A Project Report

On

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

Submitted in partial fulfillment for the award of the degree of

Bachelor of Technology

in

Electronics and Communication Engineering

by

P GOWTHAMI	20F61A0442
A B AJAY KUMAR	21F65A0401
C AJAY	20F61A0402
B JOSHI	21F65A0406
K HARISH	20F61A0450

Under the esteemed guidance of

B RAVI BABU M.Tech.

Associate professor, Department of ECE

Department of Electronics and Communication Engineering

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY

(AUTONOMOUS)

(Approved by AICTE & Affiliated to JNTUA, Ananthapuramu)

(Accredited by NBA for Civil, EEE, ECE, MECH and CSE, New Delhi)

(Accredited by NAAC with 'A+' Grade, an ISO 9001:2008 Certified Institution)

Siddharth Nagar, Narayanavanam road, Puttur-517583, A.P

2024

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY

(AUTONOMOUS)

(Approved by AICTE & Affiliated to JNTUA, Ananthapuramu)

(Accredited by NBA for Civil, EEE, ECE, MECH and CSE, New Delhi)

(Accredited by NAAC with 'A+' Grade, an ISO 9001:2008 Certified Institution)

Siddharth Nagar, Narayanavanam road, Puttur-517583, A.P

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

CERTIFICATE

This is to certify that the Project entitled "Authentication of ATM PIN by Random Word Generator Using Design Think Frame Work "that is being submitted by

P GOWTHAMI	**20F61A0442**
A B AJAY KUMAR	**21F65A0401**
C AJAY	**20F61A0402**
B JOSHI	**21F65A0406**
K HARISH	**20F61A0450**

is in partial fulfillment of the requirements for the award of BACHELOR OF TECHNOLOGY in ELECTRONICS AND COMMUNICATION ENGINEERING *to* JNTUA , ANANTHAPURAMU. *The results embodied in this Project report have not been submitted to any other University or Institute for the award of any degree.*

Internal Guide

B RAVI BABU, M.Tech

Associate professor,

Department Of ECE,

SIETK.

Head of the Department

Dr.P.RATNA KAMALA,M.Tech.,Ph.D.

Head Of the Department,

Department Of ECE,

SIETK.

Submitted for the project viva-voce examination held on _____

Internal Examiner **External Examiner**

Acknowledgement

*We wish to express our profound and sincere gratitude to Mr.**B Ravi Babu** ,Associate Professor of Electronics and Communication Engineering, **Siddharth Institute of Engineering & Technology, Puttur**, who guided us into the intricacies of this project with utmost clarity.*

*We would also like to extend our gratitude to **Dr. P Ratna Kamala**, Head of the Department of Electronics and Communication Engineering for her encouragement and for providing the facilities to carry out the work in a successful manner.*

*We are thankful to **Dr. K. Chandrasekhar Reddy**, Principal for his encouragement and support.*

*We wish to express our sincere thanks to **Dr. K. Indiraveni, Vice-Chairman,** and **Dr. K. Ashok Raju, Chairman** of Siddharth Group of Institutions, Puttur, for providing ample facilities to complete the project work.*

We would also like to thank all the faculty and staff of the Electronics and Communication Engineering Department, for helping us to complete the project work.

Very importantly, we would like to place on record our profound indebtedness to our parents and families for their substantial moral support and encouragement given throughout our studies.

TABLE OF CONTENTS

ABSTRACT

The main aim of this system he proposed system present 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.

Keywords: Arduino, ATM, pin entry, Bluetooth, GSM, RFID.

LIST OF FIGURES

LIST OF TABLES

SYMBOLS & ABBREVIATIONS

Acronym	Abbreviation
LCD	Liquid crystal display
GSM	Global System for Mobile Communications
RFID	Radiofrequency identification
ARDUINO IDE	Integrated development environment
CPU	Central processing unit
SIM	Subscriber identity module
IMEI	International mobile equipment identity
USB	universal serial bus
SPI	Serial peripheral interface
ATM	Automated teller machine

CHAPTER 1

INTRODUCTION

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.

Banks, we fabricate secure ATM violations avoidance system for quick and simple user-friendly money transactions between banks and human being with safety and security.

Embedded system implementation

Embedded systems are specialized computing systems designed to perform dedicated functions or tasks within a larger system. These systems are ubiquitous in modern technology and can be found in a wide range of applications, from consumer electronics to industrial machinery and automotive systems. Embedded systems are characterized by their integration of hardware and software components tailored to meet specific requirements, making them efficient and reliable for their intended purpose Embedded systems typically consist of a microcontroller or microprocessor at their core, which acts as the brain of the system. This microcontroller is responsible for executing instructions and controlling the various hardware peripherals connected to it, such as sensors, actuators, and communication modules. The software running on the microcontroller, often referred to as firmware, is customized to perform the precise tasks the embedded system was designed for.

One of the key features of embedded systems is their real-time operation. Many embedded systems must respond to external stimuli or events in a timely and deterministic manner. For example, in automotive applications, embedded systems control functions like engine management, braking, and airbag deployment, where rapid and accurate responses are critical for safety. Embedded systems can vary in complexity, from simple

microcontroller-based designs with minimal resources to more powerful embedded systems featuring multicore processors, advanced graphical interfaces, and connectivity options like Wi-Fi or Bluetooth. The choice of components and architecture depends on the specific requirements of the application.

In conclusion, embedded systems play a pivotal role in modern technology, enabling the automation and control of a wide array of devices and systems. Their unique combination of hardware and software customization allows them to excel in performing dedicated tasks efficiently and reliably, making them an integral part of our daily lives.

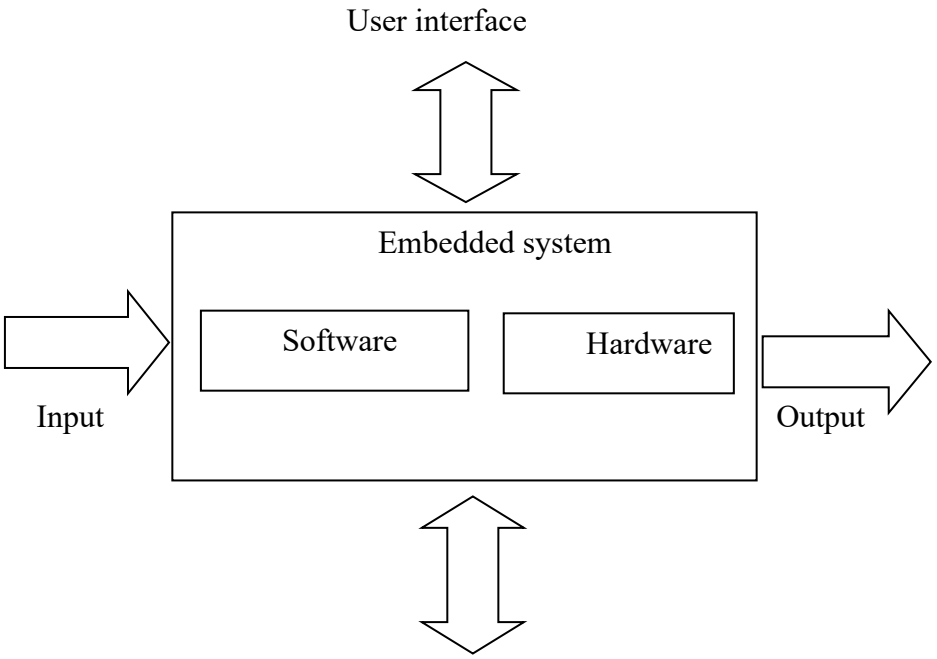

Fig 1.1 Outline of embedded systems.

Embedded system:

The embedded system includes mainly two sections, they are

1. Hardware
2. Software

Hardware is any element of a computer that's physical. This includes things like monitors, keyboards, and also the insides of devices, like microchips and hard drives. Software is anything that tells hardware what to do and how to do it, including computer programs and apps on your phone.

