



# Bus Electronic-Card payment system using IoT, Cryptography & Web technology

Madhusudan Rao Badukonda<sup>1</sup>, Darshan Battula<sup>2</sup>, Madhuri Kanakala<sup>2</sup>, Harshit Nambaru<sup>2</sup>,

Iswarya Lakshmi Potnuru<sup>2</sup>

- 1 Assistant Professor, Department of Information Technology, Anil Neerukonda Institute of Technology and Sciences, Sangivasa, Visakhapatnam, Andhra Pradesh, India  
2 Department of Information Technology, Anil Neerukonda Institute of Technology and Sciences, Sangivasa, Visakhapatnam, Andhra Pradesh, India.

**Abstract**— The Road Transport Corporation (RTC) in India faces numerous challenges related to ticketing inefficiencies, fare collection discrepancies, and passenger inconveniences. To address these issues, this project proposes the implementation of an innovative bus e-card system. Utilizing E-card technology, Internet of Things (IoT) devices, advanced cryptography techniques, and user-friendly web interfaces, this system aims to transform the payment transactions and passenger interactions within RTC.

At its core, the bus e-card system simplifies payment processes by enabling cashless transactions, eliminating the need for physical currency, and ensuring accurate fare calculations. Recharging the smart card is effortless, streamlining travel experiences and saving time during transactions. Real-time data collection enables dynamic adjustments to bus routes, optimizing travel efficiency for passengers.

Moreover, the bus e-card system is poised to bolster RTC's revenue streams by reducing revenue loss associated with manual fare collection methods. By eliminating physical ticket verification, the system minimizes instances of ticketless travel and fare evasion, ensuring precise revenue collection for the corporation.

For passengers, this system offers numerous benefits, enhancing the overall travel experience. It facilitates faster, easier, and more enjoyable trips, reducing waiting times and improving accessibility to transportation services. Online payment options

provide increased flexibility and convenience, resulting in shorter queues, reduced congestion, and improved seating

availability at bus stations. Ultimately, passengers will experience greater satisfaction with the bus system.

**Keywords** — *Road Transport Corporation, bus e-card system, Internet of Things, cashless transactions, fare collection, passenger experience.*

## I. INTRODUCTION

The Bus-E-Card payment system represents a paradigm shift in bus travel payment solutions, integrating cutting-edge web interfaces and IoT technologies to enhance the overall passenger experience and operational efficiency. Building upon the holistic approach outlined in the methodology, the applications of the Bus-E-Card system encompass a range of functionalities designed to streamline fare management, provide real-time updates, and promote sustainable practices in public transportation.

### *Applications*

Cashless Transactions, Convenient Fare Management, Real-Time Updates, Personalized Services, Route Optimization, Enhanced Security, Promotion of Sustainable Practices, Streamlined Operations.

### *Web Interfaces*

Web interfaces serve as user-friendly online platforms for managing e-cards, checking balances, topping up funds, and accessing services. These interfaces leverage HTML5, CSS3, and JavaScript to provide intuitive user experiences. Additionally, SHA-256 or SHA-512 encryption algorithms are employed to ensure data integrity and security, safeguarding user information throughout interactions with the platform.

### *IoT Technology*

The Internet of Things (IoT) encompasses devices equipped with sensors and internet connectivity for real-time data collection and monitoring. In the context of this project, IoT devices gather data on passenger flow, usage patterns, and route efficiency.

### *Integration of Web and IoT*

The seamless integration of web and IoT technologies enables interactive experiences between passengers, e-cards, and the transportation system. This integration automates fare deduction, provides real-time updates, personalized notifications, and data-driven insights for route optimization.

### *Purpose of the Study*

This study aims to introduce a revolutionary Bus-E-Card system, leveraging web and IoT technologies, to transform bus travel payment experiences. By seamlessly integrating electronic cards into the transportation system, the project endeavours to streamline payment processes, enhance passenger convenience, and optimize route efficiency.

### *Scope of the Study*

The scope of this study encompasses the development and implementation of the Bus-E-Card system, focusing on two pivotal components: web interfaces and IoT infrastructure. Through user-friendly web platforms and advanced IoT devices, the system aims to redefine bus travel by offering secure, efficient, and cashless payment solutions.

### *Significance of the Study*

The significance of this study lies in its potential to revolutionize bus travel payment systems, addressing issues related to ticketing inefficiencies, fare collection discrepancies, and passenger inconveniences. By integrating web and IoT technologies, the Bus-E-Card system aims to enhance the overall passenger experience, promote sustainable practices, and optimize transportation services.

## II. LITERATURE REVIEW

Martínez-Ballesté et al. (2023) [1] offer a comprehensive examination of ticketing systems in smart transportation, highlighting their importance in ensuring convenient and secure access to public transportation services within smart cities. The authors stress the need to address strong security and privacy requirements, given advancements in sensors, IoT devices, and 5G communication technologies.

The study underscores ticketing systems' significance in facilitating access to various modes of public transportation, while also emphasizing the importance of navigating security challenges to protect user information and transaction integrity. Key considerations include robust security mechanisms against data breaches and unauthorized access, as well as the role of lightweight

cryptography in securing ticketing systems on smartphones and IoT devices.

