WALLET FOR THE BLIND

DEPARTMENT PROJECT

LITERATURE SURVEY

Sl No	Title	Authors	Abstract
1.	Near Field Communication (NFC) - IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012	HUSSEIN AHMAD AL-OFEISHAT, MOHAMMAD A.A.AL RABABAH	NFCIP-1 enables simple, secure communication between electronic devices by allowing users to connect them effortlessly, unlike complex traditional networks, offering faster setup than Bluetooth or Wi-Fi.
2.	OneButtonPIN: A Single Button Authentication Method for Blind or Low Vision Users to Improve Accessibility and Prevent Eavesdropping: Proceedings of the ACM on Human-Computer Interaction, Volume 6, Issue MHCI	Manisha Varma Kamarushi, Stacey L. Watson, Garreth W. Tigwell, Roshan L. Peiris	OneButtonPIN is a secure, accessible PIN entry method for blind and low vision users using haptic vibrations. A user study showed its usability and resistance to shoulder surfing attacks.

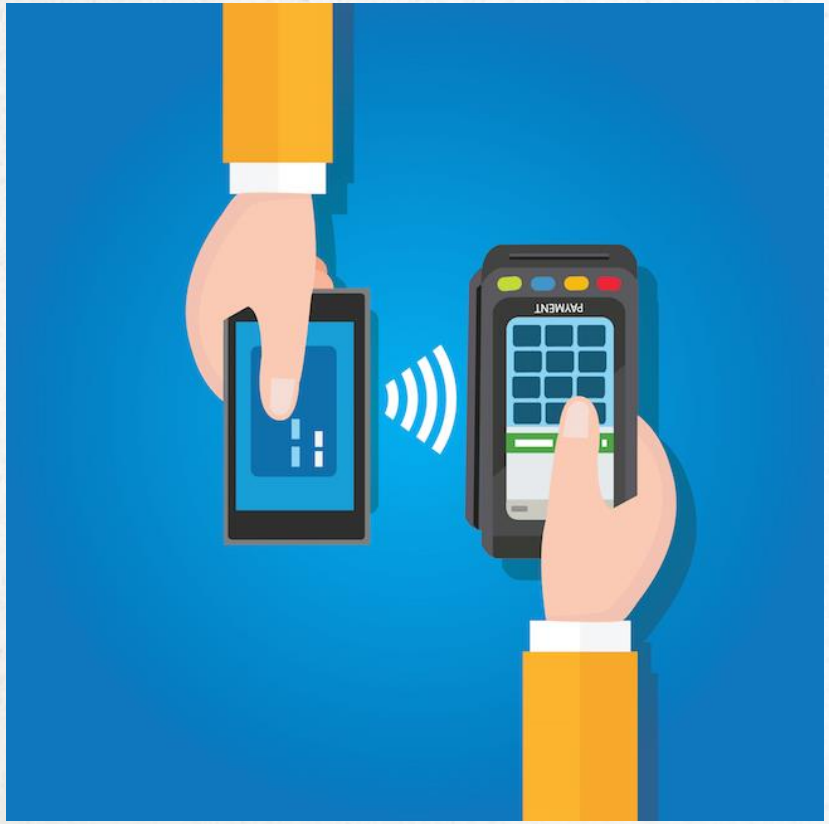
LITERATURE SURVEY

Sl No	Title	Authors	Abstract
3.	Haptic2FA: Haptics-Based Accessible Two-Factor Authentication for Blind and Low Vision People: Proceedings of the ACM on Human-Computer Interaction, Volume 8, Issue MHC	Palavi V. Bhole, Ziming Li, Shivang Bokolia, Tae Oh, Garreth W. Tigwell, Roshan L Peiris	Haptic2FA is a haptic-based two-factor authentication method designed to enhance accessibility for blind and low vision users. It replaces traditional passcodes with haptic patterns, improving usability and security. A study with 10 BLV participants evaluated its effectiveness and accessibility.
4.	A Study of Encryption Algorithms AES, DES and RSA for Security	Dr. Prerna Mahajan & Abhishek Sachdeva	This paper explores network security using cryptographic techniques, focusing on AES, DES, and RSA algorithms. It compares their encryption and decryption performance through simulation, analyzing execution time to evaluate each algorithm's effectiveness in securing data transmission.