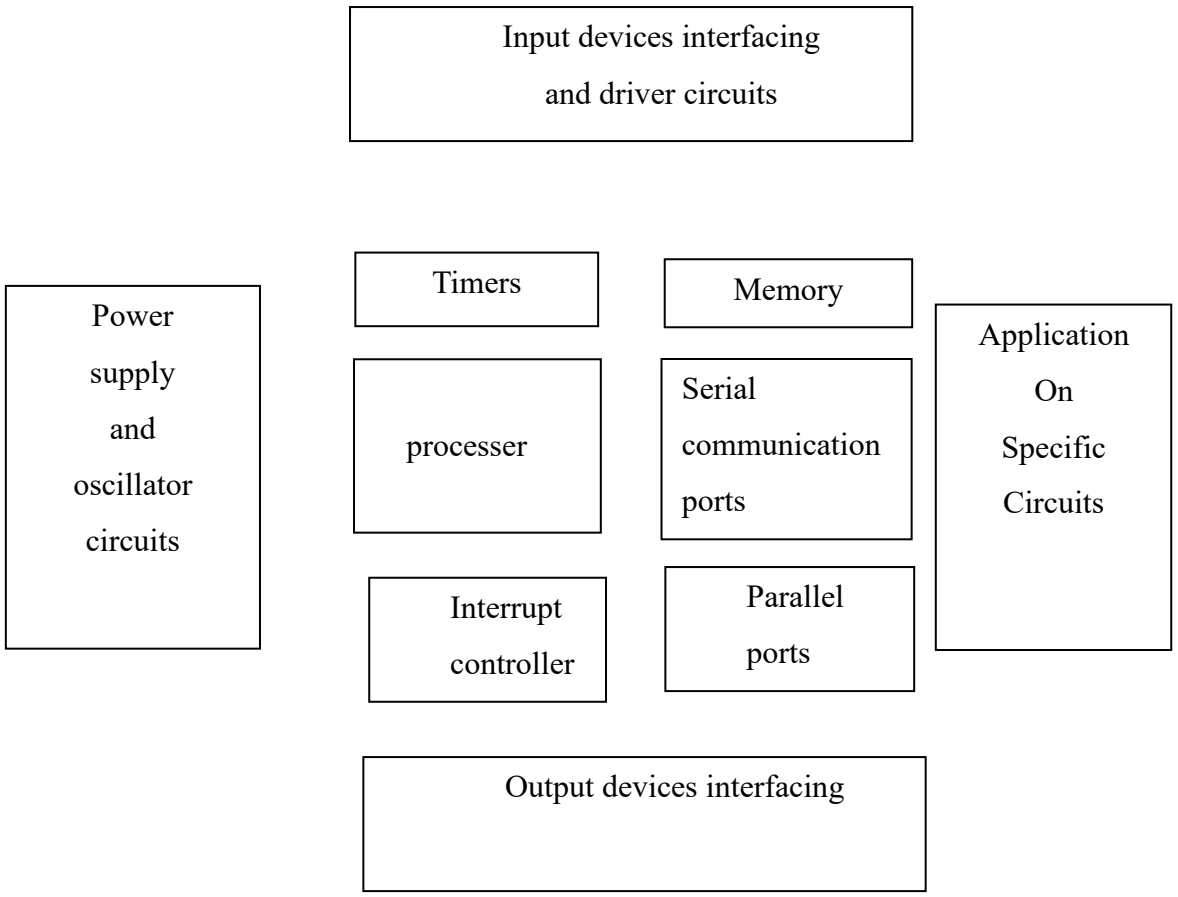

Fig 1.2 Architecture of embedded system

1.1 Motivation of The Project

- **Security**

  Introducing a random word generator for ATM PINs strengthens security against various threats by creating complex, difficult-to-guess combinations, enhancing ATM transaction security.

- **User experience**

  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.

CHAPTER 2

LITERATURE SURVEY

2.1 Observation made from paper 1

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.

2.2 Observation made from paper 2

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.

2.3 Observation made from paper 3

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.

2.4 Observation made from paper 4

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.

2.5 Observation made from paper 5

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.

2.6 Observation made from paper 6

A. 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.

2.7 Observation made from paper 7

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.

2.8 Observation made from paper 8

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.

2.9 Observation made from paper 9

A. 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.

2.10 Observation made from paper 10

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.

2.11 Observation made from paper 11

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.

2.12 Observation made from paper 12

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.

2.13 Observation made from paper 13

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.

2.14 Observation made from paper 14

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.

2.15 Observation made from paper 15

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.

CHAPTER 3

EXISTING METHOD

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

PROPOSED SYSTEM

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.

BLOCK DIAGRAM

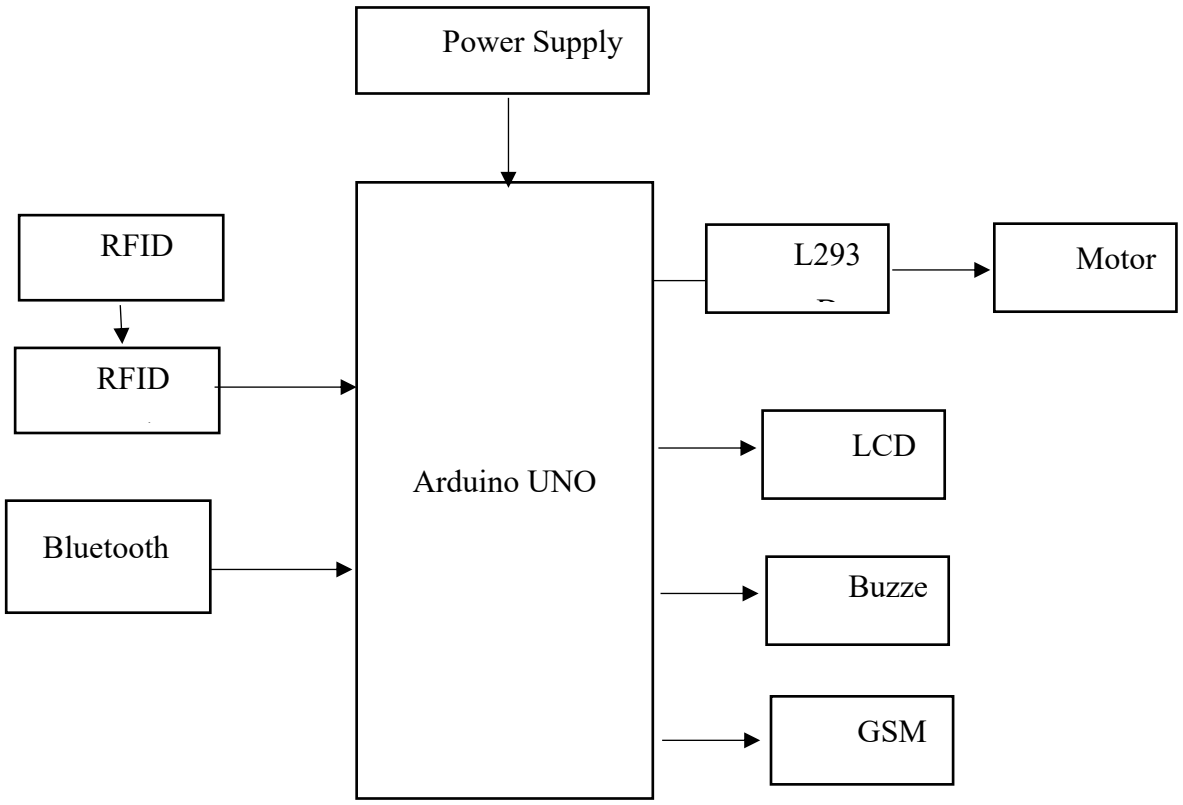

Fig 3.1 Block Diagram of Facial Expression Recognition

The framework for authenticating ATM PINs via a random word generator consists of interconnected modules. Users interact through the interface, entering their PIN and a randomly generated word. PIN verification checks the entered PIN against stored data. A unique word generated adds an additional layer of security. Comparison ensures the accuracy of the entered word. Security measures encrypt sensitive data during transmission. The database securely stores and retrieves encrypted PINs. Logging records authentication attempts for auditing purposes. Output promptly informs users of authentication success or failure. An admin interface allows for system management and error handling ensures seamless operation.

Additionally, the system includes robust error handling mechanisms to manage incorrect inputs and system failures effectively. Encryption techniques are employed to safeguard sensitive data throughout the authentication process. An administrative interface enables authorized personnel to manage system settings and access logs. The framework prioritizes user-friendliness while ensuring stringent security measures. Overall, it aims to create a reliable and efficient authentication system for ATM transactions.

CHAPTER 4

HARDWARE DESCRIPTION

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.

This is what the Arduino board looks like.

Fig 4.1 Arduino Board

The Arduino programming language is a simplified version of C/C++. If you know C, programming the Arduino will be familiar. If you do not know C, no need to worry as only a few commands are needed to perform useful functions.

PIN CONFIGURATIONS

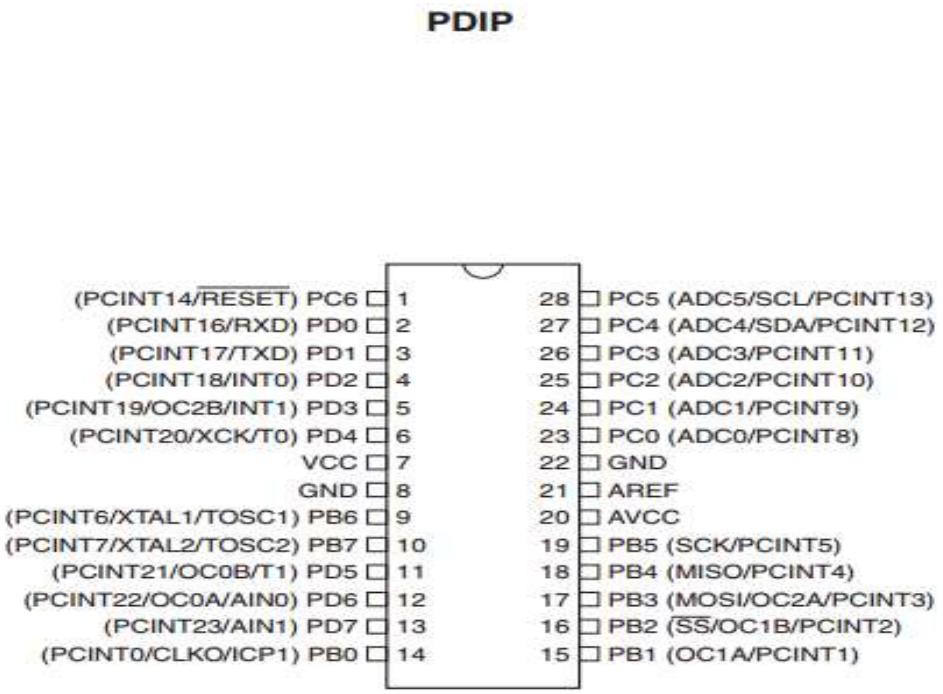

Fig 4.2 pin diagram

Pin Descriptions:

VCC: Digital supply voltage.

GND: Ground.

Port B (PB7:0) XTAL1/XTAL2/TOSC1/TOSC2: Port B is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port B output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port B pins that are externally pulled low will source current if the pull-up resistors are activated. The Port B pins are tri-stated when a reset condition becomes active, even if the clock is not running. Depending on the clock selection fuse settings, PB6 can be used as input to the inverting Oscillator amplifier and input to the internal clock operating circuit. Depending on the clock selection fuse settings, PB7 can be used as output from the inverting Oscillator amplifier. If the Internal Calibrated RC Oscillator is used as chip clock source, PB7.6 is used as TOSC2.1 input for the Asynchronous Timer/Counter2 if the AS2 bit in ASSR is set. The various special features of Port B are elaborated in" Alternate Functions of Port B" on page 76 and" System Clock and Clock Options" on page 26.

