JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Authentication of ATM PIN by Random Word Generator Using Design Think Frame Work

[1]Ravi Babu B, [2]Gowthami P, [3]Ajay Kumar A B, [4]Ajay C, [5]Joshi B, [6]Harish K
[1]Associate Professor, [2,3,4,5,&6]B.Tech. IV Year Students
[1]Department of Electronics and Communication Engineering,
[1]Siddharth Institute of Engineering & Technology, Puttur, Andhra Pradesh, India.

Abstract : The main aim of this system he proposed system presents a multi-layered security approach for access control. It initiates with RFID-based authentication, where the user's RFID card is scanned, prompting the system to generate a unique one-time password (OTP). This OTP is then dispatched to the user via GSM technology. Upon receipt of the OTP, the user must input it using a Bluetooth-enabled device, such as a smartphone or tablet. This additional verification layer guarantees that only authorized personnel can proceed further. If the entered OTP matches the one sent, the security door automatically unlocks, granting access. Conversely, an incorrect OTP entry triggers a buzzer alert, effectively thwarting any unauthorized entry attempts. This integrated system seamlessly combines RFID technology, GSM communication, Bluetooth verification, and a robust security door mechanism to establish a secure and user-friendly access control solution, offering enhanced security for various applications.

***IndexTerms* - Arduino, ATM, pin entry, Bluetooth.**

I. Introduction

This Money can be deposited and withdrawn from an ATM. A card is inserted into an ATM processor, which is an automatic teller machine that exchanges money for the card. ATMs come in two different varieties. To dump money by the user and receive a receipt based on the account is the first type. The second kind is more sophisticated; it allows for credit card payments, cash deposits, and account information retrieval. Several people utilize ATMs to deposit cash. In order to make it simple to remember, an ATM machine that is close to the user's location can be used to obtain cash if that is what they need. According to user needs, an ATM machine has two inputs and four outputs. Each ATM card has a distinct number, known as a PIN number. Introducing a random word generator for ATM PINs strengthens security against various threats by creating complex, difficult-to-guess combinations, enhancing ATM transaction security. Memorizing a random word might be more intuitive and easier for users compared to remembering a sequence of numbers. This could potentially reduce instances of forgotten PINs and the need for users to write them down, which can be a security risk in itself. Introducing a random word generator for ATM PINs represents an innovative approach to addressing security concerns. It demonstrates a willingness to think outside the box and explore unconventional solutions to traditional problems.

II. Literature Review

- **Manikandan** This survey from 2018 explores IoT security, covering vulnerabilities, countermeasures, and future directions. Security vulnerabilities in IoT systems. Analyses common security vulnerabilities in IoT systems, including those relevant to ATMs, and proposes countermeasures.
- **J. Zhang** This 2019 study explores improving user authentication through random words and facial recognition. User experience and security trade-offs in traditional PIN-based authentication. Studying using random words and facial recognition for logging in, showing how it could be easier and safer than just using PINs.
- **S. Choi** Applying Design Thinking to Develop a User-Cantered ATM Interface (2020). Traditional ATM interfaces lack user-friendliness and accessibility. Using design thinking to craft an ATM interface that's user-centric and accessible, focusing on meeting user needs and preferences as a top priority.
- **M. Hassan** An Innovative Design of a Secure and User-Friendly ATM System (2019). Security and user experience limitations of existing ATM systems. Investigating RFID technology to make ATMs safer with an extra layer of security.
- **L. Wang** Research on the Application of RFID Technology in ATM Security (2017). Security vulnerabilities related to physical access to ATMs. Investigating RFID technology to make ATMs safer with an extra layer of security.
- **Sadeghi** Security and Privacy in Cyber-Physical Systems: Foundations, Challenges, and Future Directions (2015). Security and privacy challenges in cyber-physical systems, including ATMs. Addressing the distinct security and privacy challenges of cyber-physical systems such as ATMs, emphasizing the necessity for robust security solutions.
- **Smith, J** Enhancing ATM Security: A Random Word Generator Approach. Traditional ATM PINs vulnerabilities. Introducing a new way to log into ATMs with random words, making it easier and safer with thoughtful design.
- **David Williams** Usability Evaluation of Random Word Generated ATM PINs. Forgettable and easily guessable traditional ATM PINs. Assesses how well random word-generated PINs work in ATM systems by testing with users. Shows how this method balances security and usability.

