International Journal of Innovative Research in Engineering
Volume 5, Issue1 (January-February 2024), PP: 13-15.
https://www.doi.org/10.59256/ijire.20240501003
www.theijire.com
ISSN No: 2582-8746

BLYNK RFID and Retinal Lock Access System

Yoheswari.S[1], Adhithyaram.L[2], Gokulesh.S[3], Harish Raj .K.B[4], Jivithesh Harshaa .R.D[5]
[1]Assistant Professor Department of Computer Science and Engineering, K.L.N. College of Engineering, Sivagangai, Tamilnadu, India
[2,3,4,5] Student, Department of Computer Science and Engineering, K.L.N. College of Engineering, Sivagangai, Tamilnadu, India

How to cite this paper:
YOHESWARI.S[1], ADHITHYARAM.L[2], GOKULESH.S[3], HARISH RAJ .K.B[4], JIVITHESH HARSHAA .R.D[5] "BLYNK RFID and Retinal Lock Access System", IJIRE-V5I01-13-15.

Abstract: *The BLYNK RFID AND RETINAL LOCKACCESS SYSTEM describes a digital door lock system that uses an ESP32-CAM module, which is a budget friendly development board with a very small size camera and a micro-SD card slot. The system uses retinal recognition technology to detect the retinal of the person who wants to access the door. The AI-Thinker ESP32-CAM module takes pictures of the person and sends them to the owner via the BLYNK application installed on their mobile phone. The owner can then grant permission to access the door based on the person's identity. When deploying your BLYNK RFID and retinal scanner project, it's important to consider scalability and maintenance. As your user base and access requirements may change over time, plan for future expansion and updates. Regularly review and update your system's firmware, libraries, and security measures to stay ahead of potential vulnerabilities and evolving best practices in access control. Monitoring and auditing your system's usage is crucial. The Blynk platform can help you gather data on access attempts and system performance, allowing you to analyze the data for any anomalies and potential security breaches. This data can be valuable for compliance, troubleshooting, and performance optimization.*

Key Word: *retinal and RFID scanning for lock to authentic users, using an ESP32-CAM and RFID reader controlling through BLYNK.*

I.INTRODUCTION

The Internet of Things (IoT) represents a revolutionary paradigm in there a lm of technology and connectivity. What sets IoT apart is its ability to facilitate seamless communication and data exchange between these devices, often without human inter vention. This inter connectedness enables a myriad of applications across various domains, from smart homes and cities toindustrialautomationandhealthcare.Byleveragingsensors,actuators,andinternet connectivity, IoT systems gather real-time data, which can then bean alyzed and used to inform decision-making processes. This transformative technology has the potential to enhance efficiency, optimize resource utilization, and improvetheoverallqualityoflifeforindividualsandcommunitiesworldwide. As IoT continues to evolve, it is poised to play an increase ingly integral role in shaping the way we interact with the world around us RFID technology uses electromagnetic fields to automatically identify and track tags attached to objects. In the context of access control, these tags are usually placed on keycards or fobs. When a person approaches an RFID reader, the reader emits radio waves which power the RFID tag. The tag then transmits its unique identification data back to the reader**.** Retinal scanning is a biometric technology that lever ages the unique patterns of blood vessels in the retina at the back of the eye to identify individuals.

II.RESEARCH AND FINDINGS

BLYNK is aver satile and user-friendly Internet of Things (IoT) platform that empowers individuals and businesses to seamlessly connect and control a wide range of devices and projects over the internet. What sets BLYNK apart is its intuitive drag-and-drop interface, which allows users to effortlessly create custom interfaces for their to applications without the need for extensive coding knowledge.

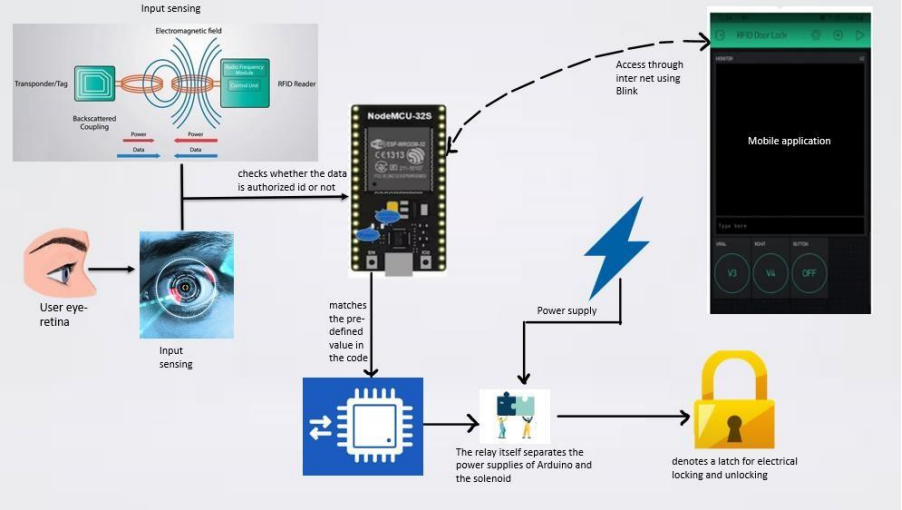
This platform supports a diverse array of hardware and communication protocols, making it compatible with an extensive range of devices, from microcontrollers like Adriano and Raspberry Pi to popular IoT development boards. With BLYNK, users can remotely monitor and manage their projects, receive real-time notifications, and even implement automation through a user-friendly mobile app. Whether for smart home a automation, industrial monitoring, or educational purposes, BLYNK offers an accessible and powerful solution for bringing IoT projects to life.

