RV College of Engineering®

Go, change the world

RASHTREEYA SHIKSHAN SAMITHI TRUST

R.V. COLLEGE OF ENGINEERING

(An Autonomous Institution affiliated to Visvesvaraya Technological University, Belagavi)

Cyber security

EL Report

Submitted by	TALASILA DHEERAJ – RVCE22BCS151
Submitted to	Dr. Krishnappa H. K. Associate Professor Theoretical Computer Science, Image Processing, Pattern Recognition

Table of Contents:

PROBLEM STATEMENT

Various Types of Digital Payment Systems: Bharat QR Code and Bharat Interface for Money (BHIM) App

INTRODUCTION

In today's digital era, cashless transactions have gained significant momentum. Digital payment systems have revolutionized the way we conduct financial transactions, providing convenience, speed, and security. In this presentation, we will delve into two prominent digital payment methods: Bharat QR Code and Bharat Interface for Money (BHIM) App. We will explore their features, benefits, and security aspects.

Bharat QR

Bharat QR is a revolutionary payment system that allows users to make digital payments using their smartphones. It is a quick, easy, and secure way to pay for goods and services without the need for cash or cards.
Bharat QR Code is a standardized QR code payment system introduced by the National Payments Corporation of India (NPCI). It enables users to make payments by scanning QR codes displayed at merchant outlets or websites.

How Bharat QR works?

1. A customer scans the QR code using a compatible payment app on their smartphone.
2. The app decodes the QR code and retrieves payment details such as merchant ID and transaction amount.
3. The customer confirms the payment and authorizes the transaction using their preferred payment method, such as a linked bank account or mobile wallet.
4. The payment is processed, and a confirmation notification is sent to both the customer and the merchant.

Benefits of Bharat QR

1. **Convenience**: Eliminates the need for physical cash, cards, or POS terminals, allowing seamless and contactless payments.
2. **Wide Acceptance**: Accepted by a vast network of merchants, including small businesses, without the need for additional infrastructure.
3. **Interoperability**: Supports multiple payment methods, such as debit cards, credit cards, UPI, and digital wallets.
4. **Security**: Provides secure transactions with end-to-end encryption and tokenization of sensitive information.

BHIM App

BHIM App is a revolutionary digital payment system that has been developed by the National Payments Corporation of India (NPCI). It allows users to make instant payments using their mobile phones, without the need for cash or credit cards. With BHIM App, users can easily transfer money to anyone with a UPI ID or mobile number, pay bills, and even recharge their mobile phones

Key features of BHIM App

1. **Easy Registration**: Users can link their bank accounts to the app by providing necessary details.
2. **Transaction Options**: Allows users to send and receive money, check balance, and make payments using virtual payment addresses (VPAs).
3. **Scan and Pay**: Users can scan QR codes to make quick payments at merchant outlets.
4. **Multiple Language Support**: BHIM App supports various regional languages, making it accessible to a wider user base.
5. **Security Measures**: Implements multi-factor authentication, device binding, and PIN protection for secure transactions.

Advantages of BHIM App

1. **User-Friendly:** Offers a simple and intuitive interface, enabling users of all technical backgrounds to navigate and use the app effectively.
2. **Speedy Transactions:** Provides real-time fund transfers, ensuring instant payment settlements.
3. **Cashback and Incentives:** BHIM App often offers cashback rewards and promotional incentives to encourage its usage.
4. **Wide Acceptance:** Supported by a large number of merchants, online platforms, and utility service providers.

