World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Biometric door lock system with automated fire detection alert

Thabagnana priya D * and R.Vadivel

Department of Information Technology, Bharathiar University, Coimbatore, Tamil Nadu, India- 641046.

World Journal of Advanced Research and Reviews, 2024, 21(03), 1201–1208

Publication history: Received on 02 February 2024; revised on 10 March 2024; accepted on 12 March 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.21.3.0842

Abstract

The reconciliation of biometric advancements and fire recognition components in shrewd homes is critical for access control and crisis readiness. The Blynk mobile app is used to access this project's biometric door lock and automated fire detection system. For access authorization, the biometric system uses cutting-edge fingerprint or facial recognition technology. The mechanized fire location framework screens the climate for potential fire dangers and triggers an alert when distinguished. The Blynk application gives controller and checking abilities, permitting inhabitants to lock or open the entryway, get ongoing warnings, and remotely screen the fire discovery framework's status. The microcontroller coordinates communications between the frameworks, outfitted with Wi-Fi availability. The Blynk application point of interaction is planned with easy-to-understand gadgets, permitting inhabitants to control and screen the coordinated frameworks. Safety efforts, for example, encoded correspondence conventions and secure stockpiling of biometric information, shield client protection. This all-encompassing approach to residential security ensures that their homes can effectively handle access control and emergencies, providing residents with security and peace of mind.

Keywords: ESP32; Biometric Door Lock; Fingerprint Sensor; Fire Detection; Alarm System; Blynk App

1. Introduction

The primary objective of this project is to combine a biometric door lock system with an automated fire detection system, utilizing the Blynk mobile app for real-time control and monitoring. The project aims to create secure and intelligent living environments that prioritize residential security and safety by integrating these technologies.Security is a matter of great concern for both individuals and organizations, and home security poses a significant challenge. The effectiveness of traditional security methods, such as door locks, has been compromised by sophisticated hacker attacks and unauthorized users. As electronic devices become more prevalent, passwords and keys have become less secure, as they can be shared and easily cracked by individuals with advanced technical knowledge. The progress of civilization has prompted the development of advanced security systems to address these challenges. Traditional locks can be easily bypassed by burglars, leaving valuable items like jewelry, bank cards, and money vulnerable to theft. Moreover, the loss or misplacement of keys can result in lengthy waiting periods for technicians to arrive, and even authorized individuals may find themselves unable to access their property if the key is locked away or misplaced. In summary, security is an urgent issue that has evolved, necessitating the implementation of more reliable measures to safeguard valuable possessions.[1]

1.1. Biometric door lock system

The project's main goal is to integrate a biometric door lock system with an automated fire detection system. This integration will be achieved by utilizing the Blynk mobile app, which will allow for real-time control and monitoring. The ultimate aim of this project is to create safe and intelligent living spaces by combining advanced technologies for

* Corresponding author: Thabagnana priya D

residential security and safety.In today's highly competitive world, the security of office premises poses a major concern, as individuals find themselves grappling with the task of safeguarding their confidential possessions manually.[2]

1.2. Automated Fire Detection System

By integrating a biometric door lock system with an automated fire detection system, the project seeks to enhance residential security and safety. The Blynk mobile app will be used for real-time control and monitoring, enabling users to have complete control over their living environments. This integration of advanced technologies aims to create secure and intelligent living spaces.

The project's objective is to integrate a biometric door lock system with an automated fire detection system, utilizing the Blynk mobile app for real-time control and monitoring. This integration aims to create secure and intelligent living environments by combining advanced technologies for residential security and safety.

The project aims to redefine residential security by providing residents with a comprehensive solution for unauthorized access and emergency responses through the use of biometric access control, fire detection technology, and IoT-driven remote control.