Retinal scanning is a biometric technology that lever ages the unique patterns of blood vessels in the retina at the back of the eye to identify individuals. This methods and sat the pinnacle of security technology, of feringun paralleled accuracy and reliability. Commonly deployed in highly sensitive areas like government facilities, research labs, and high-

security corporate environments, ret in allock accesses stems provide an exception allevel of security. The distinctiveness and complexity of retinal patterns make it nearly impossible forum authorized individual stoga in access. Unlike other biometric methods, such as fingerprints, retinal scans do notre quire physical contact with the scanning RFID technology uses electromagnetic fields to automatically identify and track tags attached to objects. In the context of access control, these tags are usually placed on keycards or fobs. When a person approaches an RFID reader, the reader emits radio waves which power the RFID tag. The tag then transmits its unique identification data back to the reader**.** RFID-based access control systems offer a convenient and efficient way to manage access permissions.

They have largely replaced traditional lock-and-key systems in many environments due to their advantages; including Users can carry a small RFID card or fob, which is much easier than carrying aset of keys. RFID cards can be encrypted and provide a higher level of security compared to traditional keys, as they are harder to duplicate. RFID cards can be easily deactivated or reactivated, providing flexibility in managing access rights. These systems can keep are cor do fall access events, providing valuable data for security audits.

III.SYSTEM IMPLEMENTATION



These diagrams are visual representations of the structure and components of a hardware system, such as a computer, server, or network infrastructure. These diagrams help illustrate how various hardware components interact and are interconnected.

1) Radio Wave communication

Radio wave communication is a cornerstone of modern technology, enabling the transmission and reception of information through electromagnetic waves. These waves span a wide frequency range, from approximately 3 kilohertz (kHz) to 300 gigahertz (GHz), Acoma dating diverse applications. Fundamentally, radio waves are a form of electromagnetic radiation characterized by oscillating electric and magnetic fields, traveling at the speed of light.

2) Retinal Scanner Authentication

Retinal scanner authentication is an advanced biometric security technology that leverages the unique patterns of blood vessels in the retina, located at the back of the eye, to verify a person's identity. This method provides an exceptionally high level of security due to the distinctiveness and stability of retinal patterns, which remain virtually unchanged throughout a person's life.

The process involves projecting a low-intensity infrared light into the eye, which is absorbed by the blood vessels in the retina. These absorbed patterns are then captured by a specialized camera, creating a highly detailed and unique biometric template.

3) Communication Connectivity

Communication connectivity is the lifeblood of our interconnected world, enabling seamless exchange of information across various platforms and devices. It encompasses the network infrastructures and technologies that facilitate this exchange, playing a crucial role in both personal and professional spheres.

At its core, communication connectivity relies on a multitude of technologies, ranging from traditional wired connections like Ethernet cables to wireless technologies like Wi-Fi and cellular networks.

These technologies enable devices to establish links and transmit data, allowing for real-time interactions, data sharing, and access to online resources. Wireless connectivity has seen exponential growth, with Wi-Fi networks forming the backbone of local communication within homes, offices, and public spaces. Cellular networks, on the other hand, provide ubiquitous connectivity, enabling mobile devices to communicate with each other and access the internet from virtually anywhere. The advent of 5G technology is poised to revolutionize connectivity further, promising faster.

IV.CONCLUSION

- There tinal door lock system is thatitre presents a highly advanced and secure access control solution. By utilizing the unique biometric pattern of an individual's retina, it offers a level of security that surpassestr additional key or code- based systems.
- This technology provides numerous benefits, including reduced risk of unauthorized access, increased convenience for users, and potentially even improved accessibility for those with disabilities.
- However, it's important to acknowledge some potential drawbacks. Cost and implementation complexity may be higher compared to conventional lock systems. Additionally, concerns about privacy and data security may arise, as biometric data is sensitive and requires string ent protection measures.
- In spite of these considerations, the retinal door lock system holds great promise for applications where robust security is paramount. It has the potential to revolutionize access control in high-security environments such as government facilities,
- Research laboratories and sensitive corporate spaces. As technology advances and costs potentially decrease, we may see widerad option of this cutting-edge security solution in various settings.

References

1. *Filip Lenko, "Specifics of RFID Based Access Control Systems Used inLogistics Centers"inTransportation Research Procedia*
2. *Volume55,2021,Pages1613-1619*
3. *Durica Jakub, Lenko Filip "Comparison of the difficulty overcoming ofRFID electronic access control systems and overcoming of pin tumblerlocks"inTransportation ResearchProcedia*
4. *Volume55,2021,Pages1620-1626*
5. *Nazariy K. Shaydyuk, "Biometric identification via retina scanning withlivenessdetectionusingspecklecontrastimaging"in2016IEEEInternationalCarnahan Conferenceon SecurityTechnology(ICCST)*
6. *Amritha Nag, J N Nikhilendra, Mrutyunjay Kalmath, "IOT Based DoorAccess Control Using FaceRecognition" in: 2018 3rd InternationalConferenceforConvergence in Technology(I2CT)*
7. *Andrea Motroni; Gabriele Bandini; Alice Buffi; Paolo Nepa "Investigation of Phase Offset Calibration for SAR-based RFID Localization in Harsh Environments" in 2023 IEEE 13th International Conference on RFID Technology and Applications (RFID-TA)*