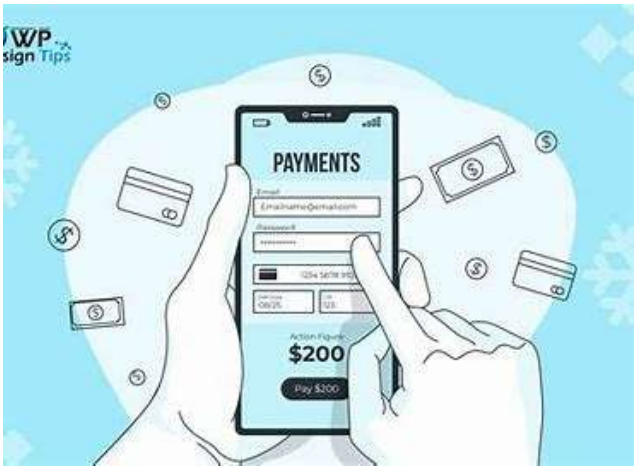
ROLE OF CYBER SECURITY

Paying through Bharat QR Code involves various technologies to ensure a secure and efficient transaction process. They are:

1) QR Code Generation and Scanning:
   •QR Code Encoding: To generate a Bharat QR Code, computer algorithms are used to encode payment-related information such as the merchant's identifier, transaction amount, and other details into a QR code format.
   •QR Code Decoding: When a user scans the QR code using a compatible payment app, computer algorithms in the app decode the QR code, extracting the payment details encoded within.

2) Secure Communication and Data Encryption:
   •Network Communication: The payment app utilizes network protocols (such as HTTPS) to securely communicate with the merchant's server or payment gateway. This ensures the confidentiality and integrity of the transmitted data.
   •Encryption: To protect sensitive information during transmission, cryptographic algorithms (such as SSL/TLS) are employed to encrypt the data, preventing unauthorized access and tampering.
   •Public Key Infrastructure (PKI): PKI concepts are used for secure key exchange and digital signatures, ensuring the authenticity and integrity of the transaction.

3) Payment Gateway Integration:
   • Backend Systems: Payment app developers need to integrate the app with the backend systems, including payment gateways, banks, and other financial institutions. This involves using APIs (Application Programming Interfaces) provided by these entities to facilitate seamless and secure transaction processing.
   • Data Validation and Verification: The payment gateway performs validation and verification of the transaction details received from the payment app, ensuring the accuracy of the information and preventing fraud.



4) Security Measures:
   • User Authentication: The payment app incorporates user authentication mechanisms such as PINs, biometrics, or passwords to ensure that only authorized users can initiate transactions.
   • Tokenization: Sensitive information, such as card details or bank account numbers, is replaced with unique tokens during the transaction process. This reduces the risk of data breaches, as tokens have limited usability and cannot be used to reconstruct the original data.
   • Anti-Fraud Measures: Various computer science techniques, such as anomaly detection, machine learning, and artificial intelligence, may be employed to detect and prevent fraudulent transactions in real-time.

5) Data Storage and Privacy:
   • Compliance: The payment app is adhered to data protection regulations and security standards to ensure the privacy and confidentiality of user data, including the General Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard (PCI DSS).
   • Secure Storage: Sensitive user data, such as transaction history or payment details, must be stored securely using encryption and access control mechanisms to prevent unauthorized access.

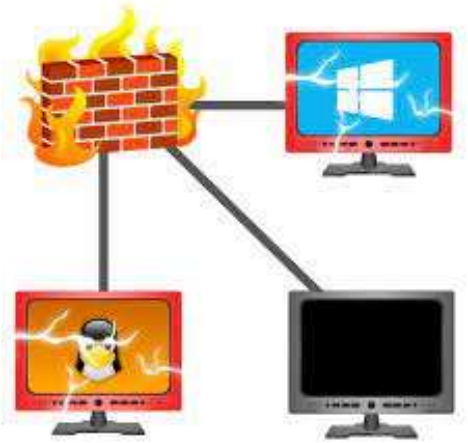
CYBER THREATS IN BHARAT QR AND BHIM APP

1) Malware and Mobile Attacks:
   •Malicious Apps: Users may unknowingly download malicious apps that mimic legitimate payment apps, which can steal sensitive information, including login credentials and transaction details.
   •Phishing Attacks: Cybercriminals may employ phishing techniques to trick users into revealing their personal information, such as usernames, passwords, or OTPs, through fake websites or emails.

