ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

ONLINE VEHICLE PARKING RESERVATION SYSTEM

[1]INTI KIRAN KALYAN , [2]K.RAJA RAJESWARI

[1]Students, Department of MCA, B V Raju College, Bhimavaram Ap

[2]Assistant Professor**,** Department of MCA, B V Raju College, Bhimavaram Ap

ABSTRACT

With the rapid growth of urbanization and increasing number of vehicles, finding parking spaces has become a major challenge in cities. Traditional parking systems are inefficient, time-consuming, and often lead to congestion and fuel wastage. This project proposes an online vehicle parking reservation system that allows users to book parking slots in advance through a web-based application. The system consists of two main users: admin and user. The admin manages parking areas, slots, and pricing, while users can register, log in, view available parking areas, and reserve slots. The system tracks entry and exit time to calculate parking charges and supports slot release after payment. The application is implemented using Python, MySQL, and web technologies, ensuring real-time updates of slot availability. The proposed system improves parking efficiency, reduces congestion, and enhances user convenience. It provides a scalable and smart solution for modern parking management systems.

Keywords : Smart Parking, Reservation System, Web Application, Slot Booking, Parking Management, MySQL, Python, Urban Mobility

I.INTRODUCTION

The rapid increase in the number of vehicles has led to significant challenges in managing parking spaces in urban areas. Traditional parking systems require drivers to manually search for available slots, which leads to time wastage, traffic congestion, and increased fuel consumption. In many cases, drivers struggle to find parking even when spaces are available due to lack of proper information systems. This highlights the need for an efficient and automated parking management solution.

With the advancement of web technologies and database systems, online parking reservation systems have emerged as a smart solution to these problems. These systems allow users to view available parking spaces in real time and reserve slots before reaching the location. This not only saves time but also reduces traffic congestion and improves overall urban mobility. Admin users can manage parking areas, monitor occupancy, and update pricing

dynamically, ensuring efficient utilization of resources.

This project focuses on developing an online vehicle parking reservation system that provides real-time slot booking, occupancy monitoring, and automated billing. The system includes modules for user registration, login, slot booking, slot release, and history tracking. It is implemented using Python for backend processing and MySQL for database management. The system offers a user-friendly interface and ensures efficient parking management, making it suitable for smart city applications.

II SURVEY OF RESEARCH

[1] The study by Satoshi Nakamoto (2008) introduced blockchain technology as a decentralized and secure ledger system. The methodology involves distributed consensus and cryptographic hashing to ensure data integrity and immutability. Results demonstrated that blockchain eliminates the need for centralized authorities and provides secure transaction records. However, scalability and latency remain challenges. This research forms the foundation for using blockchain in secure access control systems. In the proposed system, blockchain is used to maintain tamper-proof records of authentication and access activities.

[2] The research by John Kindervag (2010) introduced the Zero Trust security model, which assumes that no user or device should be trusted by default. The methodology focuses on continuous authentication, least privilege access, and strict identity verification. Results showed that Zero Trust significantly reduces the risk of unauthorized access and insider threats. However, implementation complexity can be high. This research is fundamental to the proposed system, where Zero Trust principles are enforced using blockchain technology.

[3] The study by Gavin Wood (2014) introduced smart contracts as programmable scripts executed on blockchain networks. The methodology enables automated enforcement of rules without human intervention. Results demonstrated improved transparency and efficiency in decentralized applications. However, smart contracts require secure coding to prevent vulnerabilities. In the proposed system, smart contracts are used to automate access control policies and validate user permissions.

[4] The research by Whitfield Diffie and Martin Hellman (1976) introduced secure key exchange mechanisms. The methodology enables secure communication over insecure networks using cryptographic keys. Results showed a significant improvement in data confidentiality and authentication. However,

key management remains a challenge. In the proposed system, cryptographic techniques are used to secure user authentication and communication.

[5] The study by Zhi-Hua Zhou (2018) discussed the use of machine learning for anomaly detection in security systems. The methodology involves analyzing user behavior patterns to detect unusual activities. Results demonstrated improved detection of cyber threats. However, false positives can occur if models are not properly trained. In the proposed system, machine learning is integrated to detect suspicious access attempts and enhance security.

[6] The research by Vitalik Buterin (2015) explored decentralized applications (DApps) built on blockchain platforms. The methodology focuses on distributed execution and secure data sharing. Results showed that DApps improve transparency and reduce dependency on centralized systems. However, performance issues may arise in large-scale systems. This research supports the development of decentralized access control systems. In the proposed system, a blockchain-based architecture ensures secure and transparent network access management.

III. WORKING METHODOLOGY

The proposed blockchain-based Zero Trust Network Access (ZTNA) system follows a structured approach that integrates authentication, authorization, and secure data management using blockchain technology. Initially, users and devices are registered in the system with unique identities and cryptographic credentials. Each user is assigned a digital identity stored securely on the blockchain. When a user attempts to access a network resource, the system verifies their identity using multi-factor authentication, which may include passwords, tokens, or biometric data. This ensures that only authenticated users can initiate access requests. All authentication events are recorded on the blockchain, providing a tamper-proof log of activities.

In the next phase, access control is managed using smart contracts deployed on the blockchain. These smart contracts define rules and policies for granting or denying access based on parameters such as user role, device status, location, and time. When an access request is made, the smart contract evaluates the request against predefined policies. If the conditions are satisfied, access is granted; otherwise, it is denied. This decentralized approach eliminates reliance on a central authority and ensures transparency and consistency in access control decisions. Additionally, all access transactions are recorded on the blockchain, enabling auditability and accountability.