Overall, the paper provides valuable insights into the complexities and challenges associated with ticketing systems in smart transportation, emphasizing the importance of implementing robust security measures to ensure transaction reliability and integrity.

**P. T. Blythe (2004) [2]** Discusses the rising adoption of electronic smart cards for accessing and paying for transport services, especially highlighted by the introduction of the Oyster smart card in London. The paper emphasizes the benefits of smart cards in modernizing transport systems and enhancing user experience, with efforts underway to address interoperability between schemes.

In a related study, Brand and Preston (2003) explore various technologies suitable for urban public transport systems, including smart cards. They analyze factors influencing technology selection and deployment strategies within urban transport networks.

Bagchi and White (2004) focus on utilizing smart-card data from bus systems to enhance operational efficiency and inform decision-making processes within the public transport sector.

Hounsell (2004) examines the role of intelligent transport systems, including smart cards, in optimizing bus operations and improving service reliability in urban environments.

These studies collectively highlight the growing importance of smart cards in revolutionizing public transport ticketing systems and improving the efficiency, accessibility, and sustainability of urban transportation networks.

**Turban and Brahm (2009) [3]** Provide a detailed analysis of smart card-based electronic payment systems in the transportation industry. They argue for the superiority of electronic card payment systems over traditional methods like cash or credit cards, focusing on their suitability for mass transportation. The authors discuss strategic decisions faced by transportation managers and emphasize the role of local area networks in facilitating transactions.

In a related study, Blythe (2007) explores the transformative potential of smart cards in revolutionizing access to and payment for transport services. Smart card technology is highlighted for its ability to enhance efficiency, accessibility, and sustainability of transportation networks by streamlining fare collection processes and improving service reliability.

Overall, these studies underscore the growing significance of smart card-based electronic payment systems in the transportation industry. They highlight benefits such as improved customer experience, operational efficiency, and security.

**P. Panagiotau, and N Sklavos [4]** The Internet of Things (IoT) is reshaping technology by connecting physical

devices to the internet for data exchange. Cryptography plays a vital role in securing IoT data, with symmetric key algorithms like AES commonly used. Security concerns persist due to inadequate measures in IoT hardware platforms. The UDOO Neo board is a promising choice for implementing cryptographic systems in IoT. Proposed systems leverage AES for encryption, offering advanced security schemes like AES GCM and GMAC. These systems also integrate user authentication mechanisms for enhanced security.

### III. METHODOLOGY

The methodology for developing the Bus-E-Card system encompasses a holistic approach aimed at revolutionizing bus travel payment through the seamless integration of electronic cards. At the core of this project lie two pivotal components:

1. web Interaction.
  - 1.1 Cryptography
    - 1.1.1 User Security
    - 1.1.2 Data Integrity
  - 1.2 OTP authentication
2. Internet of Things (IoT) infrastructure
  - 2.1 HMAC (Hash based message authentication code)

Commencing with user registration, individuals provide their details for E-card issuance. Upon verification and meeting eligibility criteria, users are allocated a web profile with unique login ID & password reset option. Then user should attempt the password reset after submission of new password he get an OTP for authentication after successful authentication the password will be save in the database for data integrity SHA algorithm was used. Subsequently, physical cards are prepared and dispatched to users, embedding secure details for cashless travel experiences.

Upon receiving the physical card, its role in facilitating smooth travel transactions becomes paramount. Through a simple tap-and-pay mechanism, users can effortlessly settle their travel fares. Hardware components such as NodeMCU and ESP32 take charge of user verification responsibilities, facilitating seamless interactions between users and the system.

#### 1) Web Interaction

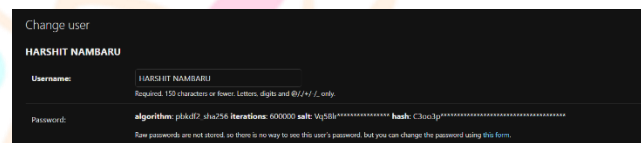
Moving on to the web profile flow, user interaction is streamlined through a user-friendly interface on the Bus-E-Card web platform. Users are presented with the option to either log in with existing credentials or register as new users. Upon successful login, users gain access to their profile, where they can manage their balance and recharge their card if necessary. For registration, users select their user type (student or employee), with details sent for verification via the admin database. Upon successful registration, users can log in using their newly created credentials, facilitated by HTML, CSS, and JavaScript-powered interfaces.

Integration with Razorpay enables users to recharge their cards seamlessly through the payment gateway. Meanwhile, the IoT flow encompasses the utilization of

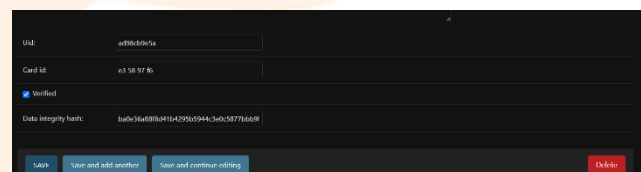
equipment such as NodeMCU, ESP32, RFID/NFC cards, LCD 16x2 I2C sensor, and buzzer for card verification. Users tap their cards on the RFID/NFC reader, initiating a [1] process where data is retrieved and communicated with the database for user verification. Python libraries such as the SMTP library for email notifications are utilized for sending login details to users during the registration process. Following a balance check, fare deduction, and balance update, users receive feedback through display messages indicating successful verification or any issues encountered.