2) Social Engineering:
   •Impersonation: Attackers can pose as legitimate organizations or individuals to deceive users into sharing confidential information, such as OTPs or bank account details, by phone calls, messages, or emails.
   •Vishing: Attackers may use voice-based phishing techniques to manipulate users into disclosing sensitive information over phone calls, often pretending to be customer support representatives or bank officials.

3) Device and Network Exploitation:
   •Man-in-the-Middle (MitM) Attacks: Attackers intercept and alter communication between the user's device and the payment infrastructure, allowing them to capture sensitive information or modify transaction details.
   •Wi-Fi Snooping: Cybercriminals can eavesdrop on insecure Wi-Fi networks to intercept and steal user data, including payment details,

when using Bharat QR or BHIM App.



4) Account Takeover:
   •Credential Theft: Attackers may employ various methods, such as keyloggers or phishing, to steal user login credentials for the Bharat QR or BHIM App, enabling them to gain unauthorized access to user accounts.
   •SIM Swapping: Attackers can attempt to convince mobile network providers to transfer a user's phone number to a new SIM card under their control, allowing them to intercept OTPs and bypass security measures.

5) Data Breaches:
•Server Breaches: Cybercriminals may target the servers storing user data and transaction information, potentially exposing sensitive details, including bank account numbers, addresses, and transaction history.
•Insider Threats: Unauthorized access or malicious actions by employees or insiders with privileged access to the systems may lead to data breaches or compromise user information.

6) Lack of Security Updates:
•Outdated Software: Using outdated versions of the Bharat QR or BHIM App or operating systems on mobile devices can leave users vulnerable to known security vulnerabilities that attackers can exploit.

BEST PRACTICES FOR CYBER SECURITY

1) Download and Update Securely:
   • Download official apps: Ensure you download the official Bharat QR or BHIM App from trusted sources like official app stores.
   • Regular updates: Keep the app and your mobile device's operating system up to date with the latest versions to benefit from security patches and bug fixes.

2) Be Cautious of Phishing Attempts:
   •Verify authenticity: Exercise caution and verify the authenticity of communication or requests before sharing any personal or financial information.
   •Avoid suspicious links: Be wary of clicking on links from unknown sources, as they may lead to phishing websites or malware downloads.

3) Strong Authentication and Passwords:
•Use strong passwords: Create strong, unique passwords for your Bharat QR or BHIM App account, and avoid using easily guessable information.
•Enable multi-factor authentication: Whenever available, enable multi-factor authentication to provide an additional layer of security to your account.

4) Secure Network Usage:
•Avoid public Wi-Fi networks: Refrain from using public Wi-Fi networks for transactions, as they are often unsecured and prone to interception. Instead, use secure networks or your mobile data connection.

5) Monitor Account Activity:
   •Regularly review transactions: Keep a close eye on your account activity and transaction history to detect any suspicious or unauthorized transactions.
   •Report suspicious activity: If you notice any unusual or unauthorized activity, promptly report it to the appropriate authorities or your bank.

CONCLUSION

In conclusion, Bharat QR and BHIM app are powerful tools that have revolutionized the way we make digital payments. However, with great power comes great responsibility, and it is important to be aware of the cybersecurity threats that come with using these apps.

We must be aware of various cybersecurity threats such as phishing, malware, and hacking, and suggested preventive measures such as using strong passwords, enabling two-factor authentication, and keeping devices updated. We should also follow some best practices such as avoiding public Wi-Fi, not sharing personal information, and reporting suspicious activities.

REFERENCES

[1] UPI123PAY: Making UPI Transactions Without Internet a Reality - INVC

[2] What Is Bharat QR Code & How It Will Benefit Your Business - 8 Questions

[3] Web Application Security: 9 Best Practices You Need To Know - Desol Int

[4] Payment Card Industry Data Security Standard (PCI DSS) | BSI Australia (

[5] National Payments Corporation of India (NPCI) - Enabling digital payments

LITERATURE SURVEY

[1] NPCI's documentation on Bharat QR Code and BHIM App

[2] Reserve Bank of India (RBI) guidelines on digital payments