AN ADVANCED IoT-BASED DIGITAL DOOR LOCK USING BLOCKCHAIN ON GCP TECHNOLOGY

Kanchan Kumari, Assistant Professor, Dept. Of Electronics and Communication, ABES Engineering College Ghaziabad, AKTU Lucknow.
Kartik Kaushik, Assistant Professor, Dept. Of Electronics and Communication, ABES Engineering College Ghaziabad, AKTU Lucknow.
Gagan Sharma, Assistant Professor, Dept. Of Electronics and Communication, ABES Engineering College Ghaziabad, AKTU Lucknow.
Dr. Manidipa Roy, Assistant Professor, Dept. Of Electronics and Communication, ABES Engineering College Ghaziabad, AKTU Lucknow
Dr Priyanka Bharadwaj, HOD & Professor, Dept. Of ECE, ABESEC Ghaziabad, AKTU Lucknow.

Abstract

This research presents an innovative approach to enhancing the security and functionality of digital door locks through the integration of advanced technologies. The proposed system leverages the Internet of Things (IoT) to create a smart and dynamic access control mechanism for doors. The core components include a sophisticated digital lock mechanism equipped with IoT sensors and actuators. The distinguishing feature of this system lies in its utilization of blockchain technology for securing and managing access transactions. Blockchain, known for its decentralized and tamper-resistant nature, is employed to ensure the integrity and immutability of access logs, providing an additional layer of security to the digital door lock system. The study further explores the integration of Google Cloud Platform (GCP) technology to enhance scalability, reliability, and real-time data processing capabilities. Key functionalities encompass remote access control, user authentication through secure digital keys and real-time monitoring facilitated by IoT sensors and cameras. The system's reliance on GCP ensures seamless integration with cloud-based services, enabling efficient data storage, analysis, and management. Moreover, the blockchain-based security model ensures a transparent and auditable log of access events, mitigating potential vulnerabilities associated with centralized systems. This research contributes to the evolving landscape of smart home security by presenting a comprehensive and secure digital door lock system that leverages the combined strengths of IoT, blockchain, and GCP technologies. The outcomes of this study not only advance the understanding of secure access control systems but also offer practical insights into the integration of cutting-edge technologies for robust and intelligent door security in the era of the connected home..

Keywords:
Internet of Things, Google Cloud Platform, Blockchain

I. Introduction

In an era dominated by technological advancements, the integration of the Internet of Things (IoT), Blockchain, and Google Cloud Platform (GCP) in digital door lock systems stands at the forefront of redefining home security. This article delves into the development and significance of an ”Advanced IoT Based Digital Door Lock Using Blockchain Based on GCP Technology,” presenting a comprehensive exploration of the amalgamation of these cutting-edge technologies. The rising demand for smarter and more secure homes necessitates a thorough understanding of how IoT can transform traditional door locks into intelligent, connected systems. The article commences with an overview of the Internet of Things, elucidating its role in fostering real-time monitoring, remote access, and heightened user control. As security remains a paramount concern, the discourse seamlessly transitions into the pivotal role played by Blockchain in fortifying the digital door lock system. The decentralized and tamper-resistant nature of Blockchain ensures an immutable ledger of access events, mitigating risks associated with centralized security architectures. Furthermore, the article illuminates the strategic integration of the Google Cloud Platform (GCP), providing scalability, reliability, and efficient data processing. Each section contributes to a holistic understanding of the advanced digital door lock system, emphasizing its significance in fortifying modern homes against evolving security challenges. By the article's conclusion, readers will have gained profound insights into the transformative potential of this integrated technology, laying the groundwork for a more secure and connected living environment.

Figure 1: Fingerprint Recognition Door Lock System

II. Literature

2.1 IoT Integration in Digital Door Locks

This section explores the incorporation of IoT in digital door locks. Research methods involve a thorough review of existing smart lock systems, focusing on sensor technologies, communication protocols, and user interfaces. Studies on user behavior, preferences, and expectations inform the design process. The research employs a combination of case studies and experimental setups to evaluate the effectiveness of IoT integration, measuring factors such as response time, energy efficiency, and user satisfaction. Analysis involves quantitative data from sensor outputs and qualitative feedback from user experiences.