Furthermore, the system records travel timestamps and deducted amounts in the database for comprehensive data integration. This data informs the user profile page, ensuring users have real-time access to their travel history and remaining balance. Through meticulous implementation of these methodologies, the Bus-E-Card system endeavours to redefine bus travel by offering a secure, efficient, and cashless payment solution.

#### [1.1.1] User Security



#### [1.1.2] Data Integration



In our project, we implement the SHA algorithm for data integrity to securely store users' new passwords in the database. Cryptographic hash functions such as SHA-256 or SHA-512 are commonly utilized for this purpose. These hash functions generate a fixed-size hash value (digest) from the input data, ensuring uniqueness to the input. Even a minor alteration in the input data results in a significantly different hash value.

To implement data integrity checks using cryptographic hashing in our models, we follow these steps:

1. Selection of Fields: We choose critical fields that represent the data whose integrity we want to verify.
2. Hash Calculation: When the data is saved to the database, we calculate the hash of these selected fields and store it alongside the data.
3. Verification Process: Upon retrieving the data, we recalculate the hash and compare it with the stored hash to verify integrity.

Checking data integrity in your application typically occurs in scenarios where you need to ensure that the critical data stored in your models hasn't been tampered with. Here are

some common scenarios where you might want to check data integrity regarding users in the application:

**Ensuring Data Integrity for Authentication:**

When a user logs in or attempts to access their account, you can verify the integrity of their user data to ensure that their account details haven't been modified since they were last saved.

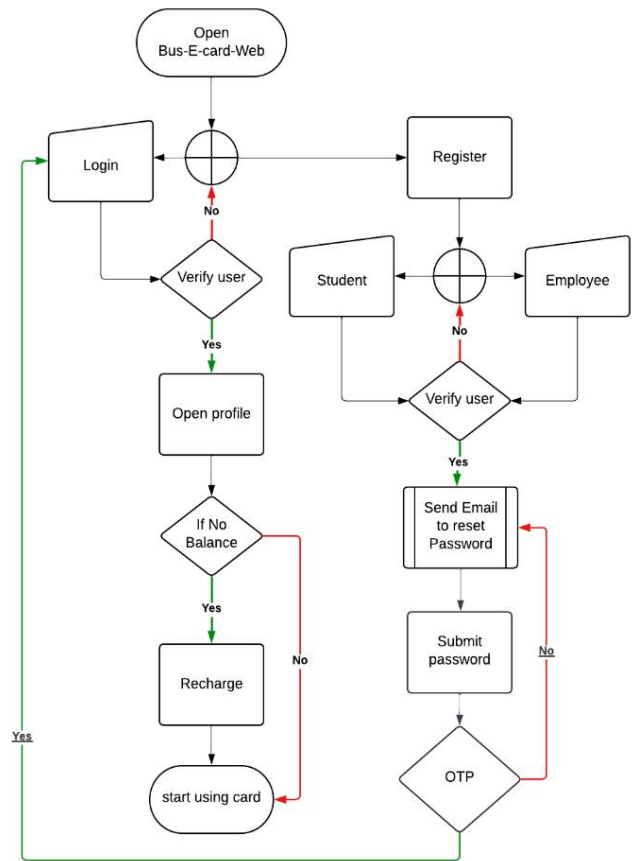
**Ensuring Data Integrity for Subscription Creation:**

Before completing the subscription creation process, it's crucial to verify the integrity of user data. This ensures that critical account details remain unchanged, enhancing security and user trust.

By employing this approach, we enhance data security in our web application by ensuring that users' new passwords are securely stored and protected against unauthorized access or tampering. The utilization of cryptographic hashing with SHA algorithms adds an extra layer of security, contributing to the overall integrity and reliability of our system.

[1.2] To enhance security and avoid sending user login credentials via email, we opted for two-factor authentication. Upon verification by the admin, an email containing a unique OTP-based authentication link is generated and sent to the user's registered email address. This email includes details such as the UID and an option to reset the user's password. After submitting the password, the user is prompted to verify their identity via OTP sent to their registered mobile number.

Using a Python OTP authentication module, a unique OTP is sent to the user's mobile device. If authentication fails, the user can attempt the process again to gain access to their profile and E-card. This two-factor authentication process adds an extra layer of security, ensuring that only authorized users can access their accounts and perform sensitive actions.



1(a) User interface workflow

**2) Internet of things (IoT) Infrastructure**

**2.1) HMACH**

**2.2) Used Equipment**

- 2.2.1) NodeMCU
- 2.2.2) ESP32
- 2.2.3) RFID/NFC Cards
- 2.2.4) LCD 16X2 I2C
- 2.2.5) Buzzer

Within the IoT flow, the Bus-E-Card system relies on a set of specialized equipment to facilitate seamless card verification and transaction processes. This hardware ensemble is carefully selected to ensure robust functionality and reliable performance in various operational environments.