- **Alshawi** Improving ATM Security using Two-Factor Authentication and Biometric Recognition (2018). Traditional PIN-based authentication poses security risks, while IoT-related privacy and trust issues are critical considerations for ATM security. Proposes a two-factor authentication system for ATMs utilizing biometric recognition alongside PINs for enhanced security.
- **T. Dimitrious** A Survey on Attacks Against ATMs (2016). Comprehensive overview of various attack vectors against ATMs. Explores various ATM attack methods like skimming, cash trapping, and malware injection, offering insights for enhancing security measures.
- **E. Bertino** Data Security and Privacy in Cloud Computing (2013). Security and privacy concerns in cloud-based systems. Discusses security and privacy challenges in cloud-based systems relevant to storing and managing ATM transaction data in the cloud.
- **M. Conti** Why Traditional PINs are No Longer Secure (2018). Vulnerability of PIN-based authentication to various attacks. Argues that traditional PINs are no longer sufficiently secure due to advances in technology and social engineering attacks, highlighting the need for alternative authentication methods.
- **D. Querzola** Applying Design Thinking Methodology to Improve ATM User Experience (2020). Lack of user-centered design in traditional ATM interfaces. Demonstrates the application of design thinking to improve the user experience of ATMs, focusing on usability and accessibility considerations.
- **N. Kumar** A Comprehensive Survey on Biometric Authentication Techniques (2020). Overview of various biometric authentication methods. Provides a comprehensive overview of different biometric authentication technologies like fingerprint, facial recognition, and iris recognition, which could be considered for ATMs.

III. EXISTING METHODOLOGY

Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as “the weakest link” in the authentication chain. Rather than arbitrary alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization. With web applications and …. mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users’ credentials. To overcome this problem, we proposed a novel authentication system.

IV. PREPARE YOUR PAPER BEFORE STYLING

The proposed system project incorporates a multi-step security process. It begins with an RFID-based authentication, where the user's RFID card is read, triggering the system to generate a one-time password (OTP). This OTP is then transmitted to the user via GSM (Global System for Mobile Communications). Upon receiving the OTP, the user is required to enter it through a Bluetooth-enabled device, such as a smartphone or tablet. This additional layer of verification ensures that only authorized individuals can proceed. If the entered OTP matches the one sent, the security door unlocks, allowing access. However, in cases of an incorrect OTP entry, a buzzer alert is activated, denying unauthorized entry attempts. This comprehensive system combines RFID technology, GSM communication, Bluetooth verification, and a security door mechanism to provide robust security measures while ensuring user convenience and access control. In Fig. 1 Circuit Diagram of the system is explained. This system helps to Under Stand the Working of inside the system.