OBJECTIVES

- Make a secure wallet for Blind people that makes use Tap to Pay technology (NFC) to provide convenience
- Establish protection from theft by using biometrics / haptics based Two Factor Authentication.
- Automatically top up the wallet when the wallet balance goes below a particular amount.
- Ensure that the size of the device does not exceed that of a normal credit card.

HOW NFC PAYMENT WORKS



1. The POS initiates transaction by sending a GPO command which contains details like transaction amount, transaction currency, etc, through NFC.
2. The card then receives this data (through NFC) and then sends the required information like card number, cvv, expiration dates, etc only after encrypting it (using means like RSA).
3. Once the POS receives this encrypted information, it processes the transaction by sending this information to the bank servers.

HOW THE WALLET WILL WORK

1. The card details like the 16 digit card no., CVV, expiry date along with a 2FA PIN will be stored inside an EEPROM chip/module (like AT24C256 EEPROM). All of this will be encrypted by using RSA and AES encryption
2. The chip/module will be connected to the microcontroller which will decrypt this data.
3. The user will first have to enter a pin to activate the wallet by using a single button with haptics in it, which uses the concept of OneButton PIN, wherein the digit entered by the user will correspond to the number of vibrations that occurred when the user held the button.
4. Once the PIN is entered, it is verified by comparing it to the PIN stored in the EEPROM. Once verified, the device will be “activated”.
5. i) For now, the wallet will send the transaction details to a dummy backend server using the 4G capabilities of the microcontroller with the necessary encryption.
   ii) In future we plan to include an NFC module which will be used to receive and send the transaction details after using the necessary encryptions. Operating frequency = 13.56MHz

RAM AND STORAGE UTILIZATION

- For taking PIN input – 2-3KB
- For reading and decrypting data from EEPROM – 190-200 bytes
- Data stored in EEPROM – 64 bytes (approx.)
- Encryption of transaction details and sending it via NFC – 1.5-2KB
- Overhead costs – 20 KB

DATA TRANSFER LOGIC

- Data -> encrypted using AES-GCM
- key to break this -> encrypted using RSA-1024 OR RSA-2024 with OAEP padding (depending on available size)
- Encrypted data + encrypted key saved on eeprom

==> SENT TO MICRO-CONTROLLER ==>

- key obtained by breaking rsa encryption using private key already available within micro-controller
- key is used to break the aes-gcm encryption
- final data is obtained

DATA TRANSFER LOGIC

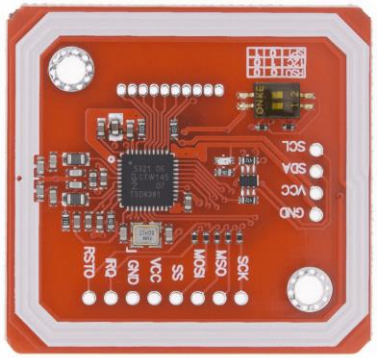
Libraries to be used

I. mbedTLS(only load required modules like "MBEDTLS_AES_C, MBEDTLS_RSA_C, MBEDTLS_CTR_DRBG_C, and MBEDTLS_ENTROPY_C" , discard modules like support for TLS protocols)

II. WolfSSL

AT24C256 EEPROM
(soldered)

Button with Haptics



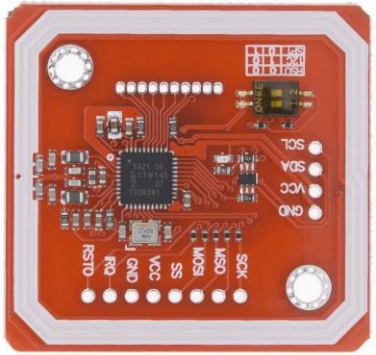
PN532 NFC
Module
(13.56 MHz)

SAMPLE MODEL

EEPROM CHIP SOLDERED ON THE MICROCONTROLLER

Custom EEPROM Module which can be attached and removed from the microcontroller

Button with Haptics



PN532 NFC Module (13.56 MHz)

SAMPLE MODEL - 2

EXTERNAL EEPROM MODULE

COST

- Button with Haptics (like AdaFruit 1201) – 200Rs
- NFC Module (PN532) – 250Rs (approx.)
- Readymade EEPROM module (AT24C256 EEPROM Module) – 60 Rs