Port C (PC5:0): Port C is a 7-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The PC5.0 output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port C pins that are externally pulled low will source current if the pull-up resistors are activated. The Port C pins are tri-stated when a reset condition becomes active, even if the clock is not running.

PC6/RESET: If the RSTDISBL Fuse is programmed, PC6 is used as an I/O pin. Note that the electrical characteristics of PC6 differ from those of the other pins of Port C. If the RSTDISBL Fuse is unprogrammed, PC6 is used as a Reset input. A low level on this pin for longer than the minimum pulse length will generate a Reset, even if the clock is not running. The minimum pulse length is given in Table 28-3 on page 308. Shorter pulses are not guaranteed to generate a Reset. The various special features of Port C are elaborated in" Alternate Functions of Port C" on page 79.

Port D (PD7:0): Port D is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port D output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port D pins that are externally pulled low will source current if the pppppiuytw0[\pull-up resistors are activated. The Port D pins are tri-stated when a reset condition becomes active, even if the clock is not running. The various special features of Port D are elaborated in "Alternate Functions of Port D" on page 82.

AVCC: AVCC is the supply voltage pin for the A/D Converter, PC3:0, and ADC7:6. It should be externally connected to VCC, even if the ADC is not used. If the ADC is used, it should be connected to VCC through a low-pass filter. Note that PC6.4 use digital supply voltage, VCC.

AREF: AREF is the Analog reference pin for the A/D Converter

ADC7:6 (TQFP and QFN/MLF Package Only): In the TQFP and QFN/MLF package, ADC7:6 serve as Analog inputs to the A/D converter. These pins are powered from the Analog supply and serve as 10-bit ADC channels.

OVERVIEW

The ATmega48PA/88PA/168PA/328P is a low-power CMOS 8-bit microcontroller based on the AVR enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the ATmega48PA/88PA/168PA/328P achieves throughputs approaching 1 MIPS per MHz allowing the system designed to optimize power consumption versus processing speed.

The AVR core combines a rich instruction set with 32 general purpose working registers. All the 32 registers are directly connected to the Arithmetic Logic Unit (ALU), allowing two independent registers to be accessed in one single instruction executed in one clock cycle. The resulting architecture is more code efficient while achieving throughputs up to ten times faster than conventional CISC microcontrollers.

BLOCK DIAGRAM

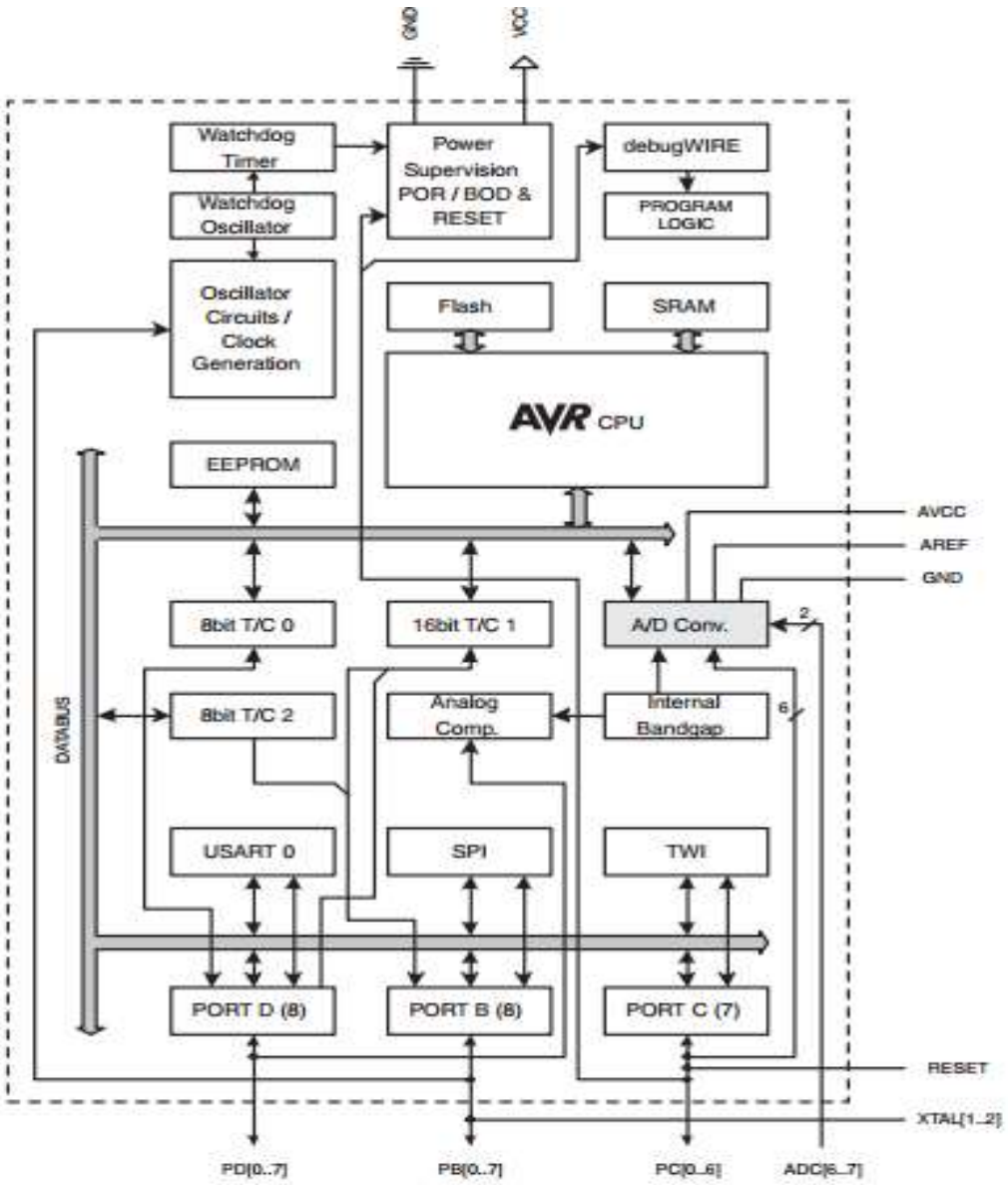

Fig 4.3 Block Diagram

The ATmega48PA/88PA/168PA/328P provides the following features: 4/8/16/32K bytes of In System Programmable Flash with Read-While-Write capabilities, 256/512/512/1K bytes EEPROM, 512/1K/1K/2K bytes SRAM, 23 general purpose I/O

lines, 32 general purpose working registers, three flexible Timer/Counters with compare modes, internal and external interrupts, a serial programmable USART, a byte-oriented 2-wire Serial Interface, an SPI serial port, a 6-channel 10-bit ADC (8 channels in TQFP and QFN/MLF packages), a programmable Watchdog Timer with internal Oscillator, and five software selectable power saving modes. The Idle mode stops the CPU while allowing the SRAM, Timer/Counters, USART, 2-wire Serial Interface, SPI port, and interrupt system to continue functioning. The Power-down mode saves the register contents but freezes the Oscillator, disabling all other chip functions until the next interrupt or hardware reset. In Power-save mode, the asynchronous timer continues to run, allowing the user to maintain a timer base while the rest of the device is sleeping. The ADC Noise Reduction mode stops the CPU and all I/O modules except asynchronous timer and ADC, to minimize switching noise during ADC conversions. In Standby mode, the crystal/resonator Oscillator is running while the rest of the device is sleeping. This allows very fast start-up combined with low power consumption.

The device is manufactured using Atmel's high density non-volatile memory technology. The On-chip ISP Flash allows the program memory to be reprogrammed In-System through an SPI serial interface, by a conventional non-volatile memory programmer, or by an On-chip Boot program running on the AVR core. The Boot program can use any interface to download the application program in the Application Flash memory. Software in the Boot Flash section will continue to run while the Application Flash section is updated, providing true Read-While-Write operation. By combining an 8-bit RISC CPU with In-System Self-Programmable Flash on a monolithic chip, the Atmel ATmega48PA/88PA/168PA/328P is a powerful microcontroller that provides a highly flexible and cost-effective solution to many embedded control applications. The ATmega48PA/88PA/168PA/328P AVR is supported with a full suite of program and system development tools including: C Compilers, Macro Assemblers, Program Debugger/Simulators, In-Circuit Emulators, and Evaluation kits.

Comparison Between ATmega48PA, ATmega88PA, ATmega168PA and ATmega328P

The ATmega48PA, ATmega88PA, ATmega168PA and ATmega328P differ only in memory sizes, boot loader support, and interrupt vector sizes. Table 2-1 summarizes the different memory and interrupt vector sizes for the three devices.

Table 2-1. Memory Size Summary

Device	Flash	EEPROM	RAM	Interrupt Vector Size
ATmega48PA	4K Bytes	256 Bytes	512 Bytes	1 instruction word/vector
ATmega88PA	8K Bytes	512 Bytes	1K Bytes	1 instruction word/vector
ATmega168PA	16K Bytes	512 Bytes	1K Bytes	2 instruction words/vector
ATmega328P	32K Bytes	1K Bytes	2K Bytes	2 instruction words/vector

Table 1.1 Memory Size Summary

ATmega88PA, ATmega168PA and ATmega328P support a real Read-While-Write Self-Programming mechanism. There is a separate Boot Loader Section, and the SPM instruction can only execute from there. In ATmega48PA, there is no Read-While-Write support and no separate Boot Loader Section. The SPM instruction can execute from the entire Flash.