The project introduces an innovative smart locking system that utilizes the Internet of Things to effectively deter unauthorized access and trespassing.[3]

1.3. Problem Statement

In contemporary residential security systems, the need for a robust and integrated solution that combines advanced access control with proactive safety measures is evident. The conventional reliance on keys for door access poses security risks, and the absence of automated fire detection systems leaves homes vulnerable to potentially devastating emergencies. Addressing these concerns, this project aims to develop a comprehensive Biometric Door Lock System with Automated Fire Detection and Alert capabilities, controlled and monitored through the Blynk mobile application. Traditional key-based door lock systems are susceptible to unauthorized duplication or loss. Residents often face challenges managing and securing physical keys, leading to potential security breaches. Residential spaces often lack sophisticated fire detection systems. The absence of early warning mechanisms increases the risk of delayed responses to fire emergencies. Existing security systems may lack remote accessibility and real-time monitoring options. Residents may face challenges in managing and monitoring their security systems while away from home. Integrating biometric technology with fire detection systems and a mobile application requires careful synchronization. Ensuring seamless communication between these components without compromising security is a technical challenge. The storage and handling of biometric data raise privacy concerns. Ensuring secure communication and storage of sensitive data is imperative to prevent unauthorized access. Users may not always be aware of the status of their security and safety systems. Lack of immediate notifications in case of security breaches or fire detection can lead to delayed responses.

2. Literature survey

The issue of security in residential and commercial settings is a common one, as there is always a risk of unauthorized access through duplicate keys. The objective of this research is to develop a biometric door lock system that utilizes fingerprints, along with a buzzer-based mechanism, to eliminate the reliance on keys and mitigate the possibility of key misplacement. In the event of an unauthorized individual attempting to gain entry, the buzzer will promptly notify the owner [4].

The security and privacy concerns brought about by the rapid advancement of technology have become a significant issue. To address this, authentication plays a crucial role in preventing fraudulent activities and thefts. A solution that has been proposed is the implementation of smart door unlock systems that utilize face recognition technology. This system utilizes a camera sensor known as the esp32-cam and employs an AI-Thinker to identify and compare the person's face with authorized faces stored in the SD card. If the individual is recognized as authorized, the door is unlocked; otherwise, it remains locked. This innovative system not only complements traditional mechanical lock methods but also assists in situations involving lost keys and provides easier access for individuals with disabilities [5].

This article examines the incorporation of biometric identification into access control systems, emphasizing the necessity for stronger and more secure solutions. The suggested approach entails a bimodal biometric procedure that combines facial and voice recognition, implemented within a Raspberry Pi system. The findings demonstrate enhanced security and dependability, although user training is required. Subsequent research could delve into remote control and GSM network integration [6].

Fingerprints have been utilized in forensic inquiries since the late 19th century. However, with the latest progress in fingerprinting technology, it is now possible to gather chemical data regarding an individual's drug consumption and handling, in addition to their identification [7].

The objective of this research was to enhance security measures in high-security zones and bank vaults by developing an intelligent door access system that utilizes a fingerprint module. This system incorporates both hardware and software technologies, featuring an emergency beep sound and an indicator to alert users of any emergencies. By granting access solely to authorized individuals and employing motors for door locking and unlocking, this system guarantees top-notch security functionalities. In contrast, conventional lock systems and passwords are constrained by the risks of loss, theft, and forgetfulness [8].

This centered around the development of a door security alarm system that incorporates SMS verification and voice recognition. By utilizing a microcontroller and an Android application, the system effectively manages door operations and promptly sends notifications in the event of an unauthorized access attempt. To ensure accurate access control, the system leverages Google's open-source speech-to-text technology [9].

Fire alarm systems play a vital role in the detection, monitoring, and control of fire hazards. A comprehensive building automation framework is designed to minimize expenses and enhance dependability. The suggested framework utilizes fiber optic connections to facilitate real-time communication and provide extensive network coverage. This groundbreaking approach guarantees effective building management [10].

A microcontroller is employed in a door lock system that utilizes fingerprint recognition. This system incorporates a fingerprint sensor module to verify users and manage an electronic door lock. The hardware components consist of an Arduino Uno, fingerprint sensor module, relay module, solenoid door lock, and adapter. Rigorous testing was conducted to assess the system's functionality, security, and usability, which successfully showcased precise user identification and effective prevention of unauthorized access [11].

3. Existing System

The previous Door Lock system project developed is a Digital Code Lock System that operates on the keypad. Any person can open the door who knows the pass keys. Hence, a Digital code lock system cannot authenticate the person hence one can easily enter which results in theft or mishap [12]. If the smartphone's battery level is low, the door cannot be opened when the fingerprint sensor is connected [13].

