products are compatible, the client may carry out the exchange. After that, the consumer will be asked to enter the amount. The amount to be accomplished at that time must then be provided by the customer. The parity sum will be displayed on the LCD show screen when the total has been decreased from the put away sum. If the RFID and the distinguishing mark are incompatible (OTP), the consumer will be prompted to enter the one-time secret word. At that time, the record holder's registered mobile number, email, or SMS (Short Message Service) will all receive the OTP. Then, the record holder must send this OTP to the following client. The customer must then enter the OTP. When the entered information has been verified, the customer will be asked to enter the amount to be performed. The sum will be deducted from the reserve money and then the balance after exchange will be entered on the LCD panel. This framework is focused on verified verification by means of using special finger impression sensors in order to increase ATM security. The suggested framework provides excellent performance while keeping a safe distance from illegal exchanges. In terms of security- related issues, it is incredibly strong.

III. PROPOSED SYSTEM

In the suggested system, we have developed a new type of ATM that may be operated using an ATM card. ATMs can be operated via our mobile devices and the Internet of Things with the help of this technology. We can also stop illegal individuals from using our property without our knowledge. Using pictures Recognition and the original image are compared to our server's database. The user's account information, their photo, and other related information about the image can be collected on the server. The ATM's camera will record the user's image and utilize Open CV to compare it to the user's image stored on the server. The user must recognize the third party as a known individual in order to start the session. In this case, the display gives the user or third user as options. If the individual who came to withdraw money is a user, he or she can click on the user option and input the withdrawal PIN immediately. The person's image is taken using a webcam if they are a third party, and then it is compared to the database in the account user's account. The photograph is then mailed to the account holder along with a note. When the user confirms that the sender is someone he knows, a window where he can input his PIN number and withdraw the money opens.

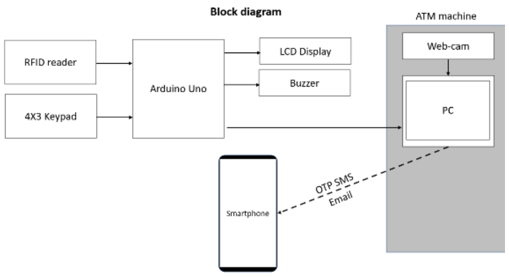


Fig: Block diagram of proposed system

IV. CONCLUSION

In conclusion, a smart ATM security system that utilizes facial recognition, OTP (One-Time Password), and RFID (Radio Frequency Identification) reader technology can provide a robust and multi-layered approach to securing ATM transactions. The combination of these three technologies can enhance the security of ATM transactions by verifying the user's identity, generating unique OTPs, and enabling contactless authentication through RFID cards or devices. Facial recognition technology adds a strong layer of security by verifying the user's identity based on their unique facial features in real-time. This makes it difficult for impostors to gain unauthorized access to ATM services using stolen cards or PINs. OTPs provide an additional layer of authentication by generating unique passwords for each transaction, which are sent to the user's registered mobile device, adding an extra factor of authentication. RFID technology enables contactless authentication through RFID cards or devices, reducing the risk of card skimming or cloning. The combination of these technologies can provide a multi-factor authentication system that significantly reduces the risk of unauthorized access and fraudulent activities at ATMs. In conclusion, a smart ATM security system that combines facial recognition, OTP, and RFID reader technology can provide a multi-layered and robust approach to securing ATM transactions, offering enhanced security and user convenience. Proper implementation, testing, and ongoing monitoring of the system, along with compliance with relevant regulations, are crucial to ensuring its effectiveness in protecting ATM transactions and user information.

REFERENCES

1. Das, S. and Debbarma, J., 2011. Designing a biometric strategy (fingerprint) measure for enhancing atm security in indian e-banking system. International Journal o f Information and Communication Technology Research, 1(5)
2. Nelligani, B.M., Reddy, N.U. and Awasti, N., 2016, August. Smart ATM security system using FPR, GSM, GPS. In 2016 International Conference on Inventive Computation Technologies (ICICT) (Vol. 3, pp. 1-5). IEEE.
3. onyesolu. m. o and ezeani. i. m, “ATM security using fingerprint biometric identifier: an investigative study”, 2012 international journal of advanced computer science and applications.
4. renee jebaline. g, gomathi. s, “a novel method to enhance the security of ATM using biometrics”, 2015 international conference on circuit, power and computing technologies
5. J.J.Patoliya, M.M. Desai, "Face Detection based ATM Security System using Embedded Linux Platform ", 2nd International
6. Conference for Convergence in Technology (I2CT), 2017.
7. M.Karovaliyaa, S.Karediab, S.Ozac, Dr.D.R.Kalbande, "Enhanced security for ATM machine with OTP and Facial recognition features",International Conference on Advanced Computing Technologies and Applications (ICACTA), 2015.
8. Hota, Jyotiranjan. (2013). Growth of ATM Industry in India. CSI Communications. 36. 23-25.
9. The Times of India, “Atm Crimes”. Available: https://timesofindia.indiatimes.c/topic/AtmCrimes [Accessed: May 08,2020].

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

☎ +91 99405 72462 +91 63819 07438 ✉ ijmrsetm@gmail.com

www.ijmrsetm.com