At the heart of the IoT infrastructure are the NodeMCU and ESP32 microcontroller units, which serve as the primary processing units for handling card verification requests and responses. These microcontrollers are chosen for their versatility, low power consumption, and compatibility with a wide range of sensors and communication protocols.

Complementing the microcontrollers are RFID/NFC cards, which serve as the primary means of user identification and authentication. These cards store unique user identifiers and are equipped with radio frequency communication capabilities, allowing them to interact with RFID/NFC readers embedded within the bus payment terminals.

The LCD 16x2 I2C sensor plays a crucial role in providing visual feedback to users during the verification process. Mounted on the payment terminals, the LCD display communicates verification status messages such as "Verified" or prompts for additional actions in case of verification failure or insufficient balance.

To enhance user experience and provide auditory feedback, a buzzer is integrated into the system. The buzzer emits distinct sounds to signify successful verification, errors, or alerts, ensuring users are promptly notified of their transaction status.

Together, these components form a robust IoT infrastructure that seamlessly integrates with the Bus-E-Card system, enabling efficient and secure card verification processes for hassle-free bus travel. Through careful selection and integration of these hardware elements, the system delivers a user-friendly and reliable payment solution that enhances the overall passenger experience. Additionally, Arduino IDE serves as the software environment for programming and configuring the IoT hardware components, ensuring seamless communication and functionality within the system.

Certainly! Below is a flow describing the interaction between the IoT device and the server, including data integrity verification using HMAC:

#### ***IoT Device and Server Interaction Flow***

##### **1. IoT Device Initialization:**

The IoT device (e.g., ESP32) initializes and connects to a local Wi-Fi network using pre-configured credentials. It establishes a connection with the Django server over HTTP.

##### **2. RFID Tag Detection:**

The IoT device waits for an RFID tag to be detected by the RFID reader module (e.g., MFRC522). Once an RFID tag is detected, the device reads the unique identifier (UID) from the tag.

##### **3. Data Preparation:**

The UID read from the RFID tag is converted into a string format. Additional data, such as the bus ID, may be collected or generated by the IoT device.

##### **4. HMAC Signature Calculation:**

The IoT device calculates an HMAC-SHA256 signature using the collected data and a pre-shared secret key. The HMAC signature ensures the integrity and authenticity of the data being sent to the server.

##### **5. HTTP POST Request:**

The IoT device constructs an HTTP POST request containing the RFID tag data and the calculated HMAC signature. It sends the POST request to a specific endpoint on the Django server dedicated to handling IoT device data.

##### **6. Django Server Endpoint:**

The Django server receives the POST request at the designated API endpoint. It extracts the RFID tag data, bus ID, and HMAC signature from the request payload.

##### **7. HMAC Signature Verification:**

The Django server recalculates the HMAC-SHA256 signature using the received RFID tag data and the same pre-shared secret key used by the IoT device. It compares the recalculated HMAC signature with the HMAC signature received in the request. If the signatures match, the server proceeds with processing the data. Otherwise, it rejects the request due to data integrity violation.

##### **8. Data Processing:**

Upon successful HMAC signature verification, the Django server retrieves the student information associated with the received RFID tag data. It updates the student's subscription details, deducting bus fare credits or performing other relevant actions. The server may also update the user's timeline with transaction details.

##### **9. Response to IoT Device:**

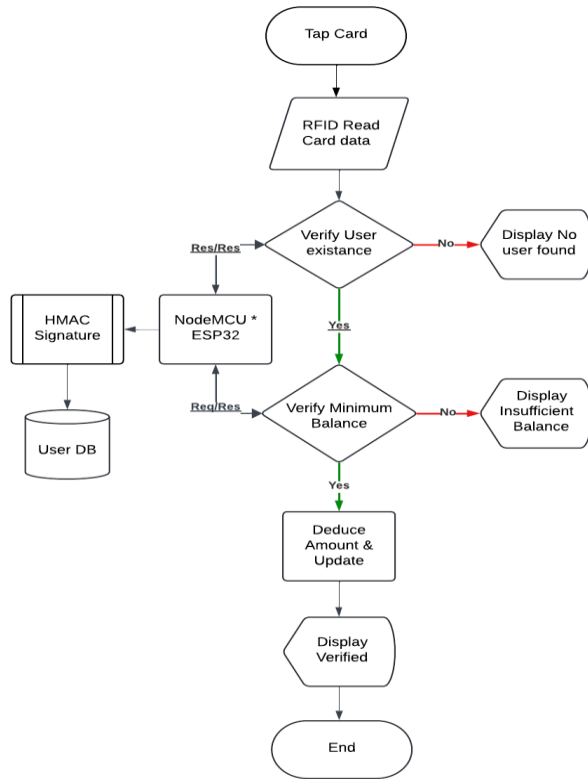
After processing the data, the Django server sends a response back to the IoT device, indicating the success or failure of the transaction. The IoT device can handle the response, accordingly, displaying feedback to the user or performing additional actions.