4. Methodology

The methodology for the development of a Biometric Door Lock System with Automated Fire Detection and Alert capabilities, integrated through the Blynk app, involves a systematic approach. The process begins with defining the requirements for the system, creating a comprehensive system architecture, and identifying the required components for the hardware setup. The biometric door lock system is implemented by selecting and integrating a biometric sensor, implementing biometric verification logic, and integrating the electric door lock mechanism. The automated fire detection system is implemented by choosing and integrating fire sensors capable of detecting smoke or heat anomalies, monitoring output, and triggering an alarm. The Blynk app is integrated by creating a new project, adding Blynk widgets, and integrating the Blynk library into the microcontroller code. Wi-Fi connectivity is set up on the microcontroller, and code is written to handle the integration of the biometric door lock system and fire detection system logic with Blynk widgets. Hardware integration is done by connecting and assembling all hardware components, ensuring proper power supply, and conducting initial testing. System testing and optimization are conducted, and user training and documentation are developed. The integrated system is deployed in the target environment, and maintenance is established for regular system checks and updates.

4.1. Components Used

4.1.1. ESP32 Devkit

The ESP32 chip offers Wi-Fi and Bluetooth connectivity for embedded devices, commonly known as IoT devices. Although ESP32 specifically refers to the chip, the manufacturer often uses the term "ESP32" to describe the modules and development boards that incorporate this chip.

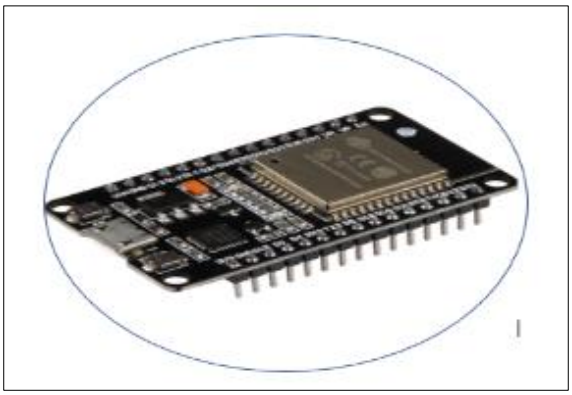

Figure 1 ESP32

4.1.2. R307 Fingerprint Module

The R307 fingerprint sensor operates by scanning an individual's fingerprint and generating a digital representation of distinct patterns found on the fingertip. Subsequently, this representation is analyzed and transformed into a mathematical algorithm, which is subsequently stored within the sensor.

Figure 2 R307 fingerprint Module

4.1.3. Solenoid Lock

A solenoid is an electromechanical apparatus that transforms electrical energy into physical movement. It is incorporated within a locking system and regulated by electronic circuitry. Solenoid locks are dependable, safe, and effortlessly operated, providing functionalities such as audit trails and remote access control.

Figure 3 Solenoid lock

4.1.4. Single channel 5V Relay Module

A DIY electronic component known as a Single Channel 5V Relay Module is designed to control high-voltage devices by utilizing a low-voltage signal, which necessitates a 5V power supply.

Figure 4 Single-channel 5v Relay Module

4.1.5. Flame sensor

A Flame Sensor is an apparatus that can be utilized to identify the existence of a fire source or any other intense light source. There are multiple methods to incorporate a Flame Sensor, however, the component employed in this undertaking is an Infrared Radiation Sensitive Sensor.

Figure 5 Flame Sensor Module

4.2. Working Principle of R307 Fingerprint Module

The optical sensor in the fingerprint capture module is utilized to capture a high-resolution image of the user's finger. Through the application of algorithms, the image undergoes processing to improve its quality and eliminate any noise present. Subsequently, a distinctive digital template is generated, encompassing mathematical representations of the fingerprint's unique characteristics. The module may possess onboard memory capable of storing multiple templates, facilitating efficient matching during the authentication process. By comparing the extracted features with the stored templates, a determination regarding a match is made. As a result, the module produces an output signal that signifies successful authentication, enabling it to regulate system access or initiate specific actions.