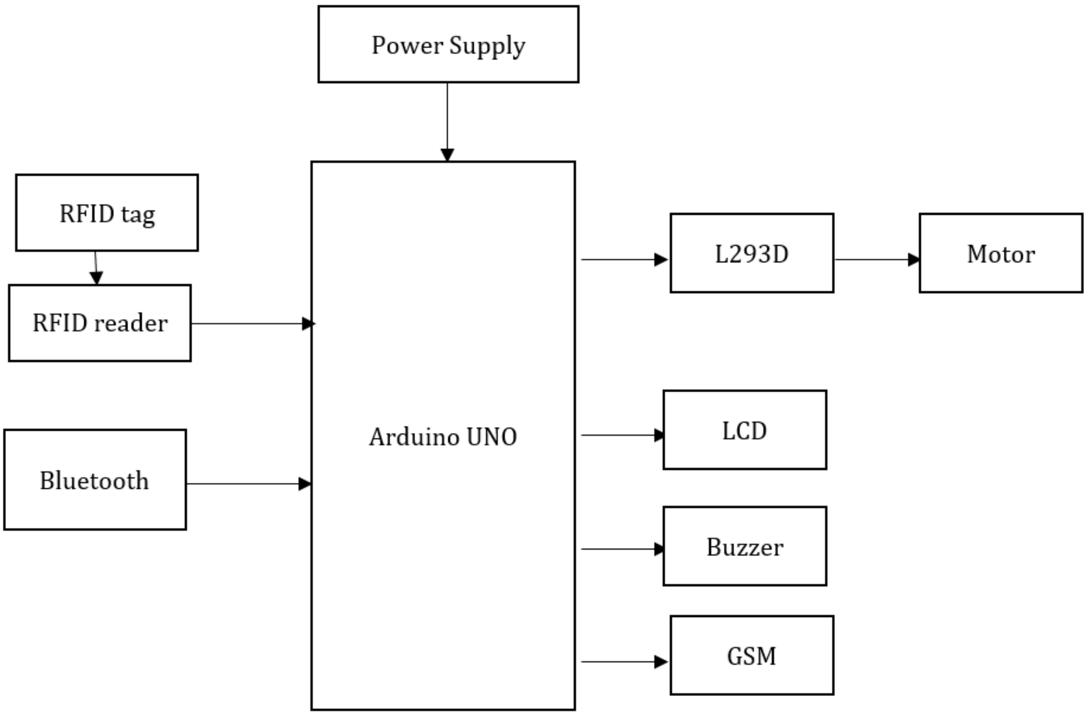


Fig. 1. Circuit Diagram

4.1 Hardware Setup

Arduino

The Arduino microcontroller is an easy to use yet powerful single board computer that has gained considerable traction in the hobby and professional market. The Arduino is open-source, which means hardware is reasonably priced and development software is free. This guide is for students in ME 2011, or students anywhere who are confronting the Arduino for the first time. For advanced Arduino users, prowl the web; there are lots of resources. The Arduino board is shown in figure 2.

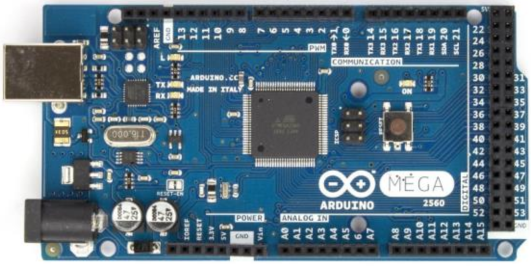


Fig. 2: Arduino Mega Board

LCD

Liquid Crystal Displays, shown in figure 3, commonly known as LCDs, are ubiquitous in modern electronics and play a pivotal role in displaying information in a wide range of devices, from digital watches to complex industrial machinery.

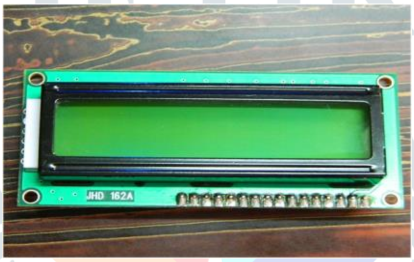


Fig. 3: LCD

RC522 RFID Module

The RC522 RFID module shown in figure 4 is a 13.56MHz RFID module that is based on the MFRC522 controller from NXP semiconductors. The module can support I2C, SPI and UART and normally is shipped with a RFID card and key fob. It is commonly used in attendance systems and other person/object identification applications.

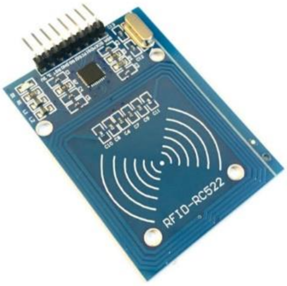


Fig. 4: RC522 RFID Module

RFID Tag

RFID has a place with the Automatic Identification and Data Capture (AIDC) innovation gathering. AIDC strategies consequently distinguish objects, gather information on them, and straightforwardly enter this information into PC frameworks with next to zero human mediation. To accomplish this, RFID techniques utilize radio waves.

