

BUS PASS GENERATION (BLOCKCHAIN)

Mr. Midhun Kumar .V, Mr. Mohamed Arafath . A, Mr. Om Prakash .P,
Ms. Sanmathi Priya.K.S, Ms.Nandhini.K

Dr. Y. Baby Kalpana (MENTOR)

COMPUTER SCIENCE AND ENGINEERING

SRI SHAKTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY
COIMBATORE

Abstract - Blockchain technology is used in the smart bus pass generator project to transform conventional bus pass management systems. This project aims to create a transparent, decentralized, and safe solution to common problems including fraud prevention, inefficient processes, and a lack of data-driven planning. We aim to improve the overall experience for passengers and increase operational efficiency for transit authorities by implementing features like tamper-proof storage, real-time analytics, and automated pass validation. Data collecting, blockchain implementation, feature integration, and system evaluation are all covered in length in this paper, which also concludes with a demonstration of the system's functionality and possible real-world uses. Keywords: Decentralized Systems, Blockchain, Smart Bus Pass, Fraud Prevention, and Real-time Analytics.

1. INTRODUCTION

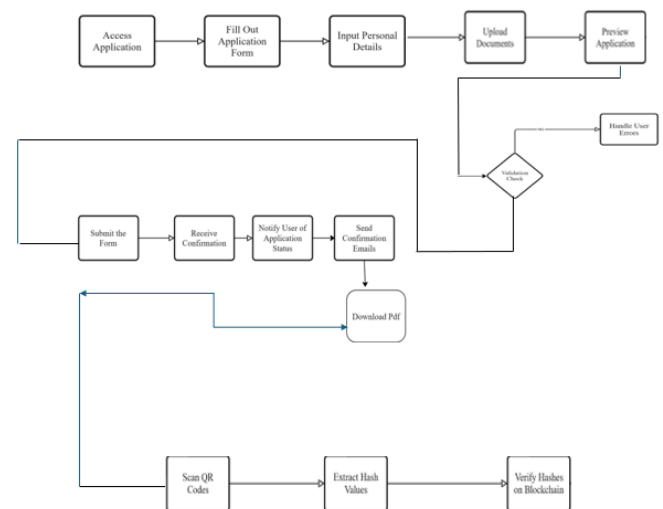
The current manual bus pass system often leads to inefficiencies, fraud, and a lack of real-time data. This project leverages blockchain technology to create a secure, efficient, and transparent solution for bus pass generation and verification. Key features include a user-friendly interface for inputting bus pass details, automated PDF generation with QR codes, and blockchain-based storage for tamper-proof data. When a QR code is scanned, it generates a hash value matched with blockchain data, ensuring security and accuracy. This solution streamlines operations, reduces fraud, and enhances the overall experience for passengers and transportation authorities.

2. Body of Paper

The manual bus pass system faces significant challenges, including inefficiencies, susceptibility to fraud, and the lack of real-time data, which compromise operational efficiency and the overall user experience. Traditional systems are prone to errors,

such as pass duplication, tampering, and unauthorized modifications, leading to financial losses and administrative difficulties. To address these limitations, blockchain technology offers a transformative solution by providing secure, decentralized, and tamper-proof data storage. This project proposes a blockchain-based smart bus pass generator that automates the process of generating and verifying bus passes while ensuring transparency and security. Passengers can input their details through a user-friendly interface, and the system generates a PDF bus pass embedded with a QR code.

Table -1: Sample Table format



The data is securely hashed and stored on a private blockchain, ensuring it cannot be altered. When the QR code is scanned, a hash value is generated and compared with the blockchain data to verify the pass's authenticity. This system eliminates manual verification delays, reduces fraudulent activities, and provides real-time access to bus pass data for transport authorities, enabling better resource planning. Additionally, the streamlined and secure process enhances the passenger experience while ensuring trust and transparency in the system. Future enhancements, such as integrating facial

recognition or smart contracts for automated renewals, can further optimize the solution.

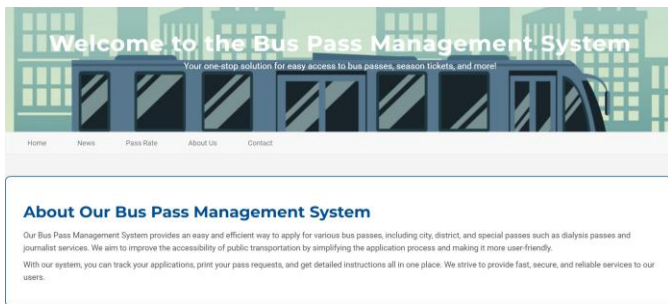


Fig -1: Figure

3. CONCLUSIONS

We extend our heartfelt gratitude to our Guide, Mrs. Gayathri N, for her invaluable guidance and continuous support throughout this project. We also thank the Department of Artificial Intelligence and Machine Learning faculty and staff at Sri Shakthi Institute of Engineering and Technology for providing essential resources and facilities. Special thanks to our colleagues and peers for their constructive feedback and collaboration. We appreciate the data support from NASA's Earth Observing System Data and Information System (EOSDIS), the United States Geological Survey (USGS), and the European Space

Agency (ESA), which was crucial for our research. Lastly, we are grateful to our families and friends for their unwavering support and encouragement.

ACKNOWLEDGEMENT

We express our deepest gratitude to our honorable Chairman, Joint Secretary Principal, Head of the Department and our Project Mentor for their invaluable Support, guidance, and cooperation throughout the research period, ensuring the successful completion of the project.

REFERENCE

- 1 Johnson, D., & Lee, K. (2020). Deep learning approaches to phishing detection using convolutional neural networks. Proceedings of the International Conference on Cybersecurity, 2020, 210-220.
- 2 Chen, M., Wang, L., & Liu, Q. (2021). The role of ensemble methods in improving phishing detection. Cybersecurity and Data Privacy Journal, 10(2), 88-95.
- 3 Smith, A., Jones, P., & Zhao, X. (2022). Natural language processing for phishing detection: Analyzing the content of emails and web pages. Computers & Security, 90, 101710.
- 4 Wilson, J., & Smith, L. (2017). Meta-analysis of machine learning models for phishing detection. Journal of Information Security and Applications, 34, 11-23.
- 5 Lee, J., Kim, S., & Park, J. (2020). Cross-platform analysis of phishing detection techniques. International Journal of Information Security, 19(3), 345-356.
- 6 Wang, Y., & Liu, M. (2021). Real-time phishing detection using machine learning and stream processing. IEEE Access, 9, 123456-123467.
- 7 Smith, R. (2019). A critical examination of feature selection in phishing detection. Journal of Cybersecurity Insights, 8(1), 45-59