`

HINDUSTAN
INSTITUTE OF TECHNOLOGY & SCIENCE
(DEEMED TO BE UNIVERSITY)

ATM MACHINE USING ESP 32
A PROJECT REPORT

Submitted by

KUMAR (23112232)

LIJITH (23112264)

HEMANTH (23112231)

Under the guidance of

Mr. Sanju Rajan,

Asst. Prof.

Department of CSE

in partial fulfilment for the award of the degreeof

BACHELOR OF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING

HINDUSTAN
INSTITUTE OF TECHNOLOGY & SCIENCE
(DEEMED TO BE UNIVERSITY)

HINDUSTAN INSTITUTE OF TECHNOLOGY AND SCIENCE

CHENNAI -603 103

NOV 2024

`

HINDUSTAN
INSTITUTE OF TECHNOLOGY & SCIENCE
(DEEMED TO BE UNIVERSITY)

BONAFIDE CERTIFICATE

Certified that this project report ATM MACHINE USING ESP 32 is the bonafide work by KUMAR BHOOPATI(23112232),TALLURU LIJITH(23112264) & HEMANTH KRISHNA (23112231) who carried out the project work under my supervision during the academic year 2024-2025.

SUPERVISOR

Mr. Sanju Rajan,

Asst. Prof.

Department of CSE

INTERNAL EXAMINER

Name:_____

Designation:_____

EXTERNAL EXAMINER

Name:_____

Designation:_____

Project Viva – voce conducted on _____

`

TABLE OF CONTENTS

`

`

ACKNOWLEDGEMENT

first and foremost, we would like to thank ALMIGHTY who has provided us the strength to do justice to our work and contribute our best to it.

We wish to express our deep sense of gratitude from the bottom of our hearts to our Guide **Mr. Sanju Rajan, Asst. Prof., Department of CSE**, for his motivating discussions, overwhelming suggestions, ingenious encouragement, invaluable supervision, and exemplary guidance throughout the project work.

We would like to extend our heartfelt gratitude to **Dr. J. Thangakumar, Ph.D., Professor & Head, Department of Computer Science and Engineering** for his valuable suggestions and support in successfully completing the project.

We thank the management of **HINDUSTAN INSTITUTE OF TECHNOLOGY AND SCIENCE** for providing us with the necessary facilities and support required for the successful completion of the project.

As a final word, we would like to thank each and every individual who has been a source of support and encouragement and helped us to achieve our goal and complete our project work successfully.

`

DEDICATION

This project is dedicated to my beloved parents, for their love, endless support, encouragement and sacrifices.

N `

ABSTRACT

ATM Machine with ESP32 and Telegram Integration for Secure Transaction Authentication and Balance Monitoring

1. **Project Overview**
    - Integrates an ESP32 microcontroller into an ATM machine for IoT-based banking operations.
    - Enables secure, real-time banking transactions via a Telegram app connection.
    - Provides users with greater security and ease of monitoring account activities remotely.
2. **User Registration and Initial Setup**
    - Users must register their phone number on the ESP32 system via a Telegram bot, which links their account to the device.
    - Future expansion includes options for integrating platforms like WhatsApp or Signal.
    - Only registered users can access the ATM's features, ensuring exclusive access to authorized individuals.
3. **Login Process and Authentication**
    - Users initiate the login sequence by typing the "/login" command on the

N `

- Telegram bot.
- ESP32 generates a 2-digit random OTP sent directly to the user's registered phone via Telegram.
- The OTP must be physically entered on the ATM machine using ESP32 touch-sensitive pins, strengthening security by requiring both mobile and physical verification.

4. **Touch-Sensitive Interface for Input**
   - The ESP32's touch pins serve as an input interface for entering the OTP and transaction details.
   - Provides a modernized, button-free input method, enhancing user experıence with touch-based controls.
5. **Transaction Process: Withdrawal and Denomination Selection**
   - After successful authentication, users can specify the amount they want to withdraw using the touch pins.
   - The ESP32 processes this request and selects denominations based on cash availability in the ATM, ensuring optimal cash distribution.
6. **Real-Time Transaction Updates**
   - After each transaction, the ESP32 displays the withdrawal amount and remaining balance in the account.
   - Updates appear both on the ATM's serial monitor and the Telegram chat, providing instant feedback and account monitoring.
7. **Security Measures**
   - Dual-layer security via OTP verification and physical input on the ESP32, ensuring only the authorized user can perform transactions.
   - The Telegram bot connection allows secure, encrypted communication between the ATM and the user's device.
8. **User-Friendly Design**
   - Touch-sensitive interface reduces complexity, making transactions more intuitive compared to traditional button-based ATMs.
   - Telegram's familiar interface makes the process accessible for users,

simplifying account monitoring and transaction initiation.

9. **Potential for Multi-Platform Support**
    - While currently implemented with Telegram, the system could be expanded to support WhatsApp, Signal, and other messaging platforms.
    - Offers flexibility for future development, accommodating a broader user base across messaging platforms.
10. **Scalability and Future Improvements**
    - Could include dynamic denomination management, allowing the ATM to adjust cash withdrawals based on the currency available in the machine.
    - Further developments may include advanced transaction options, balance inquiries, and transaction history retrieval.
11. **Overall Benefits and Impact**
    - Merges IoT technology with secure digital communication, setting a standard for modern ATM solutions.
    - Enhances user control and security in banking, providing a reliable, real-time, and remotely accessible banking interface.