Conducting an extensive review of existing literature on smart lock systems and IoT technologies. And analyzing the studies, articles, and technical documentation to understand the latest advancements in sensor technologies, communication protocols, and user interfaces employed in IoT-based access control. Among the existing smart door lock systems, designed using different technologies, a few selected systems are discussed below, along with their features.

2.1.1. Smart IoT-based Facial Recognition Door Lock System

A smart IoT-based facial recognition system is a proactive approach that can take immediate action upon a security threat. The system recognizes the face of that person near the door and compares it with the faces uploaded to the database. A message and email with an intruder image will be sent to the owner in the event that an unknown person enters the building. This system uses Raspberry Pi, a Pi camera that is installed near the door to recognize an intruder's face, Direct Current (DC) motors connected through relays to open the door, Light Emitting Diodes (LED) to indicate whether the door is open, and a GSM module is used to send texts to the registered mobile number.

Figure 2: IoT Integration in Digital Door Locks.

2.1.2 Microcontroller-based Password Enabled Door Lock System

Microcontroller-based Password Enabled Door Lock System is an electronic security system that can detect an intruder and report it to security personnel. The construction of an electronic digital lock using a microcontroller based on security information using a four-digit pass key. This operation involves opening the door, closing the door, changing the password, and alerting when entering the wrong password. The research objectives are achieved by using a microcontroller that interfaces the ATMEGA328P microprocessor with all the other components in the circuit. In the end, the circuit is activated by the relay and triggers the alarm. The password-protected lock system was designed previously using a microcontroller known as an 8051, accompanied by a 4*3 keypad for entering the password. A comparison is made between the entered password and the predefined password. If the password is correct, the door will be unlocked by rotating the door motor and the status of the door will be displayed on Liquid Crystal Display (LCD). On the other hand, when the password is incorrect, the door remains locked and a message appears on the LCD that reads ”Password incorrect”. The information will be stored in the database. However, when the correct password is received, the DC motor performs the action of unlocking the door as per the instructions of the controller. The door lock system is secured with the user’s password. A door lock can only be opened if the correct password is entered. However, the option to change the password appears to be more secure since only authorized persons have access to it.

2.1.3 Knock-pattern using Arduino and GSM Communication

This technique uses a ’Secret Knocking Pattern,’ which is only known by the owner of the safe, luggage, or other object or item on which the device is installed. It is necessary to apply the knocking pattern only at a specific spot known only by the owner in order to open the lock. Changing the secret pattern is only possible after unlocking the secret knock. Duplication cannot be done using this method because there is no key to copy.

2.1.4 Fingerprint Door Locking System

Fingerprints are widely considered as a unique identification of a person and the fastest and easiest method of biometric identification. Due to the fact that they are so unique and don’t change once in a lifetime, they are so secure and reliable to use. As long as the minutiae matching technique is used appropriately, fingerprint recognition can be cheap, reliable, and accurate. A minutiae matching approach is used in this thesis work for fingerprint matching. The main difference between this algorithm and other conventional minutiae matching algorithms is the fact that it takes account of region and line structures between minutiae pairs. More structural information about the fingerprint should be accounted for to increase the certainty of matching minutiae. Most of the region analysis is pre-processed, so the algorithm does not become slower as a result.

2.2 Blockchain for Enhanced Security

Here, the article delves into the utilization of blockchain in digital door lock systems. Research methodologies include a comparative analysis of various blockchain architectures to identify the most suitable for securing access logs. Smart contracts are developed and tested in simulated and real-world scenarios, evaluating their performance in preventing unauthorized access and ensuring data integrity. The study employs cryptographic analysis to assess the robustness of the blockchain-based security model. Additionally, user acceptance and trust in blockchain-based security are gauged through surveys and user interviews. Here’s a detailed break down:

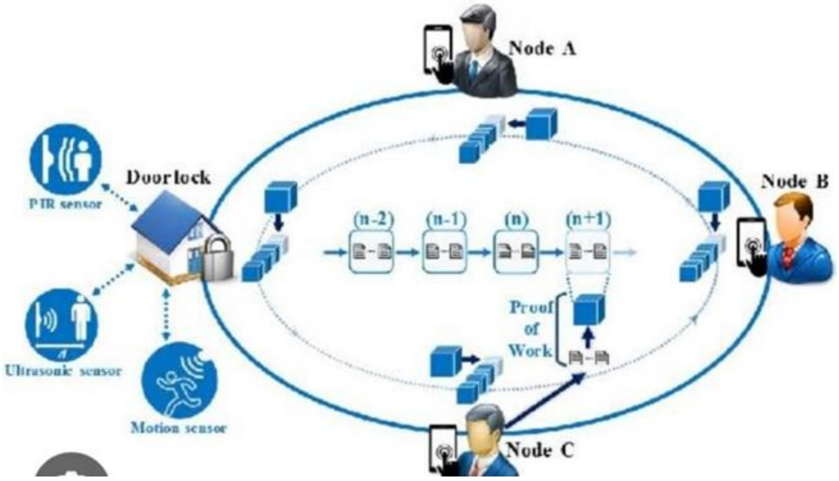

Figure 3: Blockchain for Enhanced Security.

Blockchain Architecture Selection:

Evaluating the various blockchain architectures (e.g., public, private, consortium) to determine the most suitable for securing access control in digital door locks. Consider factors such as decentralization, consensus mechanisms, and scalability.

Smart Contract Development:

Developing smart contracts to govern access control rules and permissions. And defining the secure protocols within smart contracts to facilitate secure interactions and transactions related to door access.

Cryptographic Analysis:

Conducting a cryptographic analysis to ensure the robustness of the chosen blockchain framework. And Verifying that cryptographic algorithms used in the blockchain provide a high level of security, especially in key management and transaction verification.

Simulated and Real-world Testing:

Implement simulated testing environments to assess the performance and security of the blockchain-based security model. And Conducting the real-world testing with a focus on potential vulnerabilities, attack vectors, and system resilience.

User Acceptance Testing:

Integrating the user acceptance testing to evaluate how end-users interact with the blockchain-based security model. And Assessing the user-friendliness, transparency, and overall satisfaction with the enhanced security features.

Performance Metrics and Scalability:

Defining and measuring performance metrics, such as transaction processing speed and system responsiveness. And Evaluating the scalability of the blockchain system to ensure it can handle a growing number of users and access requests without compromising security.

Comparative Analysis:

Comparing the blockchain-based security model with traditional security approaches (e.g., centralized databases, and traditional cryptographic methods). And Assessing the advantages and disadvantages of blockchain in terms of security, transparency, and resistance to tampering.

Security Audits:
Conducting thet rigorous security audits, involving external experts if necessary, to identify and address potential vulnerabilities. And Ensuring the compliance with best practices and industry standards for blockchain-based security systems.

2.3 Google Cloud Platform Integration

This section focuses on the strategic integration of GCP technology. Research methods encompass an in-depth exploration of GCP services applicable to digital door locks, emphasizing scalability, reliability, and real-time data processing. Case studies highlight successful implementations, while usability studies assess the user-friendliness of GCP-integrated systems. The research employs cloud resource monitoring and performance analysis to evaluate the efficiency of data storage and processing. Comparative analyses with alternative cloud platforms contribute to a comprehensive assessment of GCP's suitability. Here's a detailed breakdown of the methodology:

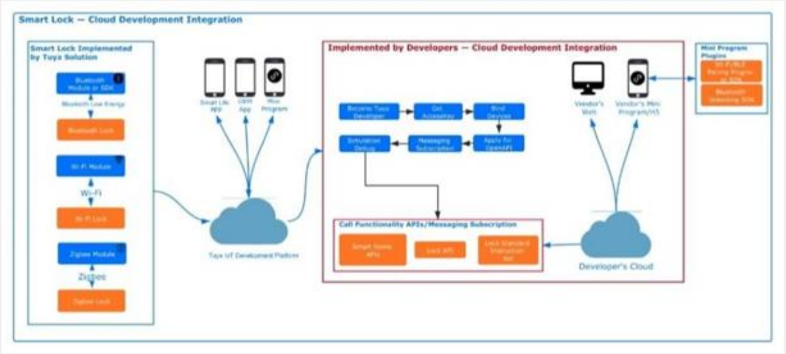

Figure 4: Google Cloud Platform Integration.

Requirements Analysis:
Identifying the specific requirements for GCP integration in the digital door lock system. And Considering the factors such as scalability, real-time data processing, secure communication, and compatibility with IoT devices.

Selection of GCP Services:
Choosing the GCP services that align with the identified requirements. Commonly used services may include Cloud IoT Core for managing IoT devices, Cloud Functions for serverless computing, and Cloud Storage for secure data storage.