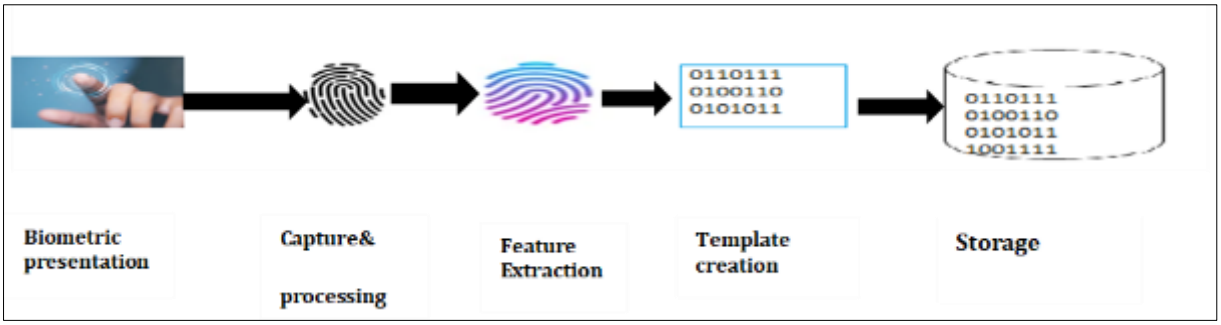

Figure 6 Fingerprint Sensor work

4.2.1. Working Principle of Flame Sensor

Flame sensors are designed to detect flames by utilizing infrared (IR) radiation emitted by the flames. These sensors are highly sensitive to specific wavelengths of IR radiation, including silicon or gallium arsenide. The IR radiation is then

converted into an electrical signal by the sensor's onboard circuitry. Once the signal surpasses a predetermined threshold level, it triggers an output signal. This output signal serves as an indication of the presence or absence of a flame. Flame sensors find applications in various fields, such as fire alarm systems, industrial safety systems, gas detection systems, and flame monitoring in combustion processes. They can either be integrated into larger systems or used independently as standalone devices.

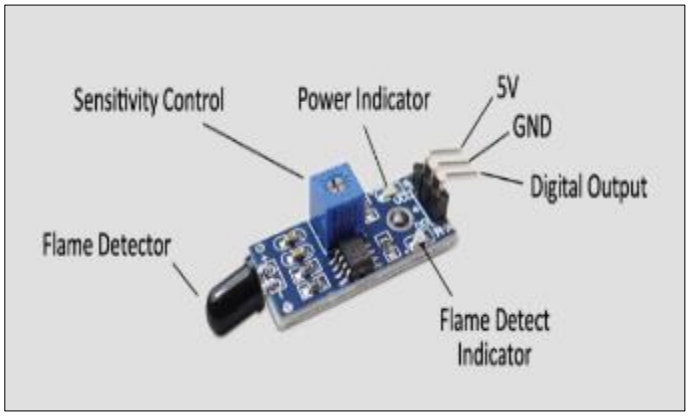

Figure 7 Flame Sensor Pinout

5. Proposed System

Real keys are the traditional method for locking or opening an entryway, but they have limitations. Brilliant locks are keyless entryway locks that open without a genuine key. These locks are electromagnetically designed and use solenoid locks. Fingerprints are a popular biometric feature, providing a reliable and confusing experience. Currently, hexadecimal keypads are used in bank storage, but this does not guarantee the best security. To address security concerns, a combination of door locks and biometrics can be implemented. Biometric verification involves identifying a person by evaluating unique biological traits, such as fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures. Using fingerprints as the key to door locks can overcome security issues and prevent unauthorized entry into homes, shops, and offices. Arduino can be used to implement this system, increasing security levels. In case there is a fire in a room is a challenge, then no one can open the door with a fingerprint. At the time It automatically opens the door and sends a notification to a mobile phone through the Blynk app.