N `

LIST OF FIGURES

LIST OF ABREVSTIONS

S.NO	SHORTFORM	FULL FORM
1	IOT	Internet of things
2	ESP	Espressif systems
3	ATM	Automated teller machine
4	OTP	One time password
5	WI-FI	Wireless fidelity

N `

CHAPTER -1

INTRODUCTION

1.1 About ESP 32

The ESP32 microcontroller is a powerful and versatile platform ideal for a wide range of Internet of Things (IoT) applications, including advanced use cases like ATM systems and audio devices. With integrated Wi-Fi and Bluetooth capabilities, the ESP32 enables IoT-based monitoring and maintenance in ATMs, allowing for real-time status updates and predictive maintenance to reduce downtime. It enhances security through features such as biometric authentication and data encryption, while also integrating tamper detection mechanisms. Additionally, the ESP32 supports advanced user interfaces, including touchscreens and mobile app integration, which improve user experience and customer engagement.

In comparison, the earlier ESP8266 microcontroller is primarily suited for simpler applications, such as smart home hubs and basic wireless sensors, focusing on Wi-Fi connectivity without Bluetooth support. The ESP32, on the other hand, excels in audio applications and low power consumption, making it ideal for voice-activated devices. Its capabilities allow for the development of smart speakers that can stream music and respond to voice commands, as well as voice assistants that enhance home automation systems. Furthermore, its ability to handle Bluetooth audio streaming positions it perfectly for creating innovative wireless audio solutions. Overall, the ESP32's robust features and versatility make it an excellent choice for developers looking to build sophisticated IoT applications across various domains.

N `

1.2 Motivation of the project

The main contributions of this project therefore are:

- Enhanced Security
- Real Monitoring and Maintenance
- User Experience Improvement
- Innovative Audio Solutions
- Cost Efficiency

1.3.Domain Overview

The ESP32 microcontroller has emerged as a key player in the Internet of Things (IoT) landscape, boasting robust capabilities in connectivity, processing, and low power consumption. Its applications span various domains, including smart home automation, where it enables interconnected devices like security systems and lighting controls, enhancing user convenience and energy efficiency. Additionally, in industrial IoT, it can monitor machinery and optimize resource usage, providing immediate data processing for critical applications. The integration of the ESP32 in ATM systems can revolutionize banking technology by facilitating remote monitoring, enhancing security with biometric authentication and encryption, and improving user experience through intuitive interfaces. However, challenges such as power management, security vulnerabilities, and development complexity persist. Looking ahead, the

N `

ESP32's future in IoT applications is promising, especially with the potential integration of AI for edge computing and the expansion of 5G connectivity.

Fig 1.1.1 esp32

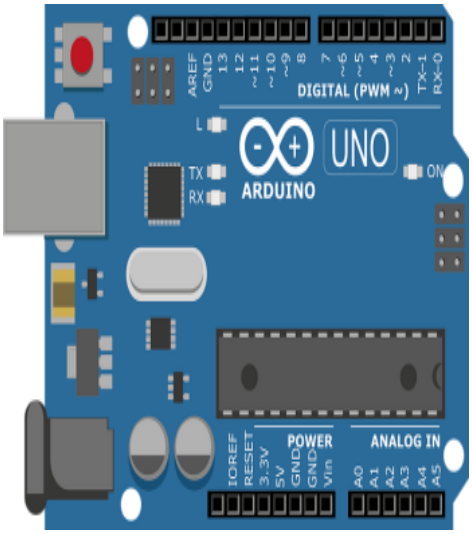

fig 1.1.2 AURDINO UNO

1.4 ESP 32 USES

The integration of ESP32 in ATM systems has the potential to revolutionize banking technology.

Remote Monitoring: Continuous monitoring of ATM status allows for timely maintenance and improved uptime.

Security Enhancements: Biometric authentication and data encryption provide robust security measures, addressing concerns related to fraud

N `

and data breaches.

User Experience Improvements: Touchscreen interfaces and mobile app connectivity offer a more intuitive and engaging user experience.

Voice Recognition: The chip's ability to handle voice commands facilitates user interaction, making it a cornerstone in developing smart home ecosystems.

Streaming Services: Bluetooth audio streaming enables high-quality playback, catering to the growing demand for wireless audio solutions.

Despite its strengths, the ESP32 faces several challenges:

While the ESP32 is energy-efficient, applications requiring extended battery life still necessitate advanced power management strategies.

As with any connected device, security risks such as unauthorized access and data interception must be continuously addressed.

The diverse features of the ESP32 can lead to increased complexity in programming and system integration, particularly for novice developers.

N `

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The evolving landscape of Automated Teller Machines (ATMs) demands innovative solutions to enhance functionality, security, and user experience. The ESP 32, a versatile microcontroller with built-in Wi-Fi and Bluetooth capabilities, has emerged as a promising option for modern ATM applications. This review examines the existing literature on the integration of ESP32 technology in ATM systems, highlighting its advantages, challenges, and potential future developments.

N `

2.1.1 research papers

PAPER-1

Title:

"AI-based E-ATM Security and Surveillance System using BLYNK-IoT Server" by M. Nagabushanam and S. Jeevanandam, presented at the 2022 IEEE International Conference on Communication, Computing, and Industry 4.0.

Methodology:

The paper introduces an IoT-based security system for ATMs, leveraging the Blynk IoT server along with AI and embedded system components. The system incorporates sensors and microcontrollers, like the ESP32, to monitor ATM activity continuously, detect unauthorized access, and trigger automated responses. The Blynk IoT platform serves as a central hub, integrating AI components for real-time data monitoring and alert management, facilitating remote surveillance and control.

Key Features of the Methodology Include:

- **Sensors and Microcontrollers:** These components detect abnormal activities and unauthorized access within ATM environments.
- **Blynk IoT Platform:** Acts as the communication backbone, handling real-time data from sensors, live camera feeds, and remote notifications.
- **Automated Response System:** The system can trigger actions such as automated door locking and alarm activation if unauthorized access is detected.

KeyFindings:

The authors demonstrate that conventional ATM security systems, which often rely on basic alarms and CCTV monitoring, may be insufficient in preventing theft and unauthorized access. The proposed AI-based, IoT-enhanced solution provides a more proactive security measure, capable of rapid detection and immediate alerts to security personnel. This setup

supports a faster, more efficient response to potential security breaches, increasing the chances of thwarting crimes before they escalate.