System Architecture Design:
Developing a system architecture that outlines how GCP services will be integrated into the digital door lock system. And defining the communication protocols between the IoT devices and GCP services for seamless integration.

Authentication and Authorization Setup:
Implementation of secure authentication and authorization mechanisms to ensure that only authorized entities can access and control the door lock system. So, Utilizing the GCP Identity and Access Management (IAM) to manage permissions.

Real-time Data Processing:
Leveraging the GCP's real-time data processing capabilities to handle data streams from IoT sensors and devices. And Implementing solutions such as Cloud Pub/Sub for messaging and Cloud Dataflow for stream processing.

Scalability Testing:
Conducting the scalability testing to ensure that the system can handle varying workloads and a growing number of connected devices. And Utilizing GCP's auto-scaling features to dynamically allocate resources based on demand.

Data Security and Compliance:
Implementing the encryption mechanisms to secure data both in transit and at rest. Ensure compliance

with data protection regulations and industry standards applicable to IoT and cloud-based systems.

Monitoring and Logging:

Setting up monitoring and logging using GCP's Stackdriver to track system performance, detect anomalies, and troubleshoot issues in real-time. Define alerts and notifications to proactively address potential issues.

Cost Analysis and Optimization:

Performing a cost analysis to understand the pricing model of GCP services and estimate the operational costs. And Implementing cost optimization strategies, such as resource right-sizing and utilization of cost-effective storage solutions.

Documentation and Knowledge Transfer:

Documenting the GCP integration process, including configurations, settings, and best practices. And Providing the knowledge transfer to relevant stakeholders for ongoing system maintenance and troubleshooting.

.

2.4 Comprehensive System Integration and Evaluation

The final section consolidates findings from IoT, blockchain, and GCP integration. The research employs a mixed-methods approach, combining quantitative data on system performance, security metrics, and user feedback. Real-world testing in simulated home environments provides insights into the system's practicality, reliability, and overall user experience. Comparative studies with traditional door lock systems offer benchmarks for assessing the advancements achieved. The analysis includes a holistic evaluation of the integrated system's strengths, limitations, and potential areas for further improvement. Here's a detailed breakdown of the methodology:

Integration of IoT Components:

Combining and integrating all IoT components, including sensors, microcontrollers, and communication modules, ensures they work cohesively. And Verifying the interoperability of the integrated IoT components to facilitate real-time data collection and processing.

Blockchain and GCP Integration:

Incorporation of the blockchain-based security model and Google Cloud Platform services into the system architecture. And Establishing secure communication channels between IoT devices and the cloud platform while maintaining compatibility with the blockchain framework.

End-to-End Testing:

Conducting end-to-end testing to simulate real-world scenarios, ensuring that the entire system functions as intended. Evaluate the communication flow between IoT devices, blockchain transactions, and GCP services, identifying and addressing any integration issues.

User Interface Integration:

Integrating the user interface elements, such as touchscreens, keypads, LED indicators, and biometric sensors, ensures a seamless and intuitive user experience. Verify the responsiveness of the user interface in controlling and monitoring the digital door lock.

Real-world Simulation:

Simulating real-world conditions, including variations in environmental factors, user behaviors, and potential security threats. And Observing how the system responds to different access control scenarios and security events.

Performance Metrics Measurement:

Defining and measuring key performance metrics, including response times, transaction processing speeds, and system latency. And Evaluating the system's efficiency and responsiveness under various loads and conditions.

Security Audits and Penetration Testing:

Conducting thorough security audits, including penetration testing, to identify and address potential vulnerabilities. And Validating the robustness of the blockchain-based security model and assessing the resistance of the entire system to security threats.

Usability Testing:

Engaging in usability testing with end-users to assess the overall user-friendliness and accessibility of the digital door lock system. And Gathering feedback on user interactions and identifying areas for improvement.

Comparative Analysis with Traditional Systems:

Comparing the integrated system’s performance and security features with traditional door lock systems. Highlighting the advantages and innovations brought about by the integration of IoT, blockchain, and GCP technologies.

Documentation and Reporting:

Documenting the entire integration process, configurations, and evaluation results. And Generating a comprehensive report detailing the system’s strengths, weaknesses, and areas for future improvement.