##### **10. End of Interaction:**

The interaction between the IoT device and the server concludes, ensuring secure and authenticated communication while maintaining data integrity.

This flow outlines the seamless interaction between the IoT device and the server, incorporating HMAC-based data integrity verification to ensure the security and reliability of the communication channel.

#### **2(a) IoT infrastructure Workflow**



minimal features such as user interaction card, recharge option, subscription details, card tracking, balance coins, and a Q&A menu.

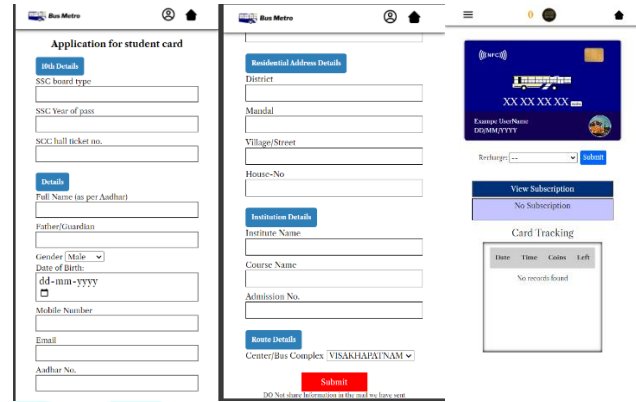


Fig 4 & 5, 6: Registration, Demo Profile

## IV.RESULTS

### 1. Web Interaction

#### A. Bus-e-Card Home

The Bus-e-Card interface begins with a "Get Started" button, leading users to an introduction about the service. Upon clicking the profile icon, users are directed to a login page where they can register as either students or employees. The Bus information is showcased in fig 1, 2 & fig 3.

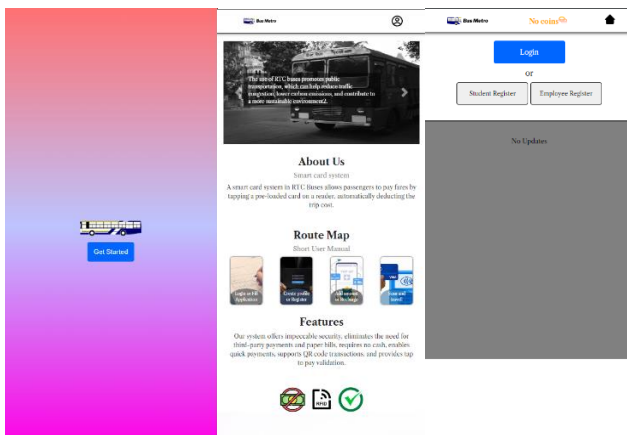


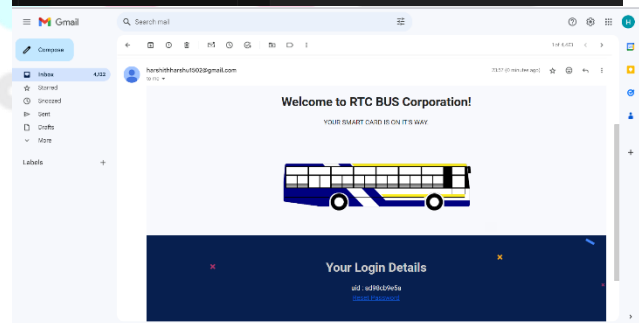
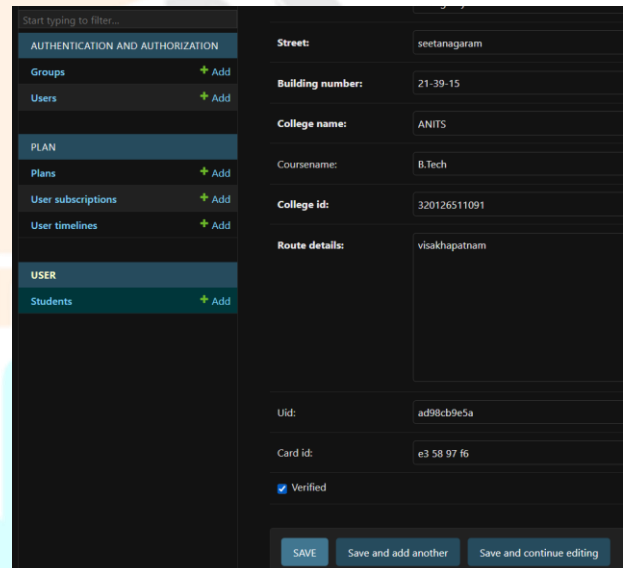
Fig 2: Information about Bus-E-Card & Login Options

#### B. User Registration

New users provide accurate details for registration. Once submitted, users gain access to a demo profile featuring

### C. Admin verification & Email login details

User data undergoes admin verification through the admin. Upon verification, login details are sent to the user via email, including a unique ID and password reset for accessing their profile. [1][1.2] OTP authentication.