Fig. 5: RFID Tags

HC-05 BLUETOOTH MODULE

HC-05 is a Bluetooth module which is designed for wireless communication. This module can be used in a master or slave configuration.

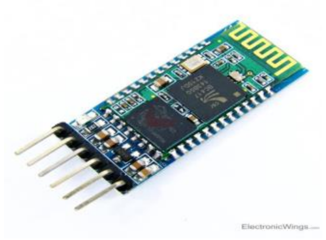


Fig. 6: HC-05 Bluetooth Module

DC-Motor

A direct current (DC) motor is a type of electric machine that converts electrical energy into mechanical energy. DC motors take electrical power through direct current, and convert this energy into mechanical rotation.

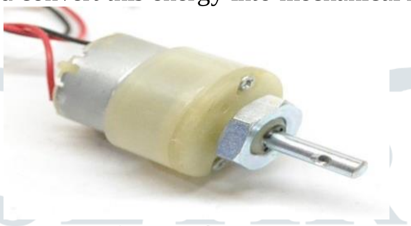


Fig. 7: DC-Motor

GSM

GSM is a mobile communication modem it stands for global system for mobile communication (GSM). The idea of GSM was developed at Bell Laboratories in 1970. It is widely used mobile communication system in the world. GSM is an open and digital cellular technology used for transmitting mobile voice and data services operates at the 850MHz, 900MHz, 1800MHz and 1900MHz frequency bands.

Fig. 8: GSM

BUZZER

A buzzer or beeper is an audio signaling device, which may be mechanical, electromechanical, or piezoelectric. Typical uses of buzzers and beepers include alarm devices, timers and confirmation of user input such as a mouse click or keystroke. Buzzer is an integrated structure of electronic transducers, DC power supply, widely used in computers, printers, copiers, alarms, electronic toys, automotive electronic equipment, telephones, timers and other electronic products for sound devices.

Fig. 9: Buzzer

RECTFIER

A rectifier is an electrical device that converts alternating current (AC), which periodically reverses direction, to direct current (DC), which flows in only one direction. The process is known as rectification, since it "straightens" the direction of current.

Fig. 10: Rectifier

IV. RESULTS AND DISCUSSION

Despite warnings, many consumers still select PINs and passwords that might be easily guessed, such as birthdays, phone numbers, and social security numbers. The demand for techniques to demonstrate that someone is actually who they say they are has increased as a result of recent instances of identity theft. Overall strong security can be developed by using the proposed method of random word generation. So, it helps us to overcome the main drawbacks of misusing highly authenticated security like fingerprints and to reduce the use of a skimmer. This way of a transaction is more secure as no one has an idea of what the concept is. It is highly confidential as they are using random words for the particular alphabet in all cases. This system helps in reducing ATM theft and all the random issues that we face during the process of money transactions. A well-designed and implemented random PIN generator using a random word can be a secure tool for generating unique and secure identification codes. However, it is important to be aware that no system is completely foolproof, and it is always a good idea to use additional security measures such as two factor authentication to protect sensitive information and resources. Overall strong security can be developed by using proposed method of rand word generation. so, it helps us to overcome the main drawbacks of misusing highly authenticated security of like fingerprint and to reduce the use of skimmer.

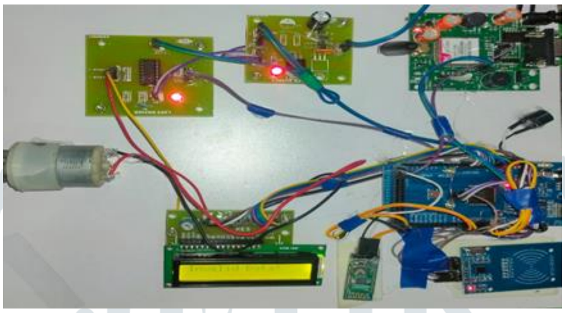
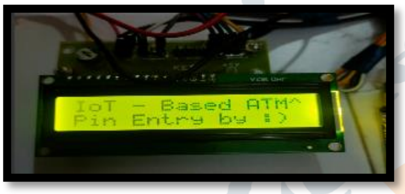
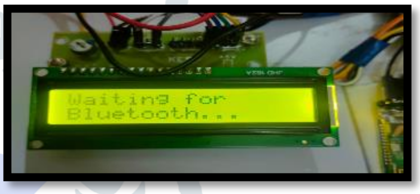