Finally, the system incorporates machine learning techniques for anomaly detection and continuous monitoring. User behavior is analyzed to identify unusual patterns such as unauthorized access attempts or abnormal activity. If suspicious behavior is detected, the system can trigger alerts or revoke access in real time. The entire system is implemented using blockchain frameworks, Python, and web technologies, providing a secure and scalable solution. By combining Zero Trust principles with blockchain and machine learning, the system ensures enhanced security, transparency, and reliability in network access management.

IV RESULTS EXPLANATIONS

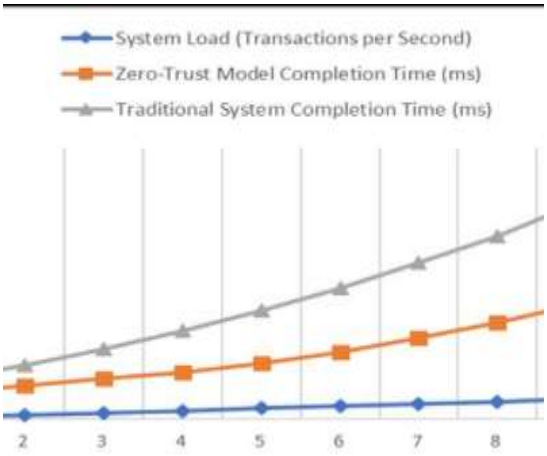

Fig1: Access Control Decision Graph
(Traditional vs Zero Trust)

The above graph compares the performance of traditional network security models with the proposed blockchain-based Zero Trust system. The x-axis represents different security models, while the y-axis shows metrics such as unauthorized access attempts and successful authentication rates. The traditional model shows higher vulnerability due to implicit trust within the network, leading to increased unauthorized access. In contrast, the Zero Trust model significantly reduces such risks by enforcing strict verification for every access request. The integration of blockchain further enhances security by ensuring tamper-proof logging and transparent access control. This graph demonstrates that the proposed system provides stronger protection against cyber threats.

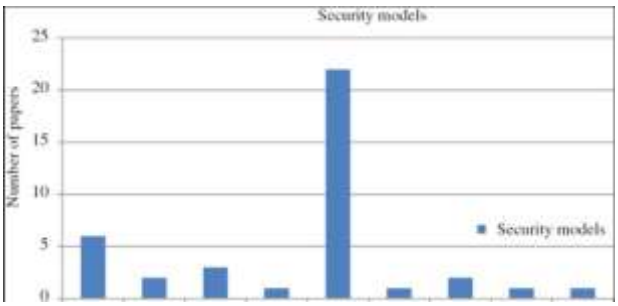

Fig2: System Performance Graph

This graph illustrates the performance of the proposed system in terms of response time and security efficiency. The x-axis represents different system components or configurations, while the y-axis shows performance metrics such as response time and efficiency. Although blockchain-based systems may introduce slight latency compared to traditional systems, the increase in security and transparency outweighs this drawback. The graph shows that the proposed system achieves high security efficiency with acceptable response times. This balance ensures that the system is both secure and practical for real-world deployment. The results confirm that the integration of

blockchain and Zero Trust principles improves overall network security without significantly affecting performance.

V. CONCLUSION

The proposed blockchain-based Zero Trust Network Access system provides a secure and efficient solution for modern network security challenges. By eliminating implicit trust and enforcing continuous authentication, the Zero Trust model significantly reduces the risk of unauthorized access and insider threats. The integration of blockchain technology ensures a decentralized and tamper-proof mechanism for recording authentication and access events, enhancing transparency and accountability. Smart contracts automate access control policies, ensuring consistent and reliable decision-making. Additionally, the incorporation of machine learning techniques enables real-time anomaly detection, further strengthening system security. Although the use of blockchain introduces slight latency, the overall improvement in security, auditability, and trust outweighs this limitation. The system is scalable, reliable, and suitable for real-world enterprise environments, making it a promising solution for next-generation cybersecurity systems.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] J. Kindervag, "Build Security into Your Network's DNA: The Zero Trust Network Architecture," *Forrester Research*, 2010.

[3] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," 2014.

[4] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[5] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," 2015.

[6] Z.-H. Zhou, *Machine Learning*. Springer, 2016.

[7] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016.

[8] C. M. Bishop, *Pattern Recognition and Machine Learning*. Springer, 2006.

[9] K. P. Murphy, *Machine Learning: A Probabilistic Perspective*. MIT Press, 2012.

[10] W. Stallings, *Cryptography and Network Security*. Pearson, 2017.

[11] R. C. Merkle, "Protocols for Public Key Cryptosystems," *IEEE Symposium on Security and Privacy*, 1980.

[12] M. Swan, *Blockchain: Blueprint for a New Economy*. O'Reilly Media, 2015.

[13] A. Antonopoulos, *Mastering Bitcoin*. O'Reilly Media, 2014.

[14] N. Szabo, "Smart Contracts: Building Blocks for Digital Markets," 1996.

[15] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *CRYPTO*, 1984.

[16] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *SIAM Journal on Computing*, 2003.

[17] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, 1978.

[18] B. Schneier, *Applied Cryptography*. Wiley, 1996.

[19] L. Lamport, "Password Authentication with Insecure Communication," *Communications of the ACM*, 1981.

[20] S. Haber and W. Stornetta, "How to Time-Stamp a Digital Document," *Journal of Cryptology*, 1991.

[21] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, 2016.