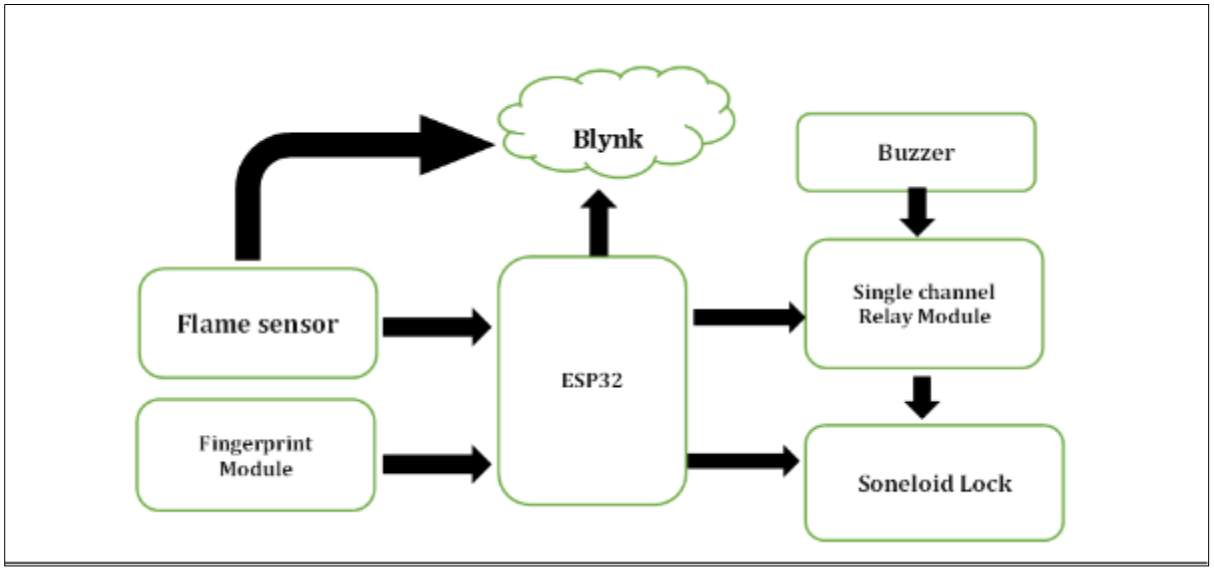

Figure 8 Block Diagram

6. Result and Discussion

The study discusses the integration of a biometric door lock system with an automated fire detection and alert system using Blynk, enhancing security through secure access control and efficient fire detection. It also explores potential improvements and the feasibility of widespread implementation. The summary highlights the system's achievements, contributions to security, and future work, suggesting improvements and avenues for further research. The study emphasizes the importance of a comprehensive discussion on individual subsystem performance and integration.

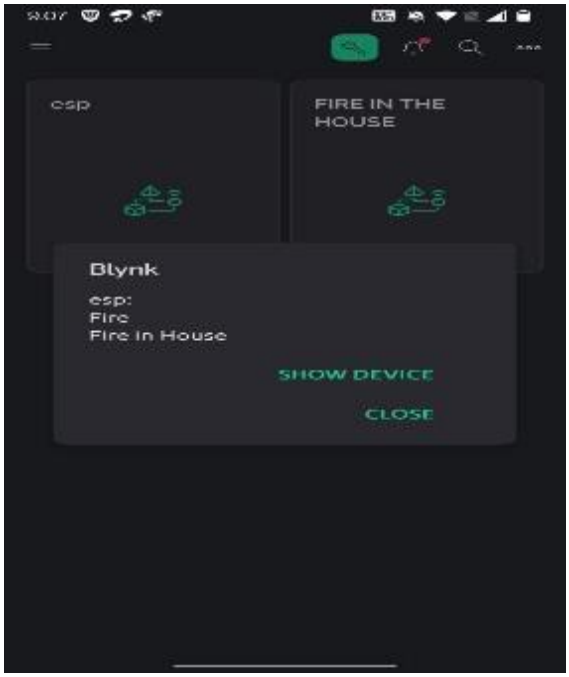

Figure 9 Blynk Notification Result

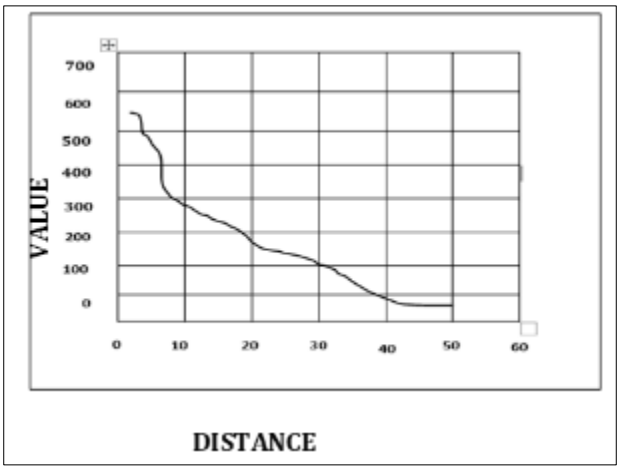

Figure 10 Flame sensor output Voltage vs Distance

7. Conclusion and Future Scope

The Blynk app is a biometric door lock system that integrates with an automated fire detection system. It offers potential for future development in areas such as multi-factor authentication, machine learning and AI, smart home integration, energy efficiency measures, IoT connectivity, advanced fire analytics, biometric data privacy enhancements, user behavioral analytics, and augmented reality integration. The app will also be updated with new features, allowing for automatic door unlocking when authorized users are in proximity. The system will also be scalable and customizable, allowing for integration with different hardware and environments. Blockchain technology will be explored for security