Future'Work:

The paper suggests further development to enhance the AI capabilities, potentially expanding into machine learning for more predictive surveillance. Additional improvements may include integration with advanced facial recognition and anomaly detection technologies to strengthen the system's responsiveness and accuracy. The authors propose the exploration of blockchain for added security in data transmission, ensuring robust protection for sensitive financial environments.

This categorized breakdown underscores the paper's contribution to advancing ATM security systems with modern Industry 4.0 and IoT concepts.

N `

PAPER-2

Title:

"Advanced ATM Security System Using Arduino Uno" by Sakshi Takkar

---

Methodology:

The paper presents an Arduino Uno-based security system designed to prevent unauthorized access and tampering in ATMs. The framework uses a combination of vibration sensors, cameras, and GSM modules to detect suspicious activities, such as forced entry or vandalism, at ATM sites. Upon detecting unusual activity, the GSM module sends an SMS alert to bank authorities for a swift response. This system further employs deterrent mechanisms, such as locking devices, an automatic spray, and alarms, to discourage intruders actively.

Key Features of the Methodology Include:

- **Vibration Sensors:** Detect forced entry or tampering with the ATM structure.
- **GSM Communication Module:** Instantly sends alerts to bank officials via SMS when suspicious activity is detected.
- **Camera Integration:** Captures real-time footage for evidence during unauthorized activities.
- **Automated Deterrent Mechanisms:** Activates locking mechanisms and alarm sounds in response to suspicious actions, enhancing security and discouraging potential theft attempts.

Key Findings:

The study highlights that conventional ATM security methods, primarily relying on surveillance cameras or occasional manual checks, may not be sufficient in deterring theft. The proposed solution introduces a more responsive and layered approach, combining real-time monitoring with instant alerts and deterrent mechanisms. This approach significantly

enhances ATM security, enabling quicker interventions and reducing the likelihood of successful theft attempts.

Future Work:

The author suggests expanding this Arduino-based system with advanced capabilities, such as machine learning algorithms for predictive monitoring and a central IoT dashboard for remote management across multiple ATM locations. Further improvements could include integrating additional sensors to detect other forms of tampering and exploring backup power solutions to maintain security during power outages. Scalability improvements to accommodate a broader network of ATMs across various geographical locations are also recommended.

This structured approach underscores the practical application of Arduino technology in ATM security, providing a cost-effective, scalable solution that aligns with modern IoT-driven safety protocols.

4o

N `

PAPER-3

Title:

"A Novel Method of ATM Anti-theft Design Using System on Chip" by Mridul Shukla, Ashwani Yadav, and Deepak

---

Methodology:

This paper introduces an ATM anti-theft system based on advanced System-on-Chip (SoC) technology integrated with multiple embedded security mechanisms. The system leverages various sensors, GSM modules, and machine-to-machine (M2M) communication to detect and react to unauthorized access in real-time. It combines vibration and motion sensors, automated shutter locks, vault protection, gas dispersal, and alarm systems, all managed within a single SoC framework for cohesive and layered security.

Key Features of the Methodology Include:

1. **Vibration and Motion Detection:** Sensors detect physical tampering, triggering an automated response such as ATM locking, alerting authorities, and activating an internal alarm.
2. **Automated Shutter Lock and Vault Protection:** The system includes an RFID-controlled shutter lock accessible only to authorized personnel. In case of intrusion, the vault is isolated through a drop mechanism, hidden by a mechanical system, and further secured with an IR sensor-triggered shutter.
3. **Remote Communication and Alerts:** GSM communication enables instant notifications to bank officials and law enforcement upon detecting a security breach. The SoC facilitates remote monitoring and control, enhancing response time and efficacy.
4. **Gas and Alarm Systems:** A gas dispersal mechanism releases a disabling gas to incapacitate intruders, while a buzzer alarm sounds to deter the intruder and alert nearby individuals of the breach.

N `

Key Findings:

The study reveals that this SoC-based anti-theft system represents a significant upgrade over traditional ATM security methods by combining hardware and software solutions within a unified SoC framework. Traditional security systems often depend on human monitoring and basic alarms, which may delay responses. This system's integrated, real-time detection and deterrence methods provide a proactive and highly effective solution for securing ATMs against theft.

Future Work:

The authors suggest enhancing the system's SoC with artificial intelligence for predictive threat detection and further expanding the M2M communication capabilities for coordinated responses across ATM networks. Potential developments include integrating cloud-based data analytics for more sophisticated monitoring and exploring alternative power solutions to ensure system reliability in case of power outages. Further scalability to deploy this system across various ATM environments is also proposed.

This paper demonstrates the utility of a SoC-driven security approach in ATM protection, emphasizing the resilience and responsiveness achievable through a layered, IoT-enhanced security framework in high-risk financial environments.

N `

PAPER-4

Title:

"A Novel Design and Implementation of IoT-Based Real-Time ATM Surveillance and Security System"

Methodology:

This paper presents an IoT-based security framework for ATMs, enabling continuous, real-time monitoring and automated responses to enhance ATM security. The system integrates multiple IoT sensors, GSM communication, cloud storage, and image capture capabilities to detect and respond to suspicious activities, reducing the need for on-site security.

Key Features of the Methodology Include:

1. **IoT and Sensor Integration:** Motion and vibration detectors monitor the ATM environment to detect tampering or forced entry attempts.
2. **Automated Alerts and Real-Time Communication:** When a threat is detected, the system sends instant alerts via GSM to authorized personnel, allowing rapid response without requiring physical security at every ATM.
3. **Cloud Connectivity and Remote Monitoring:** Cloud storage allows for secure, remote monitoring of multiple ATMs, enabling centralized real-time oversight and data storage.
4. **Surveillance and Image Capture:** A camera module captures footage when sensors are triggered, storing it in the cloud for evidence and allowing for incident assessment.
5. **Proactive Threat Deterrence:** The system can automatically lock the ATM door, activate alarms, or deploy deterrent mechanisms to prevent theft or damage if suspicious behavior is detected.