POWER

The Arduino Uno can be powered via the USB connection or with an external power supply. The power source is selected automatically. External (non-USB) power can come either from an AC-to-DC adapter (wall-wart) or battery. The adapter can be connected by plugging a 2.1mm centre-positive plug into the board's power jack. Leads from a battery can be inserted in the Gnd and Vin pin headers of the POWER connector. The board can operate on an external supply of 6 to 20 volts. If supplied with less than 7V, however, the 5V pin may supply less than five volts and the board may be unstable. If using more than 12V, the voltage regulator may overheat and damage the board. The recommended range is 7 to 12 volts. The power pins are as follows:

- **VIN**. The input voltage to the Arduino board when it's using an external power source (as opposed to 5 volts from the USB connection or other regulated power source). You can supply voltage through this pin, or, if supplying voltage via the power jack, access it through this pin.
- **5V.** This pin outputs a regulated 5V from the regulator on the board. The board can be supplied with power either from the DC power jack (7 - 12V), the USB connector (5V), or the VIN pin of the board (7-12V). Supplying voltage via the 5V or 3.3V pins bypasses the regulator, and can damage your board. We don't advise it.
- **3V3**. A 3.3-volt supply generated by the on-board regulator. Maximum current draw is 50 mA.
- **GND.** Ground pins.

Memory

The ATmega328 has 32 KB (with 0.5 KB used for the bootloader). It also has 2 KB of SRAM and 1 KB of EEPROM (which can be read and written with the EEPROM library).

I/O Ports

- 3 8-bit Ports(B, C,D)
- Each port controlled by 3 8-bit registers
- DDRx direction register
- PINx pin input value

LCD

Liquid Crystal Displays, 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. These displays are characterized by their energy-efficient operation, slim form factor, and the ability to present alphanumeric characters, numbers, symbols, and even graphics with high clarity and contrast.

LCD technology relies on the unique properties of liquid crystals, which are organic compounds that can manipulate the passage of light when exposed to an electric field. LCDs consist of multiple layers, including two polarizing layers and a layer of liquid crystals sandwiched in between. The liquid crystal layer's optical properties can be controlled by applying voltage to specific pixels, causing them to either allow light to pass through or block it, thus creating the displayed image.

One of the most prominent advantages of LCDs is their energy efficiency. Unlike older display technologies such as cathode-ray tubes (CRTs), which require a continuous electron beam to generate images, LCDs only consume power when the pixels need to change their state. This property makes LCDs ideal for battery-powered devices like smartphones and laptops, where energy conservation is essential.

Furthermore, LCDs offer exceptional clarity and visibility under various lighting conditions. They are designed to emit very little heat and provide excellent contrast ratios, ensuring that text and images remain legible even in bright sunlight or low-light environments. This characteristic makes them suitable for applications ranging from digital signage and consumer electronics to medical devices and automotive dashboards.

In addition to their primary use as display screens, LCDs are versatile and have found applications beyond traditional visual interfaces. They are often integrated into touchscreen panels, enabling users to interact directly with devices through touch gestures. This feature has revolutionized the way we interact with smartphones, tablets, and even home appliances, enhancing user experience and functionality.

In conclusion, Liquid Crystal Displays have become an integral part of modern life, driving the visual interface in an array of electronic devices. Their energy efficiency, clarity, and adaptability have made them a preferred choice for manufacturers across industries, continuously expanding their applications and capabilities in an ever-evolving technological landscape.

Images of LCD Display

Fig 4.4 Front View

Fig 4.5 Back View

Pin Diagram

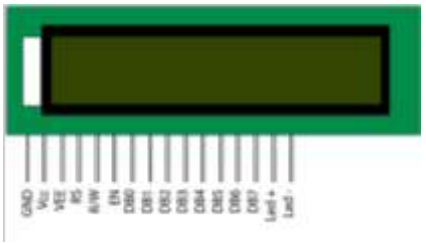

Fig 4.6 Pin Diagram

Pin Description

Pin No	Function	Name
1	Ground (0V)	Ground
2	Supply voltage; 5V (4.7V – 5.3V)	Vcc
3	Contrast adjustment; through a variable resistor	V_{EE}
4	Selects command register when low; and data register when high	Register Select
5	Low to write to the register; High to read from the register	Read/write
6	Sends data to data pins when a high to low pulse is given	Enable
7	8-bit data pins	DB0
8		DB1
9		DB2
10		DB3
11		DB4
12		DB5
13		DB6
14		DB7
15	Backlight V_{CC} (5V)	Led+
16	Backlight Ground (0V)	Led-

Table 1.2 Pin Description

RS (Register select)

It has generally two register pins

- Command Register and
- Data Register

Command Register

The LCD's instructions are stored within the command register. An instruction serves as a directive given to the LCD to carry out a specific task, such as initializing the LCD, clearing

its screen, positioning the cursor, controlling the display, and more. The processing of these instructions takes place within the command register.

Data Register

The information register serves as the repository for the data intended to be displayed on the LCD screen. This data typically consists of ASCII-encoded characters that are destined for presentation on the LCD. When transmitting data to the LCD, it gets processed and readied within the information register. Notably, by setting RS=1, we designate the information register for data processing.

Mode of LCD

As mentioned, the LCD screen includes an interface integrated circuit (IC) that can be accessed for reading or writing by the microcontroller (MCU). In most cases, the standard practice involves writing to the IC, as reading from it can introduce complexity and is rarely required. However, it is possible to retrieve information such as cursor position, status, or interrupt notifications from the IC when the need arises.

Block Diagram of LCD Display

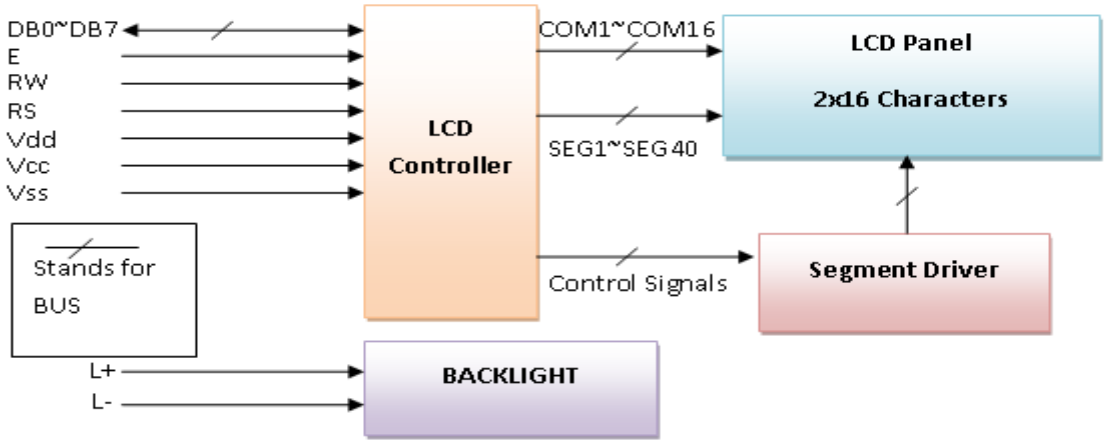

Fig 4.7 Block Diagram of LCD Display

RC522 RFID Module

The RC522 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 4.8 RC522 RFID Module

RC522 Pin Configuration

Pin Number	Pin Name	Description
1	Vcc	Used to Power the module, typically 3.3V is used
2	RST	Reset pin – used to reset or power down the module
3	Ground	Connected to Ground of system
4	IRQ	Interrupt pin – used to wake up the module when a device comes into range
5	MISO/SCL/Tx	MISO pin when used for SPI communication, acts as SCL for I2c and Tx for UART.
6	MOSI	Master out slave in pin for SPI communication
7	SCK	Serial Clock pin – used to provide clock source
8	SS/SDA/Rx	Acts as Serial input (SS) for SPI communication, SDA for IIC and Rx during UART

Table 1.4 RC522 Pin Configuration

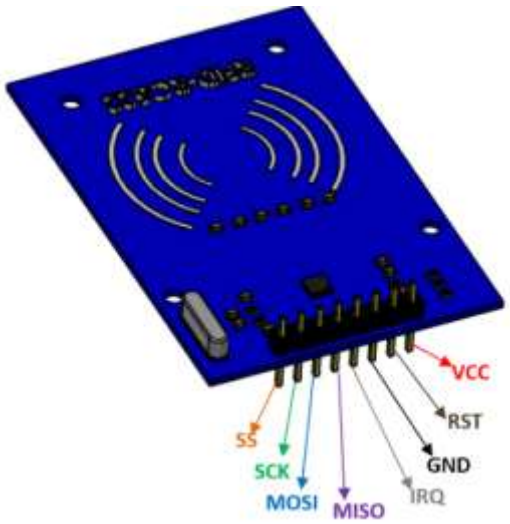

Fig 4.9 RFID Reader

RFID or **Radio Frequency Identification** system consists of two main components, a transponder/tag attached to an object to be identified, and a Transceiver also known as interrogator/Reader.

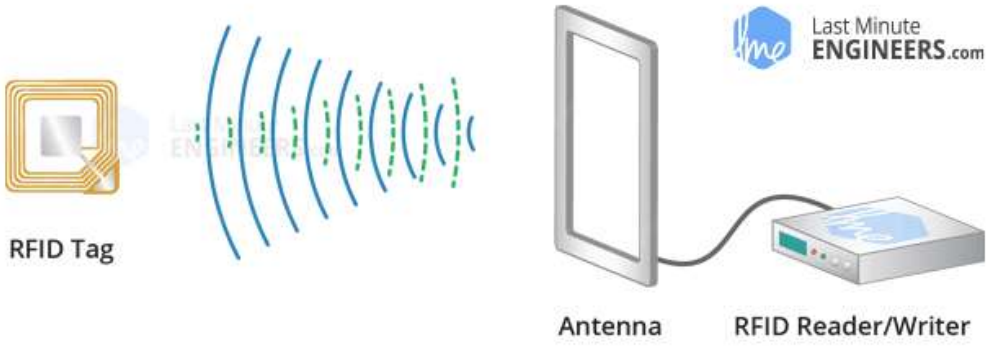

Fig 4.10 RFID Working

A Reader consists of a Radio Frequency module and an antenna which generates high frequency electromagnetic field. On the other hand, the tag is usually a passive device, meaning it doesn't contain a battery. Instead, it contains a microchip that stores and processes information, and an antenna to receive and transmit a signal.