and transparency. The system will also be globally accessible, complying with international standards. These developments will ensure the system remains at the forefront of technology, providing advanced security features and improved user experiences.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Hashem Alnabhi , Yahya Al-naamani , Mohammed Al-madhehagi ,Mohammed Alhamzi .Enhanced Security Methods of Door Locking Based Fingerprint. Volume-9 Issue-3, January 2020.

[2] Piash Paul ,Md. Abdullah Al Achib, Hazrat Sauda Hossain, Md. Kaviul Hossain.Smart Door Lock Using Fingerprint Sensor.2019 Oct.

[3] Karthik A Patil , Niteen Vittalkar ,Pavan Hiremath ,Manoj A Murthy ."Smart Door Locking System using IoT.Volume: 07 Issue: 05 , May 2020.

[4] S. Anitha ,Ch. Hima Bindu ,J. Sriram Pavan. Biometric-based Door Lock System with Buzzer. Vol. 69 No. 1 (2020) .

[5] Nagashree Y Lakshimi Venkata , c.Rupa, B.Dharmika, Teja G nithin, N.vineela. Intelligent Secure Smart Locking System using Face Biometrics.2021 Aug.

[6] Youssef Elmir,Abdeldjalil Abdelaziz ,Mohammed Haidas.Design and Implementation of Embedded Biometric-Based Access Control System with Electronic Lock Using Raspberry Pi.2023 June.

[7] Dr. Pompi Hazarika,Prof,David A.Russell. Advances in Fingerprint Analysis. 2012 Mar.

[8] Anu ,Dinesh Bhatia.A Smart Door Access System Using Fingerprint Biometric System.Volume-6 No-3, 2014 July.

[9] A.Falohun, O.S. Makinde, B.Akin-Olayemi , T. H. Akinleye, F. W.Kehinde, O. P.Oyelami T. Design And Construction Of A Door Security Alarm System Based On Sms Verification And Voice Recognition.2021 June.

[10] F. Anwar,R .I. Boby,M.M .Rashid,M.M. Alam And Z.Shaikh.Network Based Real-Time-Integrated Fire Detection And Alarm (FDA) System With Building Automation.2017 Aug.

[11] Yasmin, Sharmin. Fingerprint Door Lock System Using Arduino. Theseus-2023.

[12] Prof. A.A. Ranaware,N.S. Desai, S.R. Teli., S.D. Londhe, S.R. Pisal.Arduino Based Fingerprint Door Lock System. Volume:04, Issue:08 August-2022.

[13] Ponmalar A, Anand J, Dharshini S, Aishwarya K ,Mahalakshimi S, Abinaya S.Smartphone controlled Fingerprint Door Lock System. Volume-40,2021 Nov.

Author's Short Biography

	**Thabagnana Priya D** received a Bachelor's degree in Information Technology in the year 2019-2022 from V.V. Vanniaperumal College for Women, Madurai Kamaraj University, Virudhunagar, Tamil Nādu. She is currently pursuing a Master's Degree in Information Technology From 2022-2024, At Bharathiar University, Coimbatore, Tamil Nadu. Her area of Interest IoT.
	**Dr.R.Vadivel** is an Associate Professor, in the Department of Information Technology, at Bharathiar University, Tamil Nadu, India. He received his Ph.D. degree in Computer Science from Manonmaniam Sundaranar University in the year 2013. He obtained his Diploma in Electronics and Communication Engineering from the State Board of Technical Education in the year 1999, B.E., Degree in Computer Science and Engineering from Periyar University in the year 2002, M.E., degree in Computer Science and Engineering from Annamalai University in the year 2007. He has published over 106 journal papers and over 50 conference papers both at the National and International level. His areas of interest include Information Security, Data mining, Digital Signal Processing.