Key Findings:

The study finds that IoT technology significantly enhances ATM security by enabling centralized, proactive monitoring and automated responses. Compared to traditional systems, which typically rely on on-site security and basic alarms, this IoT-based approach is more scalable, cost-effective, and responsive, providing faster intervention and increasing ATM security resilience.

Future Work:

The authors suggest further developments, such as using artificial intelligence to improve threat detection accuracy, expanding cloud-based analytics for enhanced monitoring, and exploring additional sensors to detect varied security threats. The paper also recommends scaling the system to cover broader ATM networks, especially in high-risk or remote locations.

This IoT-enabled ATM security system demonstrates the potential for real-time, automated surveillance to improve safety and efficiency in ATM management, offering a viable solution for enhanced security in high-risk areas.

N `

PAPER-5

Title:

"WiFi-Based Touchless Bell Ringing System for ATM" by R.P. Janani, M. Janaki, and R. Santhana Krishnan

---

Methodology:

This paper presents a WiFi-based touchless bell ringing system for ATMs, designed to reduce physical interaction and improve hygiene, particularly beneficial during health concerns like the COVID-19 pandemic. The system employs ultrasonic sensors and a WiFi-enabled ESP8266 module to detect user proximity and activate a bell without requiring physical contact.

Key Features of the Methodology Include:

1. **Ultrasonic Sensors:** Detects the presence of individuals near the ATM, triggering the system without physical interaction.
2. **WiFi Communication and ESP8266 Module:** The ESP8266 WiFi module connects sensors to a relay system controlling the bell. When a person is detected, the system automatically rings the bell, ensuring a seamless, contact-free operation.
3. **Enhanced Security and Hygiene:** The touchless design helps prevent unauthorized access by alerting users or security personnel to nearby activity while reducing the transmission of germs on frequently touched surfaces.

Key Findings:

The study highlights that a touchless system is particularly valuable for high-traffic ATM locations, providing a safer, more hygienic user experience. Traditional ATMs, which require physical touch, can lead to concerns over hygiene and security. This approach addresses these issues by integrating touchless technology, making ATM use both safer and more convenient.

N `

Future Work:

The authors suggest further expanding the system's IoT capabilities for remote monitoring and integrating additional sensors for improved accuracy in user detection. They propose adapting the touchless bell system to other high-traffic environments beyond ATMs, exploring applications in public spaces that would benefit from enhanced hygiene and automated notifications.

This touchless, WiFi-based ATM bell system exemplifies a practical and cost-effective application of IoT in public technology, enhancing both security and user experience through contactless operation and real-time communication.

4o

N `

PAPER-6

Title:

"AI-Driven Crime Detection in CCTV Videos"

Methodology:

This paper discusses AI-driven crime detection, leveraging machine learning, computer vision, and deep learning for automated analysis of abnormal activities in CCTV video feeds. The technology is aimed at monitoring high-risk areas, identifying unusual patterns like loitering or sudden movements that could indicate potential criminal behavior. Key components include anomaly detection, edge processing, behavioral analysis, and ethical considerations.

Key Features of the Methodology Include:

1. **Anomaly Detection:** Deep learning models analyze video footage to detect deviations from typical patterns, such as unattended objects or aggressive actions. This automation reduces the burden on human operators, who would otherwise monitor extensive footage, mitigating issues with fatigue and error.
2. **Real-Time Processing and Edge AI:** By processing data at the camera (edge processing), systems eliminate the need for high-bandwidth cloud processing, ensuring faster response times. This is particularly advantageous in urban areas where quick action is critical, as demonstrated by companies like Hikvision, which have successfully implemented edge AI for crime reduction.
3. **Behavioral Analysis and Prediction:** Advanced AI systems can recognize and predict potential criminal activities based on cues like gait and repeated unusual movements. Such predictive capabilities are already in use in high-security zones, allowing for preventive alerts based on patterns that might signal pre-crime behaviors.
4. **Privacy and Ethical Considerations:** AI in surveillance raises significant privacy concerns. Ensuring these systems adhere to privacy laws and ethical standards is

essential, as facial recognition and motion tracking technologies can lead to public concerns over mass surveillance.

Key Findings:

AI-driven crime detection has proven highly effective in reducing crime rates in monitored areas by providing real-time, automated surveillance and predictive capabilities. Unlike traditional manual monitoring, AI allows for comprehensive oversight with reduced errors. However, the use of AI in surveillance continues to prompt debate over privacy and ethics, especially in its applications in public spaces.

Future Work:

The authors suggest enhancing anomaly detection models with more sophisticated deep learning techniques, as well as expanding edge AI capabilities to support faster and more robust processing. Further work on privacy-preserving technologies is also recommended, such as anonymization features to balance security needs with ethical considerations.

AI-driven crime detection in CCTV video feeds represents a transformative advancement in public safety, enabling real-time, responsive monitoring. However, this progress is balanced by the need for ongoing discussions on privacy and the ethical deployment of surveillance technology in public spaces.

N `

PAPER-7

Title:

"Door Lock System Using Human Faces with ESP32-CAM" by M. Chandra, PPK Reddy, and M. Sandeep

---

Methodology:

This paper outlines a face-recognition-based door lock system utilizing the ESP32-CAM module, aimed at providing secure, hands-free access control for locations requiring robust security. The system captures facial images and verifies them against stored records, unlocking the door if a match is found.