The powered chip inside the tag then responds by sending its stored information back to the reader in the form of another radio signal. This is called backscatter. The backscatter, or change in the electromagnetic/RF wave, is detected and interpreted by the reader which then sends the data out to a computer or microcontroller

What is an RFID Tag

The picture given is that of a RFID tag (brilliant card molded tag). RFID labels are accessible in various sorts of size and shapes. The Tag contains an IC for putting away the information, a reception apparatus for transmitting and accepting, and a modulator. Tags are very small in size and they can hold only few bits of data.

Fig 4.11 RFID Tags

Bluetooth Module

Introduction

- It is used for many applications like wireless headset, game controllers, wireless mouse, wireless keyboard and many more consumer applications.
- It has range up to <100m which depends upon transmitter and receiver, atmosphere, geographic & urban conditions.
- It is IEEE 802.15.1 standardized protocol, through which one can build wireless Personal Area Network (PAN). It uses frequency-hopping spread spectrum (FHSS) radio technology to send data over air.
- It uses serial communication to communicate with devices. It communicates with microcontroller using serial port (USART).

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.

Fig4.12 HC-05 Bluetooth Module

Pin Description

Fig4.13 Pin Description

Bluetooth serial modules allow all serial enabled devices to communicate with each other using Bluetooth.

It has 6 pins,

1. **Key/EN:** It is used to bring Bluetooth module in AT commands mode. If Key/EN pin is set to high, then this module will work in command mode. Otherwise by default it is in data mode. The default baud rate of HC-05 in command mode is 38400bps and 9600 in data mode.

HC-05 module has two modes,

2. **VCC:** Connect 5 V or 3.3 V.

3. **TXD:** Transmit Serial data (wirelessly received data by Bluetooth module transmitted out serially on TXD pin)

4. **RXD:** Receive data serially (received data will be transmitted wirelessly by Bluetooth module).

5. **State:** It tells whether module is connected or not.

Command Mode

- When we want to change settings of HC-05 Bluetooth module like change password for connection, baud rate, Bluetooth device's name etc.
- To do this, HC-05 has AT commands.
- To use HC-05 Bluetooth module in AT command mode, connect "Key" pin to High (VCC).
- Default Baud rate of HC-05 in command mode is 38400bps.
- Following are some AT command generally used to change setting of Bluetooth module.
- To send these commands, we have to connect HC-05 Bluetooth module to the PC via serial to USB converter and transmit this command through serial terminal of PC.

Command	Description	Response
AT	Checking communication	OK
AT+PSWD=XXXX	Set Password e.g. AT+PSWD=4567	OK
AT+NAME=XXXX	Set Bluetooth Device Name e.g. AT+NAME=MyHC-05	OK
AT+UART=Baud rate, stop bit, parity bit	Change Baud rate e.g. AT+UART=9600,1,0	OK
AT+VERSION?	Respond version no. of Bluetooth module	+Version: XX OK

		e.g. +Version: 2.0 20130107 OK
AT+ORGL	Send detail of setting done by manufacturer	Parameters: device type, module mode, serial parameter, passkey,etc.

Table 1.5. Command Mode

Motor Driver

A motor driver is an integrated circuit chip which is usually used to control motors in autonomous robots. Motor driver act as an interface between Arduino and the motors. The most commonly used motor driver IC's are from the L293 series such as L293D, L293NE, etc. These ICs are designed to control 2 DC motors simultaneously. L293D consist of two H-bridge. A DC motor, or direct current motor, converts electrical energy into mechanical energy. It operates based on the principle of Lorentz force, where a current-carrying conductor in a magnetic field experiences a force. In a DC motor, this conductor is usually a coil of wire called the armature. The magnetic field is generated by permanent magnets or electromagnets.When a current flows through the armature, it interacts with the magnetic field, causing the armature to rotate. This rotation is facilitated by a commutator, which reverses the direction of current flow in the armature coils as it rotates, ensuring continuous motion in the same direction.DC motors come in various types, including brushed and brushless

Fig 4.14 DC Motor

The first practical DC motor was invented some years later in 1886 by Frank Julian Sprague, whose invention lead to the first motor powered trolley system in 1887, and the first

GSM

GSM is a mobile communication modem; it is 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.

GSM system was developed as a digital system using time division multiple access (TDMA) technique for communication purpose. A GSM digitizes and reduces the data, then sends it down through a channel with two different streams of client data, each in its own particular time slot. The digital system has an ability to carry 64 kbps to 120 Mbps of data rates.

There are various cell sizes in a GSM system such as macro, micro, pico and umbrella cells. Each cell varies as per the implementation domain. There are five different cell sizes in a GSM network macro, micro, pico and umbrella cells. The coverage area of each cell varies according to the implementation environment.

GSM Architecture

A GSM network consists of the following components:

- **A Mobile Station:** It is the mobile phone which consists of the transceiver, the display and the processor and is controlled by a SIM card operating over the network.
- **Base Station Subsystem:** It acts as an interface between the mobile station and the network subsystem. It consists of the Base Transceiver Station which contains the radio transceivers and handles the protocols for communication with mobiles. It also consists of the Base Station Controller which controls the Base Transceiver station and acts as a interface between the mobile station and mobile switching centre.
- **Network Subsystem:** It provides the basic network connection to the mobile stations. The basic part of the Network Subsystem is the Mobile Service Switching Centre which provides access to different networks like ISDN, PSTN etc. It also consists of the Home Location Register and the Visitor Location Register which provides the call routing and roaming capabilities of GSM. It also contains the Equipment Identity Register which

maintains an account of all the mobile equipments wherein each mobile is identified by its own IMEI number. IMEI stands for International Mobile Equipment Identity.

Features of GSM Module:

- Improved spectrum efficiency
- International roaming
- Compatibility with integrated services digital network (ISDN)
- Support for new services.
- SIM phonebook management
- Fixed dialing number (FDN)
- Real time clock with alarm management
- High-quality speech
- Uses encryption to make phone calls more secure
- Short message service (SMS)

The security strategies standardized for the GSM system make it the most secure telecommunications standard currently accessible. Although the confidentiality of a call and secrecy of the GSM subscriber is just ensured on the radio channel, this is a major step in achieving end-to- end security.

GSM Modem

A GSM modem is a device which can be either a mobile phone or a modem device which can be used to make a computer or any other processor communicate over a network. A GSM modem requires a SIM card to be operated and operates over a network range subscribed by the network operator. It can be connected to a computer through serial, USB or Bluetooth connection.

A GSM modem can also be a standard GSM mobile phone with the appropriate cable and software driver to connect to a serial port or USB port on your computer. GSM modem is usually preferable to a GSM mobile phone. The GSM modem has wide range of applications in transaction terminals, supply chain management, security applications, weather stations and GPRS mode remote data logging.

Fig 4.15 GSM

It requires a **SIM (Subscriber Identity Module)** card just like mobile phones to activate communication with the network. Also they have **IMEI** (International Mobile Equipment Identity) number similar to mobile phones for their identification. A GSM/GPRS MODEM can perform the following operations:

1. Receive, send or delete SMS messages in a SIM.
2. Read, add, search phonebook entries of the SIM.
3. Make, Receive, or reject a voice call.

The MODEM needs **AT commands**, for interacting with processor or controller, which are communicated through serial communication. These commands are sent by the controller/processor. The MODEM sends back a result after it receives a command. Different AT commands supported by the MODEM can be sent by the processor/controller/computer to interact with the **GSM and GPRS cellular network**.

GSM Architecture

The GSM architecture is divided into Radio Subsystem, Network and Switching Subsystem and the Operation Subsystem. The radio sub system consists of the Mobile Station and Base Station Subsystem.

The mobile station is generally the mobile phone which consists of a transceiver, display and a processor. Each handheld or portable mobile station consists of a unique identity

stored in a module known as SIM (Subscriber Identity Chip). It is a small microchip which is inserted in the mobile phone and contains the database regarding the mobile station.

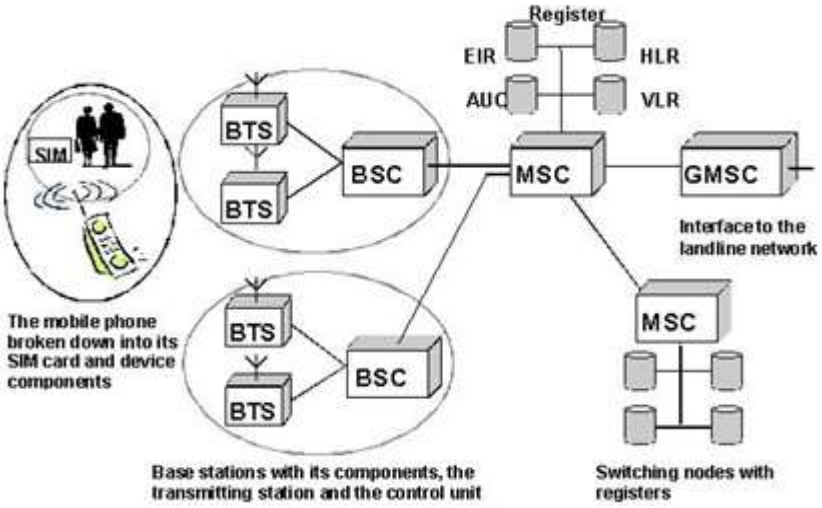

Fig 4.16 GSM Architecture

Buzzer

A buzzer or beeper is an audio signalling 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. Active buzzer 5V Rated power can be directly connected to a continuous sound, this section dedicated sensor expansion module and the board in combination, can complete a simple circuit design, to "plug and play.

Fig4.17 Buzzer

Buzzer Pin Configuration

Pin Number	Pin Name	Description
1	Positive	Identified by (+) symbol or longer terminal lead. Can be powered by 5V DC
2	Negative	Identified by short terminal lead. Typically connected to the ground of the circuit

Table 1.5. Buzzer Pin Configuration

Buzzer Features and Specifications

- Rated Voltage: 6V DC
- Operating Voltage: 4-8V DC
- Rated current: <30mA
- Sound Type: Continuous Beep
- Resonant Frequency: ~2300 Hz
- Small and neat sealed package
- Breadboard and Perf board friendly.