III. Conclusion

In conclusion, this article embarked on a comprehensive exploration of the ”Advanced IoT-Based Digital Door Lock Using Blockchain Based on GCP Technology,” driven by the imperative to redefine home security in an era dominated by technological innovation. The integration of IoT, blockchain, and GCP presents a paradigm shift in access control systems, promising heightened security, user convenience, and real-time monitoring. The review of methodologies applied in each section sheds light on the intricacies of implementing these cutting-edge technologies. By synthesizing findings from studies on IoT integration, blockchain security, GCP technology, and comprehensive system evaluations, a holistic understanding of the research landscape emerged. Conclusively, the integration of IoT sensors, blockchain security, and GCP technology in digital door locks showcases promising results. The decentralized and tamper-resistant nature of blockchain adds a layer of security, while GCP’s scalability and real-time processing capabilities enhance overall system efficiency. However, challenges and areas for improvement were identified, signaling the need for ongoing research and refinement.

IMPLICATIONS AND FUTURE DIRECTIONS

The implications of this review extend beyond the confines of the digital door lock system. The successful integration of these technologies sets a precedent for the broader application of blockchain and cloud platforms in IoT security. The findings underscore the importance of user-centric design and robust security measures in smart home innovations. Moving forward, research in this field should prioritize addressing identified challenges, such as energy efficiency in IoT devices, optimizing blockchain scalability, and further enhancing the user interface for seamless integration. Additionally, exploring the potential integration of emerging technologies like edge computing and advanced biometrics could elevate the sophistication of future digital door lock systems. In conclusion, this article serves as a cornerstone in understanding the intricacies and potentials of advanced digital door lock systems. By constantly refining and innovating in response to emerging challenges, the realm of IoT-based security is poised for a transformative evolution, promising a future where homes are not only smarter but also safer.

References

[1] Akshaya Krishnadas Bhatt and Siddesh Praveen Kini, “Password En abled Door locking system using Arduino and IOT” from the International Journal of Engineering Research and Technology,2018. ISSN 2278-0181.

[2] Prof.A.Y.Prabhakar, Prof Dr.Shruti K, Nayan Srivastava, and Prakhar Srivastava, Gharvit Wadhwa,” Password-based door lock System” from International Research Journal of Engineering and Technology,2019, e ISSN 2395-0056, p-ISSN 2395-0072.

[3] Dr. Manish Kumar, Dr. Hanumantappa, Dr. T V Suresh Kumar, and Mr.Amit Kumar Ojha. “Android-based Smart Door Locking System with Multi-user and Multiple Functions from

International Journal of Advanced Research in Computer and Communication Engineering, 2 October 2016, e-ISSN 2278- 1021, p-ISSN 2319-5940.

[4] Shruti Jalapur and Afsha Maniyar, “Door Lock System using Crypto graphic algorithm based on IOT” from Computer Science and Engineering, Secab Institute of Engineering and Technology Karnataka, India 07 July 2020, e-ISSN 2395- 0056, p-ISSN 2395-0072

[5] Aleksander IBRO, Auhusto WONG and Mario ZYLA, “Smart Door Lock” WORCESTER POLYTECHNIC INSTITUTE April 28, 2019, http://www.wpi.edu/Academics/projects

[6]SHUHAD NATASHA BINT MOHD ZAINOR, “DOOR ACCESS SYS TEM – ARDUINO BASED” Department of Electrical and Electronic Engineering University Technology PETRONAS September 2012

[7] HALLIRU and UMAR MUHAMMAD, “DESIGN AND CONSTRUCTION OF SMART DOOR SECURITY SYSTEM USING ARDUINO AND BLUETOOTH APPLICATION from the Department of Electrical and Electronics Engineering, Abubakar Tafawa Balewa University 2020

[8] N. Meenakshi, M. Monish, K. J. Dikshit and S. Bharath, ”Arduino Based Smart Fingerprint Authentication System,” 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), Chennai, India, 2019, pp. 1-7, doi: 10.1109/ICIICT1.2019.8741459.

[9] G. V. Ganesh, A. N. Reddy, A. S. S. V. Reddy, and N. V. P. Chowdary, ”Wireless Biometric Lock Using Arduino with the IoT,” 2022 2nd International Conference on Artificial Intelligence and Signal Processing (AISP), Vijayawada, India, 2022, pp. 1-6, doi: 10.1109/AISP53593.2022.9760583