Fig. 11: ATM Setup



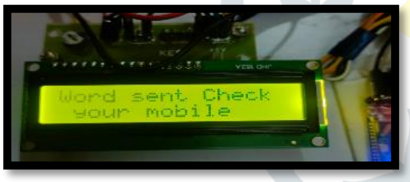
IoT - Based ATM^
Pin Entry by :)

Fig. 12: Interface



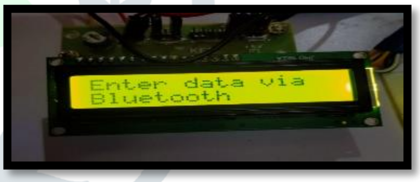
Waiting for
Bluetooth...

Fig. 13: Waiting for Bluetooth



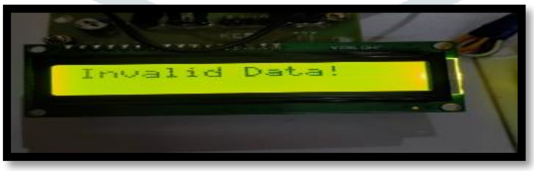
Word sent Check
your mobile

Fig. 14: Word sent message



Enter data via
Bluetooth

Fig. 15: Waiting message



Invalid Data!

Fig. 16: Invalid Message

V. CONCLUSION

The proposed method of random word generation stands as a promising approach to bolster overall security measures. By introducing dynamic and unpredictable elements in password creation, this method addresses key drawbacks associated with conventional security measures like fingerprint authentication. Unlike static biometric measures, random word generation provides an added layer of complexity, making it significantly harder for malicious actors to exploit or misuse highly authenticated security systems. Additionally, the adoption of this method plays a crucial role in minimizing the vulnerability of skimmer devices, which often target traditional authentication methods. The use of randomly generated words not only enhances the resilience of security systems but also reduces the risk of unauthorized access and potential data breaches. As a result, this innovative approach contributes to the development of a robust security framework, safeguarding sensitive information and thwarting malicious activities in a technologically evolving landscape.

REFERENCES

[1] Ms.Ojaswi K. Kasat, Dr.Umesh S. Bhadade, "Revolving Flywheel PIN Entry Method to Prevent Shoulder Surfing Attacks", 3rd International Conference for Convergence in Technology (I2CT), pp.1-5, Apr 06-08, 2018.

[2] S. Priyadharshini, Mrs. R. Kurinjimalar, "security enhancement in automated teller machine", International Conference on Intelligent Computing and Control(I2C2),2017.

[3] Apurva Taralekar, Gopal singh Chouhan, Rutuja Tangade, Nikhil kumar Shardoor, “One Touch Multi-banking Transaction ATM System using Biometric and GSM Authentication”, International Conference on Big Data, IoT and Data Science (BID) , Vishwakarma Institute of Technology, Pune, pp.61-68, Dec 20-22,2017.

[4] Jong-Hoon Kim, Gokarna Sharma, Irvin Steve Cardenas, Do Yeon Kim, Nagarajan Prabakar, S.S. Iyengar, “DynamicPIN: A Novel Approach towards Secure ATM Authentication”, International Conference on Computational Science and Computational Intelligence, pp. 69-73,2017.

[5] Taekyoung Kwon, Sarang Na, "Stegano PIN: Two-Faced Human Machine Interface for Practical Enforcement of PIN Entry Security", IEEE Transactions on Human-Machine Systems, vol. 46, pp. 314-317, September 2016.