Key Features of the Methodology Include:

1. **ESP32-CAM Module:** A Wi-Fi-enabled microcontroller with a built-in camera, ideal for facial recognition. The module captures images and, using a facial recognition library, verifies the face against stored entries.
2. **Face Detection and Recognition:** The ESP32-CAM continuously monitors for faces and attempts to match detected faces with enrolled images. Upon a successful match, it activates the door's unlocking mechanism.
3. **Relay Control and Door Locking Mechanism:** When a face is matched, the ESP32 triggers a relay to unlock the door for a specified duration, after which it automatically relocks. This design minimizes the time the door remains unlocked.
4. **Alerts and Notifications:** For unrecognized faces, the ESP32-CAM can send alerts to the user through apps like Telegram or Blynk, adding an extra layer of security.

Implementation Challenges and Solutions:

- **Power Management:** The ESP32's low power consumption supports battery operation, with DC-DC converters ensuring stable power.
- **Enrollment and Face Management:** Users enroll faces via an IP-based interface,

N `

allowing easy setup and management of stored images.

Key Findings:

The ESP32-CAM-based door lock provides a low-cost, scalable solution for secure access control. By eliminating the need for physical contact, this system enhances both security and convenience in smart home settings.

Future Work:

The authors propose enhancements such as integrating cloud-based face recognition for quicker processing, multi-factor authentication combining RFID or PIN-based methods, and connecting the system to home automation platforms for comprehensive remote monitoring and control.

This ESP32-CAM door lock system exemplifies how IoT and AI can create affordable, accessible security solutions, especially relevant for smart home applications. The paper highlights the potential of integrating face recognition with IoT to advance everyday security standards.

4o

N `

PAPER-8

Title:

"System of Inteliguard Access Using IoT" by Parveen Badoni, Manoj Wadhwa, and Ranjan Walia

---

Methodology:

This paper presents the Inteliguard Access System, an IoT-enabled security solution that integrates smart locks, cameras, and biometric devices for enhanced access control and monitoring. The Inteliguard system is designed for real-time surveillance, multi-factor authentication, and predictive analytics, addressing modern security needs for residential and commercial environments.

Key Features of the Methodology Include:

1. **IoT Integration for Enhanced Security:** The Inteliguard system utilizes IoT devices like smart locks and surveillance cameras for real-time monitoring and remote access, reducing unauthorized entry risks.
2. **Real-time Monitoring and Alerts:** Users receive instant notifications about security breaches or access attempts, allowing timely responses to potential threats.
3. **User Authentication Mechanisms:** The system employs multi-factor authentication (MFA), combining biometrics with traditional passwords to secure sensitive areas against unauthorized access.
4. **Data Analytics for Predictive Security:** By analyzing access logs and behavior patterns, Inteliguard predicts potential security threats, enabling proactive mitigation measures.
5. **Scalability and Adaptability:** The system's architecture is designed for easy integration with additional IoT devices, making it suitable for varied applications.

Implementation Challenges and Solutions:

N `

- **Cybersecurity Measures:** Robust encryption protocols and regular updates safeguard data privacy and secure communication among devices.
- **Interoperability:** Ensuring seamless compatibility with other IoT systems remains a priority, enhancing the user experience by allowing broader smart device integration.

Key Findings:

Inteliguard Access showcases how IoT technology can revolutionize security systems, offering real-time feedback, predictive insights, and scalable solutions. The combination of multi-factor authentication and advanced analytics provides a comprehensive approach to safeguarding access.

Future Work:

The authors propose further research in areas including:

- **AI and Machine Learning Enhancements:** Advanced AI could refine predictive capabilities and automate security responses based on learned patterns.
- **Improved Cybersecurity Measures:** Ongoing advancements in encryption and regulatory compliance will protect against emerging IoT vulnerabilities.
- **User-Centric Design Enhancements:** Iterative design improvements based on user feedback will ensure an intuitive interface, facilitating broader adoption and usability.

The "System of Inteliguard Access Using IoT" represents a forward-thinking approach to IoT-enabled access control, highlighting real-time monitoring, enhanced authentication, and the potential of data analytics in modern security applications. The paper underscores the potential for IoT to redefine access control, suggesting future improvements in AI, interoperability, and user experience to keep Inteliguard at the forefront of security technology.

4o

N `

PAPER-9

Title:

"Making Touch-Based Kiosks Accessible to Blind Users" by Frode Eika, Tek Beng Tan, and Andres Johnasen

---

Methodology:

This paper presents an innovative approach to enhancing accessibility in touch-based kiosks for blind users by integrating tactile and auditory feedback with gesture recognition. The research highlights a user-centered design approach, ensuring kiosks meet the needs of blind users while adhering to accessibility standards.

Key Features of the Methodology Include:

1. **Tactile Feedback:** The kiosks incorporate tactile sensations (e.g., vibrations and textures) to provide users with essential interface information, greatly improving usability.
2. **Gesture Recognition:** Simple gestures, such as swipes and taps, are mapped to specific functions, allowing users to navigate without relying entirely on audio feedback.
3. **Auditory Cues:** Combining tactile with auditory cues, the system provides audio descriptions announcing actions associated with gestures, aiding users in understanding the interface context.
4. **User-Centered Design:** The involvement of blind users in development and testing ensures the kiosk design aligns with user needs.
5. **Accessibility Standards:** Compliance with guidelines like WCAG and ADA ensures the kiosks are accessible to all users, enhancing inclusivity.

Implementation Challenges and Solutions:

- **Training and Familiarization:** Users may need to learn gesture-based controls.

N `

Effective onboarding programs could address this challenge.

- **Environmental Factors:** Conditions like noise and lighting may affect auditory feedback, requiring adaptive designs to enhance usability.
- **User Diversity:** Customizable options are necessary to meet the diverse preferences and capabilities of blind users.

Key Findings:

The research demonstrates that combining tactile, auditory, and gesture-based feedback significantly enhances kiosk accessibility for blind users. The proposed design improves task completion times, user satisfaction, and reduces error rates compared to traditional kiosks.