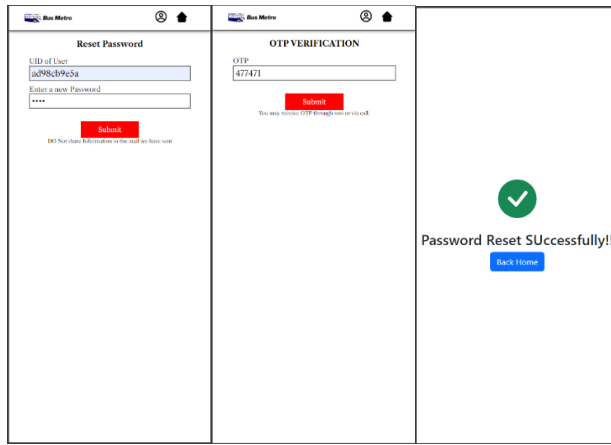


Fig 7, 8: Admin Panel, Login Details Email

**D. Login & profile**

Upon successful login with provided credentials, users gain access to their Bus-e-Card profile, where they can conveniently view essential information such as their image, UID, active/inactive status, username, subscription expiration date, subscription details, and card stacking.

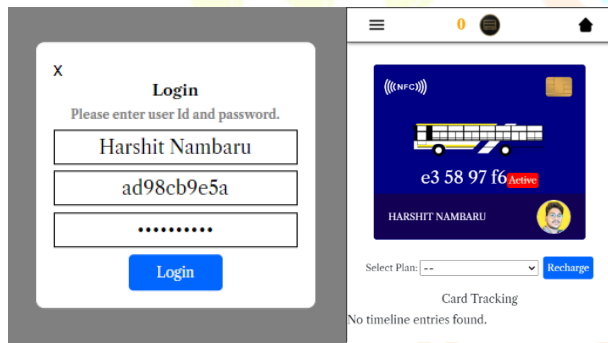


Fig 9, 10: Login panel, User profile

**E. Subscription**

Users can conveniently select a subscription plan from the dropdown menu and proceed to payment using available options such as Razorpay. The integration of Razorpay into our system provides users with a seamless and authentic payment experience, ensuring secure transactions and streamlined subscription activation. Once payment is completed, users' profiles and cards are automatically activated, with subscription details promptly updated to reflect the expiration date & active status.

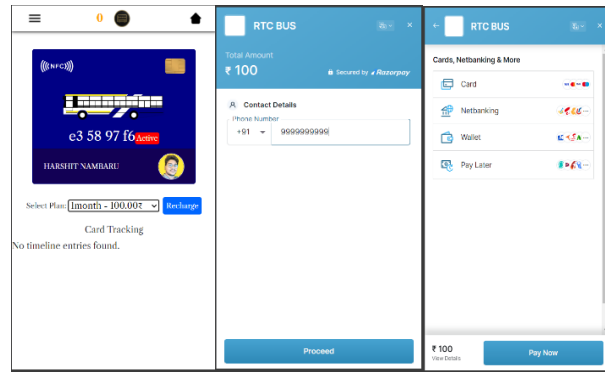


Fig 11, 13: select plan, Initiating Payment

During the implementation phase, users are provided with a convenient mobile number selection payment option, as demonstrated in Fig 13. The payment amount corresponds to the chosen plan, as depicted in Figure 11. To finalize the transaction, users are guided to input a phone number for verification, as indicated in Figure 12. This process seamlessly integrates the Razorpay payment gateway, ensuring smooth and secure transactions for users throughout the payment process.

User must full fill all the pre-requisites as the original payment. After doing all the steps the user card and account will get activated from then he can start using the card.