Rectifier

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 4.18 Rectifier

CHAPTER 5

SOFTWARE DESCRIPTION

Arduino IDE

The Arduino IDE software is a open source software, where we can have the example codes for the beginners. In the Present world there are lot of versions in the Arduino IDE in which present usage is Version1.0.5. It is very easy to connect the PC with Arduino Board.

First, we have to install the Arduino IDE software according to the below instructions:

Insert the CD-ROM or PENDRIVE which Contains the software and then Copy the Setup File to your desired location.

After Copying, now click on the setup you will see an window shown below Click On NO, not this time. Then after NEXT

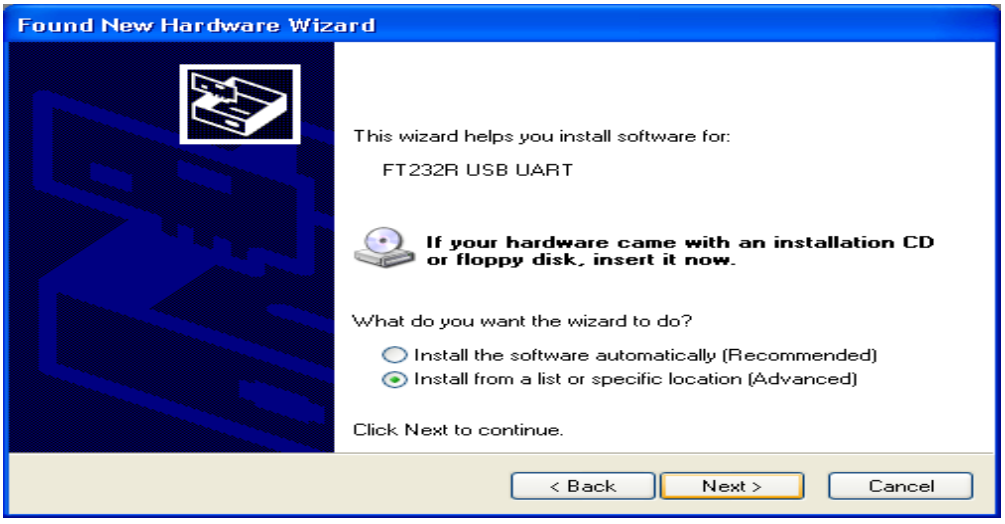

Fig 5.1 Arduino IDE interface

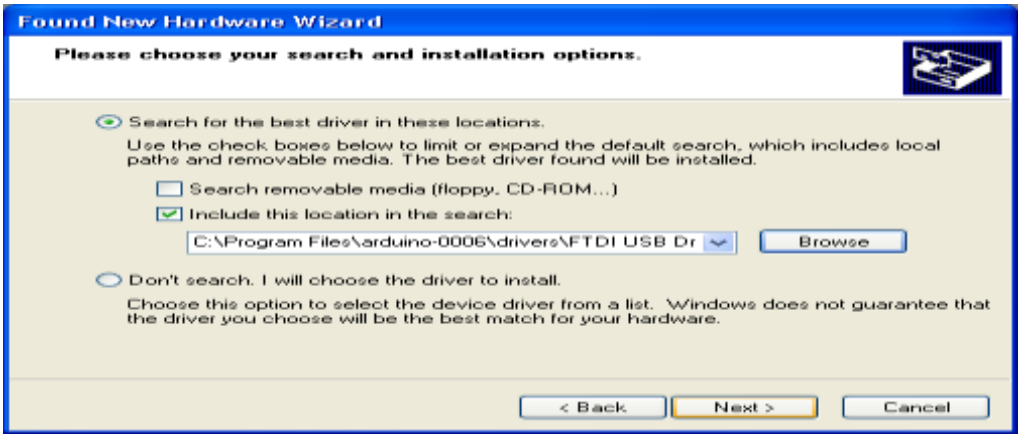

Fig 5.2 selecting the path

✓ Select “include this location in the search” and then click Browse option available in it.

- ✓ Now it will Automatically check the USB driver and the software is installed click Finish.

Fig 5.3 Finish the IDE

- ✓ Now click Finish, the Software will be downloaded.
- ✓ Now click on the Arduino IDE icon present on your Desktop. A window will appear like this.

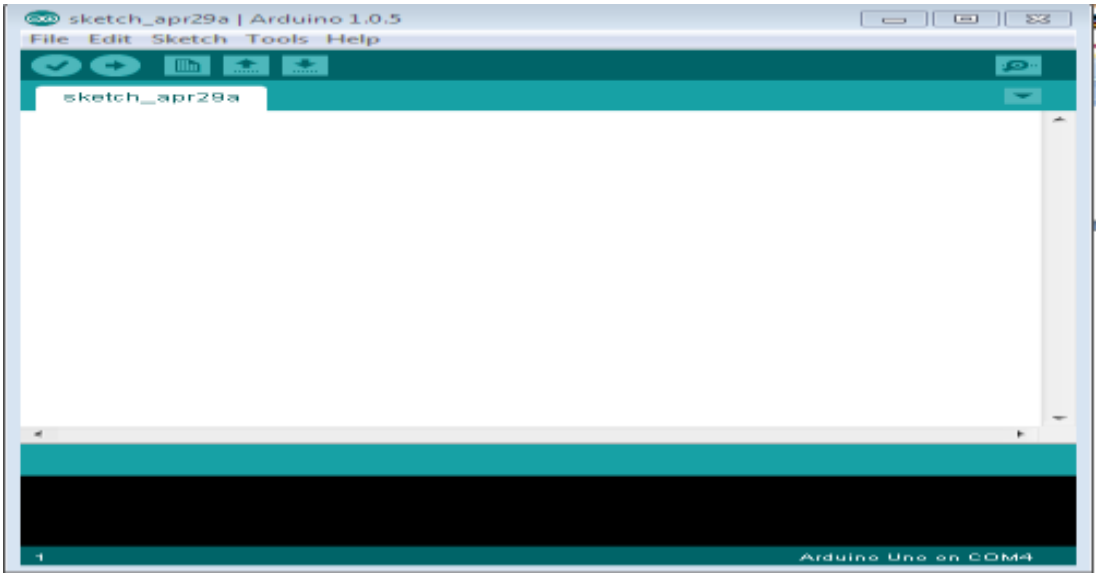

Fig 5.4 Opening Blank Interface

- ✓ For any sample programs, select FILE option→Examples.

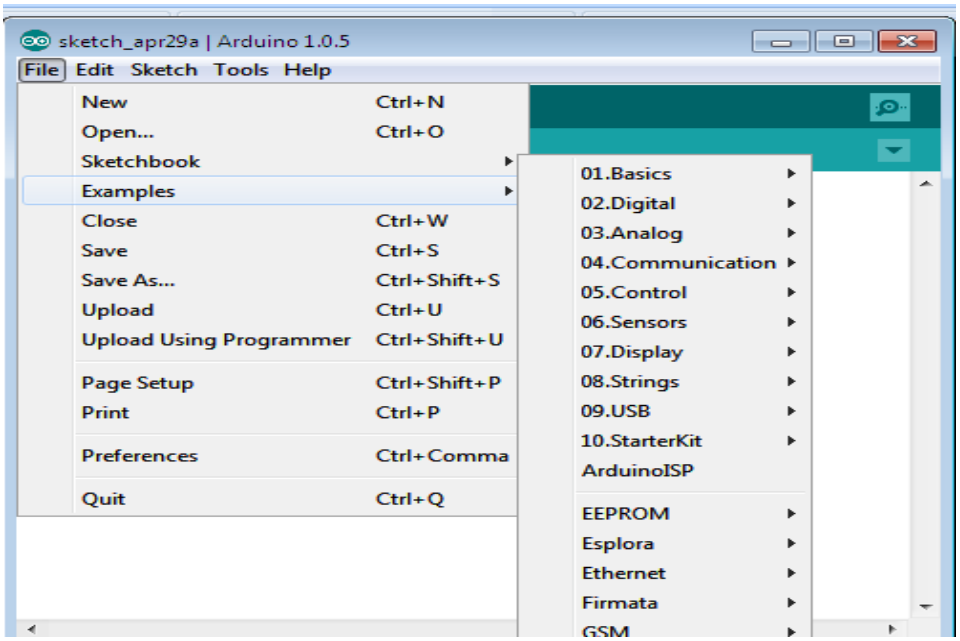

Fig 5.5 Opening Example

✓ After Entering the Sample Code in the file, it would look like this

Fig 5.6 Program

✓ Before Connecting we have to select which Board is used by the user, Basically UNO. By selecting TOOLS→Board→ARDUINO UNO

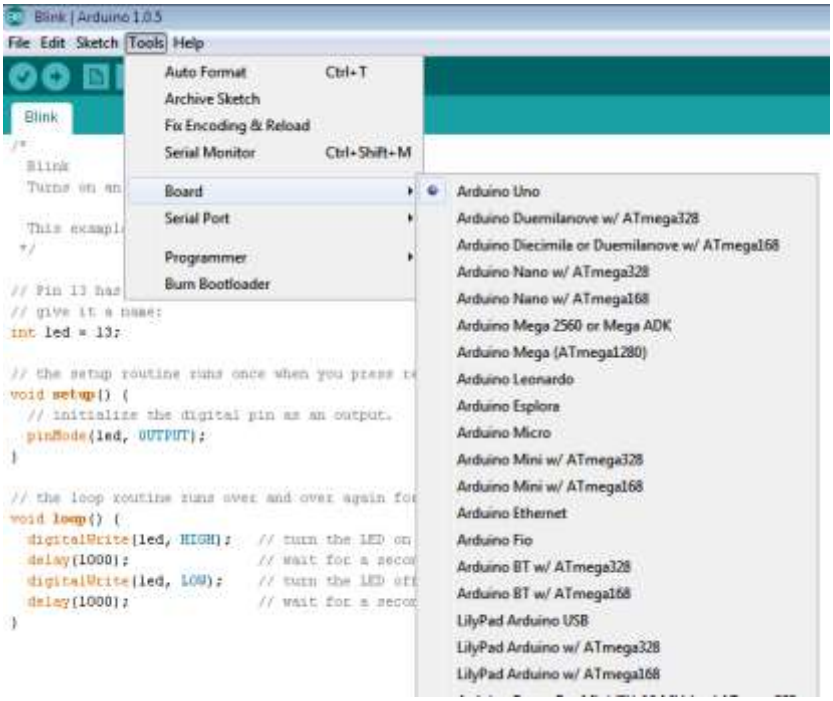

Fig 5.7 selecting The Board

- ✓ Now to dump the in the board Connect the Arduino to the PC through the USB port available in it. Like this TOOLS→SERIAL PORT→COMM4,COMM8 etc;