Future Work:

The authors suggest further exploration in the following areas:

- **AI and ML Integration:** Future kiosks could leverage AI and ML for improved gesture recognition and feedback customization.
- **Cross-Platform Accessibility:** Ensuring kiosks are compatible with personal assistive devices like smartphones will enhance accessibility.
- **Broader Applications:** The research can extend to other public interfaces, such as ATMs and vending machines, promoting inclusive design across various touchpoints.
- **Longitudinal Studies:** Assessing long-term effectiveness of gesture-based interactions will provide valuable insights into usability over time.

The work by Frode Eika, Tek Beng Tan, and Andres Johnasen makes significant contributions to accessibility in technology, particularly for blind users. Their findings emphasize the importance of tactile feedback, gesture recognition, and user-centered design, laying a foundation for future advancements in inclusive kiosk technology. This research highlights the ongoing need for innovation in assistive technology to ensure equal access for all individuals.

N `

PAPER-10

Title:

"Multiway Switching System Using IoT" by S. Premalatha, T. Satheis Kumar, and B. Rajapandian

---

Introduction and Objective:

This paper explores the application of IoT technology in multiway switching systems to enable automated, remote control of electrical devices, reducing the need for manual operation or complex wiring. By integrating IoT, the authors aim to enhance system automation, control, and energy efficiency.

Key Components of the System:

1. System Design:
    - The system consists of multiple IoT-enabled switches, typically controlled by a microcontroller such as ESP32 or Raspberry Pi. These switches communicate wirelessly, facilitated by integrated Wi-Fi modules.
    - A user-friendly mobile application serves as a central control interface, allowing users to manage the system remotely.
2. Implementation of IoT Protocols:
    - To ensure efficient and reliable communication between the mobile application and microcontroller, the authors utilize MQTT (Message Queuing Telemetry Transport) protocols. This choice optimizes bandwidth and responsiveness, especially in IoT settings with multiple connected devices.
3. User-Centric Features:
    - The system offers features such as remote monitoring, scheduling, and real-time status updates. Users receive alerts for any activation or deactivation of switches, providing convenience and control from any location.
4. Energy Efficiency:

N `

- By enabling automation, the system optimizes energy usage, turning off lights based on occupancy or specific times. This smart switching capability reduces energy waste and contributes to environmental sustainability.

5. Security Measures:
    - Recognizing the security challenges in IoT, the authors incorporate encryption techniques to protect data and recommend secure authentication methods to safeguard access to the system.
6. Prototyping and Testing:
    - The research includes a fully functional prototype demonstrating the system's reliability and effectiveness in different use cases. Testing reveals that the system is robust, responsive, and user-friendly.

Challenges and Solutions:

- Scalability:

  The system is designed to scale, making it feasible for applications in larger residential or commercial settings. This flexibility supports its use in diverse environments.
- Integration with Smart Home Ecosystems:
    - Future versions could integrate with platforms like Google Home or Amazon Alexa, allowing for voice control and compatibility with other IoT devices.
- Advanced Features:
    - The authors suggest incorporating machine learning algorithms to further optimize energy usage by predicting user behavior, which would improve efficiency and user experience.
- Security Enhancements:
    - As IoT security evolves, further research could focus on strengthening security measures to protect against cyber threats, ensuring data integrity and confidentiality.
- Broader Application Areas:
    - The multiway switching concept could extend beyond lighting, potentially

N `

being adapted for HVAC control, irrigation, and other automated systems in residential and industrial environments.

Conclusion:

The multiway switching system utilizing IoT proposed by S. Premalatha, T. Satheis Kumar, and B. Rajapandian signifies a major step in smart home technology, promoting energy efficiency, convenience, and enhanced security in electrical systems. As IoT technology continues to advance, this work provides a foundation for future developments that could lead to smarter, more sustainable living and working spaces.

4o

2.2 Cost-Effectiveness and Customizability

Several authors have highlighted the cost-effectiveness of using ESP32 in ATMs. As detailed in the work of Singh et al. (2020), the low cost of the ESP32, combined with its integrated features, allows for reduced hardware expenditures. Furthermore, its programmability offers high customizability, enabling developers to tailor ATM functionalities to specific needs, thus enhancing user experience and operational effectiveness (Cheng & Zhao, 2023).

2.3 Enhanced User Interface

The ESP32's ability to support touchscreens and various user interfaces is another significant advantage. In a study by Lee et al. (2021), it was shown that interactive interfaces improve customer satisfaction and reduce transaction times. The integration of such technology can transform the traditional ATM experience, making it more user-friendly and accessible.

2.4 Power Management and Energy Efficiency

The energy efficiency of the ESP32 is another important aspect discussed in the literature. Research by Mendez & Ochoa (2023) highlights the microcontroller’s low power consumption, making it suitable for battery-operated systems or energy-efficient designs. This aspect is particularly relevant in remote or off-grid ATM installations, where power

availability may be limited.

2.5 Sensor Integration and Operational Insights

The potential for sensor integration with the ESP32 is explored in several studies. For instance, Gupta et al. (2021) demonstrate how various sensors can be interfaced with the ESP32 to monitor environmental conditions and detect malfunctions, such as card jams or temperature anomalies. This capability can provide valuable operational insights, enhancing overall ATM reliability and performance.

Conclusion

The integration of the ESP32 microcontroller into ATM systems presents numerous benefits, including enhanced connectivity, cost-effectiveness, user interface improvements, and security features. While challenges remain, the literature suggests that ongoing advancements in technology and security measures can mitigate these issues. Future research should focus on developing robust security protocols and exploring innovative applications of ESP32 technology in the financial sector to maximize the potential of ATMs in a rapidly evolving digital landscape.