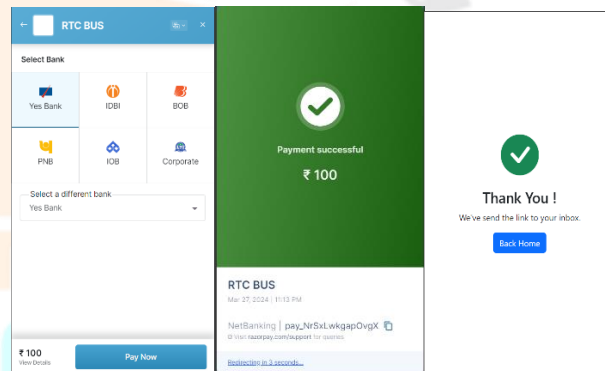


Fig 14, 15: Payment processing

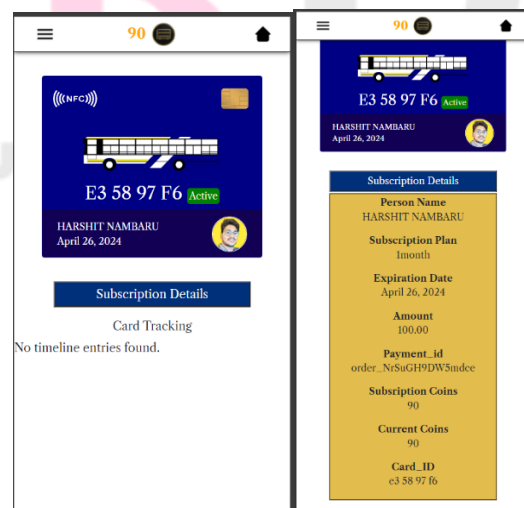


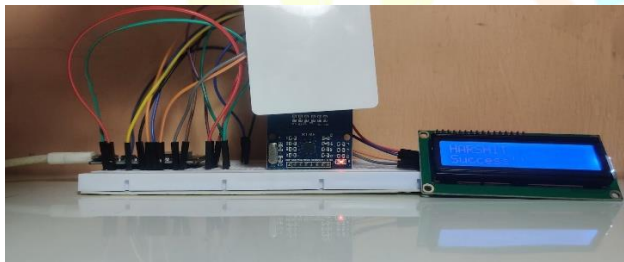
Fig 17, 18: Profile update & Subscription Details

## 2. Internet of Things (IoT) Setup



### A. User Card Authentication & Amount Deduction

After successful recharge, users tap their cards at the sensor for authentication. The NodeMCU \* ESP32 communicates with the database for verification. Upon successful verification, the screen displays user verification status along with the username. If the minimum balance is present, the amount is deducted, and the user profile is updated with the number of coins and card tracking details.



Card Tracking

Date	Time	BusId	Balance
27/03/2024	23:50:10	111V	80

Fig 2, 3, 4: Tap card, Screen displays verification, Table tracks user amount deduction.

### B. Card Decline (No Balance & No User Found)

If verification fails due to insufficient balance or invalid user, the system rejects the user, displaying a message on the screen. The system also detects expired plans and updates the user profile accordingly.

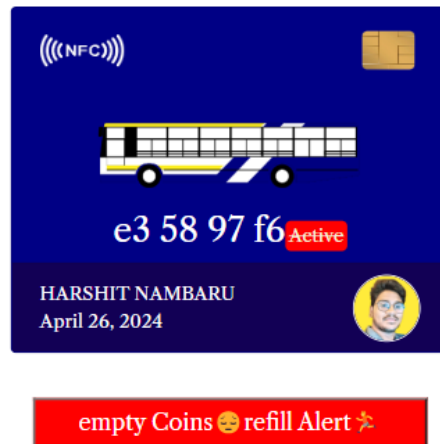
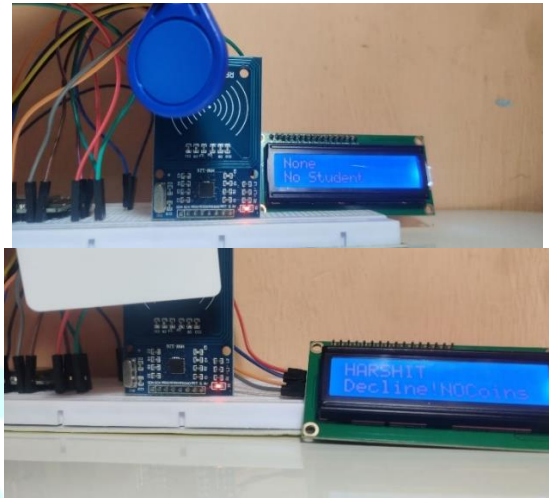


Fig 5, 6, 7: No Student or user found, Card Decline due to low balance, Due to no balance status Inactive & empty coins message refill alert.

## V. CONCLUSION

The Bus-e-Card system offers a convenient and efficient solution for users to manage their travel subscriptions. Through user registration, admin verification, and subscription management, users can easily access and utilize the service, ensuring a seamless travel experience.

Bus-e-Card system not only provides a convenient and efficient solution for managing travel subscriptions but also prioritizes data security through the implementation of cryptographic techniques such as SHA algorithm and HMAC.

The utilization of SHA algorithm ensures data integrity by generating fixed-size hash values from user credentials and critical data. This hash value, unique to the input data, detects even minor changes in the stored information, enhancing the overall security of user accounts and transactional data.



Additionally, the integration of HMAC (Keyed-Hash Message Authentication Code) further strengthens data security by verifying the authenticity and integrity of messages exchanged between system components. By employing a shared secret key, HMAC ensures that both the sender and receiver can validate the origin and integrity of transmitted data, safeguarding against unauthorized access and tampering.

Through the robust implementation of SHA algorithm and HMAC, the Bus-e-Card system guarantees the confidentiality, integrity, and authenticity of user data, fostering trust and confidence among users. This commitment to data security underscores the system's dedication to providing a secure and reliable travel management solution for passengers in today's digital age.

### ACKNOWLEDGMENT

We wish to express our sincere appreciation for the completion of our final project. We are deeply grateful to our supervisor for their invaluable guidance and mentorship throughout this endeavour. Their support has been pivotal in steering us through this process. This project stands as a testament to our collaborative efforts and unwavering commitment to achieving excellence.