CHAPTER 6

ADVANTAGES AND APPLICATIONS

7.1 Advantages

- Enhanced Security

  Randomly generated PINs are harder for attackers to predict or brute-force.
- User-Centric Design

  Solutions are developed with a deep understanding of the users' needs and behaviors.
- Innovation

  Encourages out-of-the-box thinking to address complex problems.
- Iterative Development

  Allows for continuous refinement of the solution based on user feedback and testing.
- Reduced PIN Memorization
- Reduced Fraud
- Low cost
- Good performance
- Dynamic and Adaptive

7.2APPLICATION

- Banking and Finance
- Access Control
- Government Services
- Smart Home

CHAPTER 7

EXPERIMENTAL RESULTS

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.

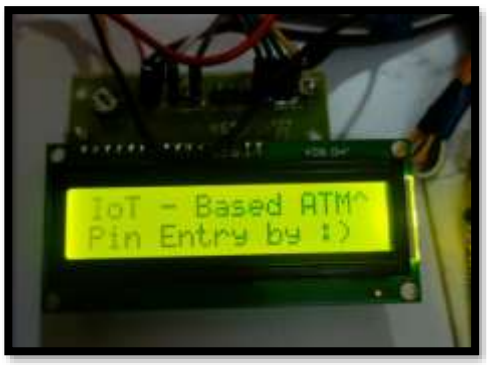

Fig 7.1 Interface of LCD

Fig 7.2 Waiting for Bluetooth

Fig 7.3 Word sent Message

Fig 7.4 Enter the Word Via Bluetooth

Fig 7.5 Data Verified Message

Fig 7.6 Data Invalid Message

Connection Diagram

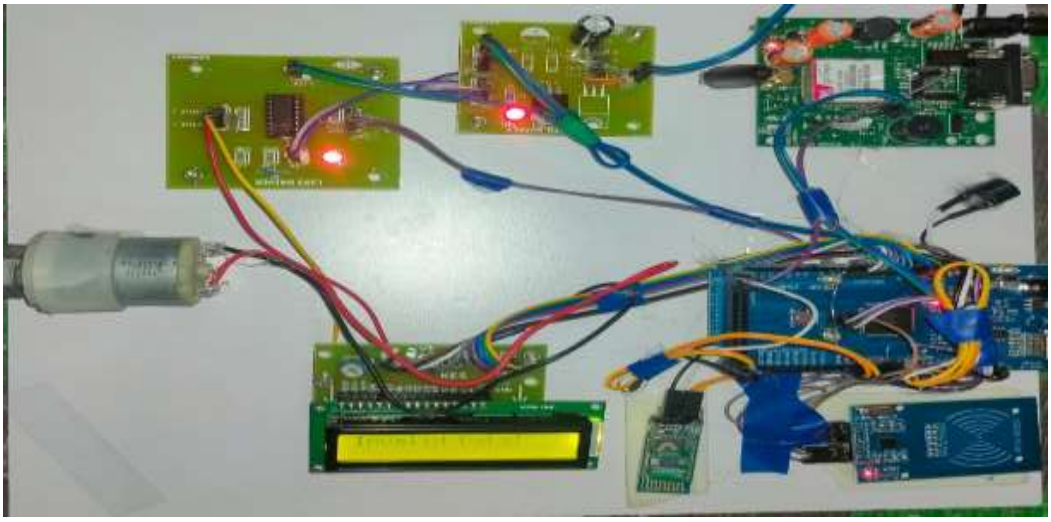

Fig 7.7 Output Diagram

CHAPTER 8

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.

FUTURE SCOPE

In envisioning the future scope of implementing ATM PIN authentication through a random word generator, the Design Thinking framework offers a structured approach. Initially, empathizing with users' needs and concerns regarding PIN security provides valuable insights. Through defining the problem statement and setting clear objectives, such as enhancing security and usability, the project gains direction. Ideation then allows for creative exploration of various implementation methods, considering factors like randomness and resistance to attacks. Prototyping brings these ideas to life, with user feedback guiding iterative refinement. Testing in real-world scenarios, followed by implementation and continuous iteration, ensures a robust and user-friendly solution. This approach ensures alignment with user needs, regulatory requirements, and industry standards, ultimately driving the successful adoption of the innovative ATM PIN authentication method.

CHAPTER 9

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, Gopalsingh Chouhan, Rutuja Tangade, Nikhilkumar 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] A. Marimuthu, S. Manikandan, "ATM Security System using GSM and MEMS Technology", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 9, September 2015.

[5] V. P. Leela, K. R. Sivaramakrishnan, "An Improved Authentication System for ATM using Fingerprint and GSM Technology", International Journal of Computer Applications, Vol. 72, No. 16, June 2013.

[6] R. Ramya, Dr. S. Suganya, "Enhanced ATM Security Model Using Fingerprint and GSM", International Journal of Computer Science and Mobile Computing, Vol. 4, Issue 4, April 2015.

[7] S. Sivasankar, P. Karthik, "Enhanced ATM Security System using GSM and Biometric Authentication", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 10, October 2014.

[8] M. Punithavalli, M. Shanmugapriya, "Secured ATM Transactions Using OTP and GSM Technology", International Journal of Science and Research (IJSR), Vol. 4, Issue 1, January 2015.

[9] K. Palanivel, S. Rajarajeswari, "ATM Security Enhancement Using Biometric and GSM Technology", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Issue 10, October 2014.

[10] R. Ganesan, M. Nagaraj, "A Study on Security Issues and Countermeasures in ATM Transaction Processing System", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 2, February 2014.

[11] M. Anbarasi, S. Arumugam, "An Intelligent ATM Theft Detection System using GSM Technology", International Journal of Engineering and Advanced Technology (IJEAT), Vol. 2, Issue 2, December 2012.

[12] G. Priya, T. Jayanthi, "Enhanced ATM Security System Using Biometric Technology and GSM", International Journal of Emerging Trends in Electrical and Electronics (IJETEE), Vol. 9, Issue 1, February 2014.

[13] S. N. Sandeep, R. Jayarani, "Design and Implementation of Secure ATM System Using GSM and Fingerprint Recognition", International Journal of Engineering Science and Technology (IJEST), Vol. 3, Issue 5, May 2011.

[14] A. Subashini, S. Saravanakumar, "Design and Implementation of Biometric ATM Security Model", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 5, May 2013.

[15] V. Thirumalaisamy, S. Sasirekha, "Design and Implementation of GSM Based ATM Theft Prevention System", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Issue 11, November 2014.