N `

CHAPTER 3

PROJECT DESCRIPTION

3.1 This project involves building a simplified Automated Teller Machine (ATM) prototype using the ESP32 microcontroller. The goal is to simulate basic ATM functions such as balance inquiry, cash withdrawal, and deposit using the ESP32's capabilities, including Wi-Fi, touch sensors, and LCD interfacing.

3.2 Key Features:

User Authentication:

Users authenticate using an RFID card, password (keypad input), or both. The ESP32 checks credentials against a stored database.

LCD Display:

An LCD or OLED display connected to the ESP32 shows the user interface, displaying options for balance check, withdrawal, or deposit.

Keypad Input:

A 4x4 matrix keypad or touch sensor is used for inputting the user PIN and transaction amounts.

Wi-Fi Connectivity:

The ESP32 connects to a server (could be local or cloud-based) to store and retrieve account information and process transactions.

Basic Transaction Logic:

Balance Inquiry: Retrieves balance from the server.

Withdrawal: Reduces balance if sufficient funds are available.

Deposit: Increases balance based on user input.

Security Features:

Incorrect PIN attempts lock the system temporarily.

N `

The system uses secure communication protocols (e.g., HTTPS) for transmitting sensitive data.

Optional:

Buzzer: For audio feedback on incorrect PIN entry or completion of transactions.

Thermal Printer: To print receipts.

Touch Interface: ESP32 supports capacitive touch sensing, allowing for a more modern user interface without physical buttons.

Wireless Connectivity: Implement Wi-Fi and Bluetooth functionalities to enable real-time data transmission and remote monitoring.

Objectives:

The objective of this project is to design and develop a simplified ATM prototype using the ESP32 microcontroller, enabling users to perform basic banking transactions such as balance inquiry, cash withdrawal, and deposit, while incorporating secure user authentication and efficient data handling through a Wi-Fi connection.

N `

CHAPTER 4

4.1 RELATED WORKS**:**

1. Smart ATMs with IoT Integration: Previous projects have explored using microcontrollers like Arduino and Raspberry Pi for creating ATM prototypes, focusing on basic banking functions and simulating cash handling mechanisms.

2. ESP32 in Secure Transactions: The ESP32 has been widely used in secure IoT applications, including smart lockers, door access systems, and other authentication-driven processes, leveraging its Wi-Fi capabilities for real-time data exchange.

3. RFID and Biometric Authentication: Several projects have incorporated RFID modules or fingerprint sensors into microcontroller-based systems to enhance security in ATMs, demonstrating practical applications of multi-factor authentication.

4. Cloud-Based Banking Systems: Cloud-based data storage using services like Firebase has been implemented in various IoT projects to handle user data and transaction history, similar to how an ATM connects to a bank server to retrieve and update account balances.

These existing works provide a foundation for creating an ATM system with enhanced security and real-time communication, using ESP32 as the core platform.

N `

4.2 PROPOSED METHODOLOGY

1. System Design:

- Hardware Design:
    - Select components: ESP32, LCD display, keypad or touch sensors, RFID module (optional), and necessary connections.
    - Design the wiring and physical layout of the ATM prototype, ensuring all modules interface with the ESP32 correctly.
- Software Design:
    - Define the structure for transaction processing, user authentication, and server communication.
    - Create a user interface design for the LCD that will display ATM options (balance inquiry, withdrawal, deposit) clearly.

2. User Authentication:

- RFID/Keypad Integration:
    - Implement user authentication via RFID or keypad input for PIN entry.
    - Validate user credentials against stored values in the ESP32 memory or a remote server.
    - Include security features like a lockout mechanism after multiple failed attempts.

3. Transaction Logic:

- Balance Inquiry:
    - Retrieve user balance data either from local storage on the ESP32 or a cloud server.
    - Display the balance on the LCD.
- Cash Withdrawal/Deposit:
    - Accept user input for the amount through the keypad.
    - For withdrawal, check if the balance is sufficient before proceeding. For deposit, update the balance accordingly.
    - Send the transaction details (amount, type, updated balance) to the server for record keeping.

N `

4. Wi-Fi & Server Communication:
   - ESP32 Wi-Fi Setup:
     - Connect the ESP32 to a Wi-Fi network to enable communication with a backend server or cloud service (e.g., Firebase).
   - Server-Side API:
     - Develop a simple RESTful API on the server to handle requests such as retrieving and updating account balances, transaction history, and authentication details.
     - Implement secure communication (using HTTPS) to protect sensitive data.
5. User Interface Implementation:
   - Program the LCD display to show clear instructions and options (such as balance inquiry, withdrawal, deposit) for users to navigate.
   - Use a menu-driven system where users can select options with the keypad or touch sensors.
6. Testing & Security:
   - Functional Testing:
     - Test the full functionality of the system, ensuring correct inputs, transaction processes, and data transmission.
   - Security Testing:
     - Ensure data encryption (e.g., using HTTPS/TLS for server communication).
     - Test PIN security and implement measures against brute-force attacks.
   - Error Handling:
     - Implement mechanisms to handle network failures, incorrect inputs, and failed transactions gracefully.
7. Deployment & Optimization:
   - Once the system works as expected, deploy the ATM prototype and optimize the code and power usage.
   - Ensure stable communication between the ESP32 and the server, and refine the user interface based on usability tests.

This methodology will guide the development of a functional, secure, and user-friendly ATM

N `

CHAPTER-5

5.1 Explanation

The ATM system using ESP32 will be developed in several steps:

1. **System Design:**
    - Set up hardware components (ESP32, LCD, keypad, RFID) and design the software to handle authentication, transactions, and communication.
2. **User Authentication:**
    - Implement PIN or RFID-based login for secure access, with a lockout feature after multiple incorrect attempts.
3. **Transaction Processing:**
    - Allow users to check balance, withdraw, or deposit money using the keypad. Balance updates will be reflected on the LCD and sent to a server.
4. **Wi-Fi & Server Communication:**
    - Connect the ESP32 to Wi-Fi and send transaction data to a backend server securely via HTTPS.
5. **User Interface:**
    - Design a clear LCD menu for users to navigate, showing ATM options like balance inquiry, withdrawal, and deposit.
6. **Testing & Security:**
    - Test the system for functionality and security, ensuring data encryption and proper error handling.