OR

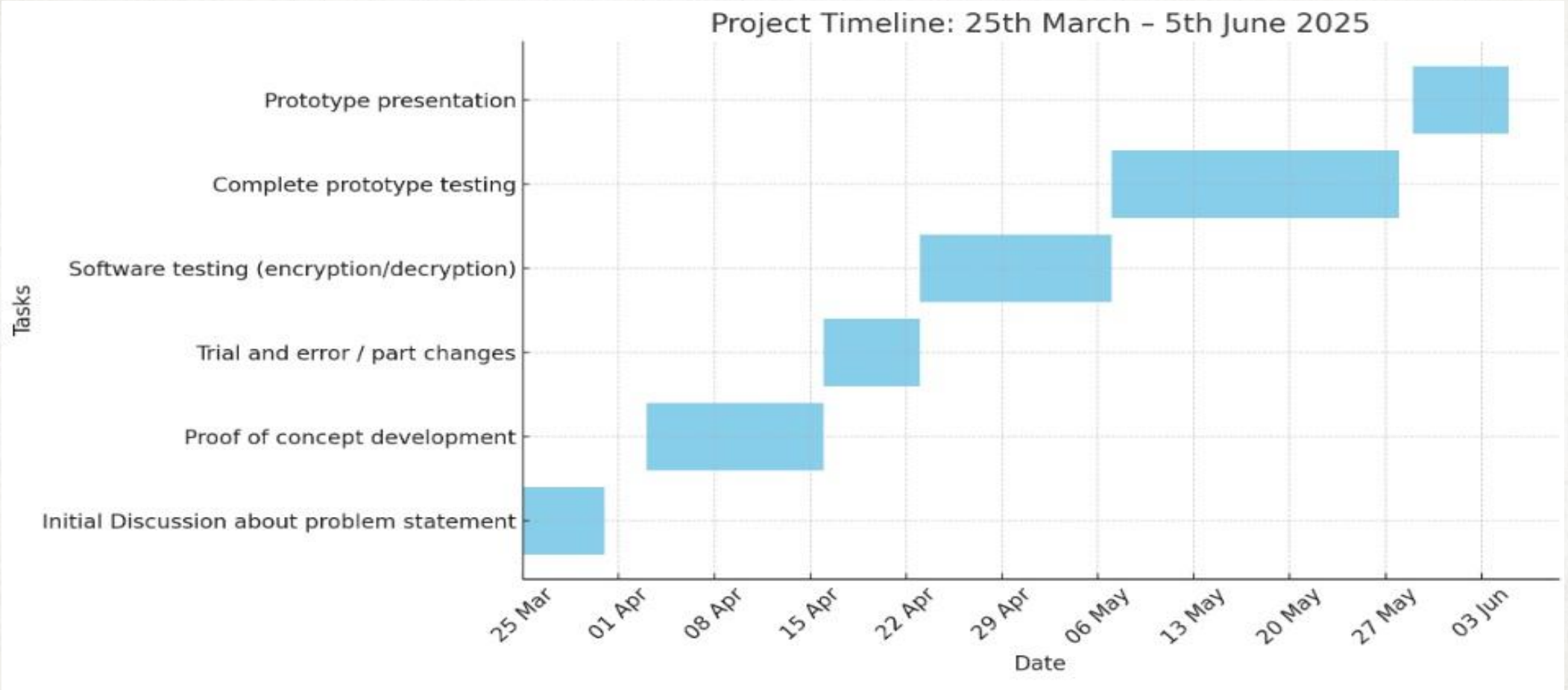
Custom EEPROM module (to conveniently attach/detach it from microcontroller) :

i)Custom Security Key – 400 Rs

ii)Reading mechanism for custom key – 300 Rs

} 700 Rs

GANTT CHART


Project Timeline: 25th March – 5th June 2025
Tasks
Prototype presentation
Complete prototype testing
Software testing (encryption/decryption)
Trial and error / part changes
Proof of concept development
Initial Discussion about problem statement
25 Mar
01 Apr
08 Apr
15 Apr
22 Apr
29 Apr
06 May
13 May
20 May
27 May
03 Jun
Date

CONTRIBUTION CHART

1. Amol Vyas: Two Factor Authentication required before making transaction
2. Akshat Arya: Data Transfer Procedures
3. Akshat Gupta: Implementation of the algorithms and simulation of bank server
4. Abhyuday Sharma: Selection of most cost effective and optimised hardware for storing encrypted data(pin, card account number, , expiry date etc) - Research on hod available Dot Peening to Laser Engraving

END