ANNEXURE-A

SOURCE CODE

```
#include <Wire.h>
#include <SoftwareSerial.h>
#include <MFRC522.h>
#include <LiquidCrystal.h>

#define SS_PIN 8   // Define SS_PIN for RFID
#define RST_PIN 9   // Define RST_PIN for RFID

SoftwareSerial gsmSerial(10, 11);

LiquidCrystal lcd(A5, A4, A3, A2, A1, A0);
MFRC522 mfrc522(SS_PIN, RST_PIN);
#define BUZZER_PIN 3
#define DC_MOTOR_PIN1 4
#define DC_MOTOR_PIN2 5
char receivedWord[5];
char actualWord[5];

// Declare the function before it's used
void dump_byte_array(byte *buffer, byte bufferSize);

void setup() {
  lcd.begin(16, 2);
  Serial.begin(9600);
  // Initialize serial for Bluetooth data
  pinMode(BUZZER_PIN, OUTPUT);
  pinMode(DC_MOTOR_PIN1, OUTPUT);
  pinMode(DC_MOTOR_PIN2, OUTPUT);
  digitalWrite(BUZZER_PIN, LOW);
  digitalWrite(DC_MOTOR_PIN1, LOW);
  digitalWrite(DC_MOTOR_PIN2, LOW);

  gsmSerial.begin(9600);

  SPI.begin();
  mfrc522.PCD_Init();
  lcd.clear();
  lcd.print("IoT - Based ATM^_^");
  lcd.setCursor(0, 1);
  lcd.print("Pin Entry by :)");
  delay(2000);
  lcd.clear();
  lcd.print("Random Word:)");
```

```
 lcd.setCursor(0, 1);
 lcd.print("Generator  ^_^");
 delay(2000);
 lcd.clear();  // Clear the LCD before waiting for user input
}

void loop() {
 if (checkRFID()) {
   generateRandomWord();        // Generate a new random word when an RFID card is detected
   printCardDetails();          // Print RFID card details to serial monitor
   sendGeneratedWord();         // Send the generated word via GSM
   delay(500);  // Add a delay to ensure a new random word for the next RFID card
   waitForBluetoothInput();     // Wait for user input via Bluetooth
   receiveAndValidateData();    // Receive and validate data via Bluetooth
 }
}

bool checkRFID() {
 if (mfrc522.PICC_IsNewCardPresent() && mfrc522.PICC_ReadCardSerial()) {
   return true;
 }
 return false;
}

void printCardDetails() {
 dump_byte_array(mfrc522.uid.uidByte, mfrc522.uid.size);
}

void generateRandomWord() {
 // Introduce a new random seed for better randomness
 randomSeed(analogRead(A0));

 // Generate a new random 4-letter word each time an RFID card is detected
 for (int i = 0; i < 4; i++) {
   actualWord[i] = char(random('A', 'Z' + 1));
 }
}

void sendGeneratedWord() {
 SendMessage("YourPhoneNumber", actualWord);  // Replace "YourPhoneNumber" with the
actual phone number
}

void SendMessage(const char* phoneNumber, const char* messageWord) {
 gsmSerial.println("AT");              // test check communication with GSM module
 delay(500);
```

```
  gsmSerial.println("ATE0");            // ATE0: Switch echo off. ATE1: Switch echo on.
  delay(500);
  gsmSerial.println("AT+CMGF=1");       // set SMS text mode
  delay(500);
  gsmSerial.println("AT+CMGS=\"+918688509417\"");
  gsmSerial.print(phoneNumber);
  gsmSerial.println("\"");              // send specific number
  delay(500);
  gsmSerial.print("Word: ");
  gsmSerial.print(messageWord);
  delay(500);
  gsmSerial.write(26);                 // ASCII code for Ctrl+Z to send SMS
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Word sent Check");
  lcd.setCursor(0, 1);
  lcd.print(" your mobile");
  delay(5000);
}

void waitForBluetoothInput() {
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Waiting for");
  lcd.setCursor(0, 1);
  lcd.print("Bluetooth...");

  // Wait for user input via Bluetooth
  while (!Serial.available()) {
    // Wait for data to be received
  }

  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Enter data via");
  lcd.setCursor(0, 1);
  lcd.print("Bluetooth");
  delay(2000);
}

void receiveAndValidateData() {
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Waiting for Data...");

  // Wait for data to be received via Bluetooth
```

```
 while (!Serial.available()) {
  // Wait for data to be received
 }

 // Read the received Word
 for (int i = 0; i < 4; i++) {
  receivedWord[i] = Serial.read();
 }
 // Validate the received data
 if (validateData()) {
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Data Verified!");
  // Perform actions for correct data (e.g., rotate motor)
  digitalWrite(DC_MOTOR_PIN1, HIGH);
  digitalWrite(DC_MOTOR_PIN2, LOW);
  delay(6000);
  digitalWrite(DC_MOTOR_PIN1, LOW);
  digitalWrite(DC_MOTOR_PIN2, LOW);
 } else {
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Invalid Data!");
  // Perform actions for incorrect data (e.g., activate buzzer)
  digitalWrite(BUZZER_PIN, HIGH);
  delay(5000);
  digitalWrite(BUZZER_PIN, LOW);
 }
}

bool validateData() {
 // Validate the received word with the generated word
 for (int i = 0; i < 4; i++) {
  if (receivedWord[i] != actualWord[i]) {
   return false;
  }
 }
 return true;
}

void dump_byte_array(byte *buffer, byte bufferSize) {
 for (byte i = 0; i < bufferSize; i++) {
  Serial.print(buffer[i] < 0x10 ? " 0" : " ");
  Serial.print(buffer[i], HEX);
 }
}
```

Annexure-B

ANNEXURE-B

PROJECT BUDGET DETAILS

S.no	Component Cost	Cost ($)
1	Arduino (AT Mega)	1259
2	Motor Driver(L293D)	100
3	LCD	250
4	Dc Motor	225
5	Buzzer	69
6	GSm	1700
7	Power Supply	250
8	RFID Module (RC522)	189
9	Bluetooth	190
10	Connecting wires & other	500
	Total	4,732

Annexure-C

© 2024 JETIR April 2024, Volume 11, Issue 4 www.jetir.org(ISSN-2349-5162)

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.

© 2024 JETIR April 2024, Volume 11, Issue 4 www.jetir.org(ISSN-2349-5162)

- **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.

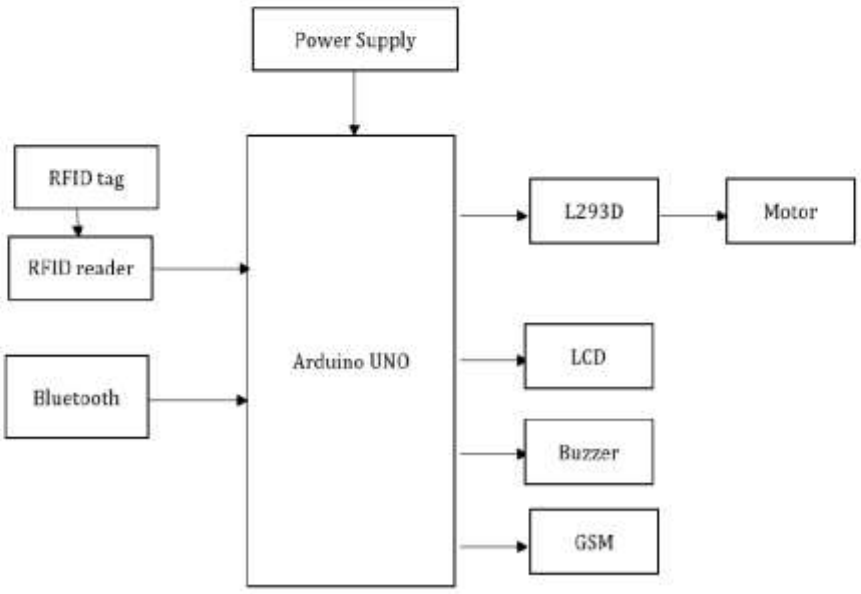

Fig. 1. Circuit Diagram

© 2024 JETIR April 2024, Volume 11, Issue 4 www.jetir.org(ISSN-2349-5162)

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

© 2024 JETIR April 2024, Volume 11, Issue 4 www.jetir.org(ISSN-2349-5162)

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

© 2024 JETIR April 2024, Volume 11, Issue 4 www.jetir.org(ISSN-2349-5162)

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.

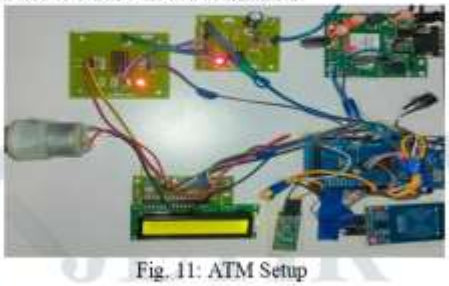

Fig. 11: ATM Setup

Fig. 12: Interface

Fig. 13: Waiting for Bluetooth

Fig. 14: Word sent message

Fig. 15: Waiting message

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.

© 2024 JETIR April 2024, Volume 11, Issue 4 www.jetir.org(ISSN-2349-5162)

[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.

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal Peer-reviewed, Refereed Journal
www.jetir.org | editor@jetir.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)

Is hereby awarding this certificate to

Ravi Babu B

In recognition of the publication of the paper entitled

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

Published In JETIR (www.jetir.org) ISSN UGC Approved (Journal No: 63975) & 7.95 Impact Factor

Published in Volume 11 Issue 4 , April-2024 | Date of Publication: 2024-04-18

Parisa P
EDITOR

EDITOR IN CHIEF

ISSN 2349-5162

JETIR2404666 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2404666 Registration ID : 537125

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal Peer-reviewed, Refereed Journal
www.jetir.org | editor@jetir.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)

Is hereby awarding this certificate to

Gowthami P

In recognition of the publication of the paper entitled

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

Published In JETIR (www.jetir.org) ISSN UGC Approved (Journal No: 63975) & 7.95 Impact Factor

Published in Volume 11 Issue 4 , April-2024 | Date of Publication: 2024-04-18

Parisa P
EDITOR

EDITOR IN CHIEF

ISSN 2349-5162

JETIR2404666 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2404666 Registration ID : 537125

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal Peer-reviewed, Refereed Journal
www.jetir.org | editor@jetir.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)

Is hereby awarding this certificate to

Ajay Kumar A B

In recognition of the publication of the paper entitled

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

Published In JETIR (www.jetir.org) ISSN UGC Approved (Journal No: 63975) & 7.95 Impact Factor

Published in Volume 11 Issue 4 , April-2024 | Date of Publication: 2024-04-18

Parisa P
EDITOR

EDITOR IN CHIEF

ISSN 2349-5162

JETIR2404666 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2404666 Registration ID : 537125

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal Peer-reviewed, Refereed Journal
www.jetir.org | editor@jetir.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)

Is hereby awarding this certificate to

Ajay C

In recognition of the publication of the paper entitled

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

Published In JETIR (www.jetir.org) ISSN UGC Approved (Journal No: 63975) & 7.95 Impact Factor

Published in Volume 11 Issue 4 , April-2024 | Date of Publication: 2024-04-18

Parisa P
EDITOR

EDITOR IN CHIEF

ISSN 2349-5162

JETIR2404666 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2404666 Registration ID : 537125

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal Peer-reviewed, Refereed Journal
www.jetir.org | editor@jetir.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)

Is hereby awarding this certificate to

Joshi B

In recognition of the publication of the paper entitled

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

Published In JETIR (www.jetir.org) ISSN UGC Approved (Journal No: 63975) & 7.95 Impact Factor

Published in Volume 11 Issue 4 , April-2024 | Date of Publication: 2024-04-18

Parisa P
EDITOR

EDITOR IN CHIEF

ISSN 2349-5162

JETIR2404666 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2404666 Registration ID : 537125

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal Peer-reviewed, Refereed Journal
www.jetir.org | editor@jetir.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)

Is hereby awarding this certificate to

Harish K

In recognition of the publication of the paper entitled

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

Published In JETIR (www.jetir.org) ISSN UGC Approved (Journal No: 63975) & 7.95 Impact Factor

Published in Volume 11 Issue 4 , April-2024 | Date of Publication: 2024-04-18

Parisa P
EDITOR

EDITOR IN CHIEF

ISSN 2349-5162

JETIR2404666 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2404666 Registration ID : 537125