### REFERENCES

- [1] Martínez-Ballesté, A., Villalobos, N., Batista, E., López-Aguilar, P., & Solanas, A. (2023). Ticketing Systems for Smart Public Transportation: Tools at the User Side. *Lecture Notes in Electrical Engineering*, 1036, 337-348.
- [2] P. T. Blythe. (2015) Improving public transport ticketing through smart cards. ISSN 0965-0903 | E-ISSN 1751-7699 Volume 157 issues 1, March 2004, pp. 47-45
- [3] Efraim Turban & Joseph Brahm (2000) Smart Card-Based Electronic Card Payment Systems in the Transportation Industry, *Journal of Organizational Computing and Electronic Commerce*, 10:4, 281-293, DOI: 10.1207/S15327744JOCE1004\_06
- [4] Muhammad Wasim Raad, Mohamed Deriche & Tarek Sheltami (2020) An IoT-Based School Bus and Vehicle Tracking system using RFID Technologies and Mobile data Network. Volume 46, pages 3087-3097, (2021)
- [5] Jisha, R., Jyothindranath, A., & Kumary, L. S. (2017). IoT based school bus tracking and arrival time prediction. *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 509–514.
- [6] Badawy, E., Elhakim, A., Abdulhameed, A., & Zualkernan, I. (2016). An IoT Based School Bus Tracking and Monitoring System. *International Conference on Education and New Learning Technologies*, 5537–5546.
- [7] Bin Ibne Reaz, M. (2013). Radio Frequency Identification from Systems to Applications. *IntTechOpen*.

- [8] Pang, Y., Ding, H., Liu, J., Fang, F., & Chen, S. (2018). A UHF RFID-based system for children tracking. *IEEE Internet Things J.*, 5(6), 5055–5064.
- [9] Alsinglawi, B., Elkhodr, M., Nguyen, Q. V., Gunawardana, U., Maeder, A., & Simoff, S. (2017). RFID localisation for Internet of Things smart homes: a survey. *arXiv preprint arXiv:1702.02311*.
- [10] Pedraza, C., Vega, F., & Manana, G. (2018). PCIV, an RFID-based platform for intelligent vehicle monitoring. *IEEE Intell. Transp. Syst. Mag.*, 10(2), 28–35.
- [11] Kumari, M., Kumar, A., & Khan, A. (2020). IoT based intelligent real-time system for bus tracking and monitoring. *International Conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC)*, 226–230.
- [12] Dhanasekar, N., Valavan, C., & Soundarya, S. (2019). IoT based intelligent bus monitoring system. *\*Int. J. Eng. Res. Technol. (IJERT)\**, 7(11), 1–4.
- [13] Luo, X. G., Zhang, H. B., Zhang, Z. L., Yu, Y., & Li, K. (2019). A new framework of intelligent public transportation system based on the Internet of Things. *\*IEEE Access\**, 7, 55290–55304.
- [14] Ahmed, A. (2019). An intelligent and secured tracking system for monitoring school bus. *\*International Conference on Computer Communication and Informatics (ICCCI)\**, 1–5.
- [15] Habadi A. A., & AbuAbdullah, Y. S. (2018). Intelligent safety school buses system using RFID and carbon dioxide detection. *\*1st International Conference on Computer Applications and Information Security (ICCAIS)\**, 1–7.
- [16] Fadzir, T. M. A. M., Mansor, H., Gunawan, T. S., & Janin, Z. (2018). Development of school bus security system based on RFID and GSM Technologies for Klang Valley Area. *\*IEEE 5th international conference on smart instrumentation, measurement and application (ICSIMA)\**, 1–5.
- [17] Kumar, T., Gupta, S., & Kushwaha, D. S. (2017). A smart cost-effective public transportation system: an ingenious location tracking of public transit vehicles. *\*5th International Symposium on Computational and Business Intelligence (ISCBI)\**, 134–138.
- [18] Mizuno, K., & Shimizu, M. (2007). Transportation quality monitor using sensor active RFID. *\*International Symposium on Applications and the Internet Workshops\**, 19–19.
- [19] Danese, G., et al. "An embedded multi-core biometric identification system." *Embedded Hardware Design: Microprocessors and Microsystems* (2011).
- [20] Panagiotou, P., et al. "Cryptographic system for data applications, in the context of internet of things." *Microprocessors and Microsystems* (2019). [DOI: 10.1016/j.micpro.2019.102921]

[21] Sunday D, Aliyu WA (2016) Design of mobile-based travel e-ticketing using QR-code. In: Proceedings of the second annual research conference of Federal University Lafia, Nigeria, p 241

[22] Gupta A, Iram B, Samrit B, Dhage C, Khan N (2018) Online facility of ticket booking and generating bus pass using qr code. Int Res J Eng Technol 5:03–51

[23] Satpalkar T, Salian S, Stephen S, Shaikh S (2016) Smart city parking: a QR code-based approach. Int J Eng Res Technol (IJERT) 5(2):2278–0181

[24] Conde-Lagoa D, Costa-Montenegro E, González-Castaño FJ, Gil-Castiñeira F (2010) Secure eTickets based on QR-codes with user-encrypted content. In: 2010 digest of technical papers international conference on consumer electronics (ICCE), pp 257–258.