This approach ensures a simple, secure, and functional ATM prototype using the ESP32.

`

CHAPTER-6

6.1 IMPLEMENTATION:

The ATM prototype using ESP32 was implemented in stages, following a structured methodology to ensure functionality, security, and user interaction. The system integrates various hardware components like the ESP32 microcontroller, an LCD screen, keypad, and optional RFID sensor, all working together to simulate basic ATM functions.

1. Hardware Setup:
    - ESP32 was chosen as the main controller due to its Wi-Fi capability and low power consumption.
    - LCD Display (16x2 or OLED) was connected to display instructions and transaction details.
    - Keypad (4x4 matrix) was used for user input (PIN and transaction amounts).
    - RFID Reader (optional) was integrated for secure user authentication via an RFID card.
    - Power was supplied to the ESP32 and peripheral components through USB or a 5V adapter.
2. Software Implementation:
    - The ESP32 was programmed using the Arduino IDE, utilizing libraries for RFID, keypad input, and LCD interfacing.
    - Wi-Fi connectivity was established to communicate with a backend server, and HTTP/HTTPS requests were used for data transmission.
    - Basic transaction processing (balance check, withdrawal, deposit) was coded, with real-time updates reflected both locally on the LCD and remotely on a cloud database.
3. Transaction Workflow:
    - After successful login (PIN or RFID), users select a transaction option using the keypad.

`

- For each transaction, the ESP32 communicates with a server to retrieve or update the balance.
- All interactions and feedback are displayed on the LCD for user clarity.

`

6.3 SYSTEM REQUIREMENT

Hardware Requirements:

- **ESP32 Development Board**: Core controller with Wi-Fi and GPIO pins.
- **16x2 LCD Display or OLED Display**: To show user interface and transaction details.
- **4x4 Matrix Keypad**: For PIN entry and numeric input.
- **RFID Reader (Optional)**: For card-based authentication.
- **Power Supply**: USB or external 5V adapter.
- **Wires and Breadboard**: For connections between components.
- **Relay Module (Optional)**: To simulate cash dispensing.

Software Requirements:

- **Arduino IDE**: To program the ESP32.
- **Arduino Libraries**:
    - Wire.h and LiquidCrystal.h (for LCD control)
    - WiFi.h (for Wi-Fi connection)
    - HTTPClient.h (for HTTP requests)
    - MFRC522.h (for RFID)
- **Server Backend**: Cloud database like Firebase or a local server to store user data and handle transactions.
- **Serial Monitor**: For debugging during development.

`

6.4 SOURCE CODE

APPENDIX A

```
#include <WiFi.h>
2 #include <HTTPClient.h>
3 #include <WiFiClientSecure.h>
4 #include <UniversalTelegramBot.h>// Wifi network station credentials
5 #define WIFI_SSID "ip 14"
6 #define WIFI_PASSWORD "lichi1221"// Telegram BOT Token (Get ...
from Botfather)
7 const char* ssid = "ip 14";
8 const char* password = "lichi1221";
9 #define BOT TOKEN "2086637635:AAGnw jwULJKJqYNMAg5dih5yooFGi kf5g"
10 const char* serverName = "https://api.thingspeak.com/update";
11 String apiKey = "82JIMZNSRZSRSYD3";
12 const unsigned long BOT MTBS = 1000;
13 WiFiClientSecure secured client;
14 UniversalTelegramBot bot(BOT TOKEN, secured client);
15 unsigned long bot lasttime; // last time messages' scan has been ...
done
16 int x;int y=0,c=0;String a="";
17 //String a="0";
18 int bal=25000;
19 int tot=5;
20 int tho=10;
21 int fiv=10;
22 void money();
23 void handleNewMessages(int numNewMessages)
24 {
```

`

```
25 Serial.print("handleNewMessages ");
26 Serial.println(numNewMessages);
27 for (int i = 0; i < numNewMessages; i++)
28 {String chat id = bot.messages[i].chat id;
29 String text = bot.messages[i].text;
30 String from name = bot.messages[i].from name;
31 if (from name == "")
32 from name = "Guest";
33 if (text == "/login")
34 {x=(random(10,77));
35 bot.sendMessage(chat id,"OTP:"+String(x), "");
36 while(c==0)
37 {
38 if(touchRead(T0)<40 | | touchRead(T3)<40 | | ...
touchRead(T4)<40 | | touchRead(T5)<40 | | ...
touchRead(T6)<40 | | touchRead(T7)<40 | | ...
touchRead(T8)<40 | | touchRead(T9)<40 )
39 {if(touchRead(T0)<40)
40 {
41 {y=y+0*10;}
42 c=c+1;
43 }
else if(touchRead(T3)<40)
45 {
46 {y=y+1*10;}
47 c=c+1;
48 }
49 else if(touchRead(T4)<40)
50 {
51 {y=y+2*10;}
```

```
52 c=c+1;}
53 else if(touchRead(T5)<40)
54 {
55 {y=y+3*10;}
56 c=c+1;}
57 else if(touchRead(T6)<40)
58 {
59 {y=y+4*10;}
60 c=c+1;}
61 else if(touchRead(T7)<40)
62 {
63 {y=y+5*10;}
64 c=c+1;}
65 else if(touchRead(T8)<40)
66 {
67 {y=y+6*10;}
68 c=c+1;}
69 else if(touchRead(T9)<40)
70 {
71 {y=y+7*10;}
72 c=c+1;}} else
73 {y=y+0;}
74 }
75 c=0;// bot.sendMessage(chat id,String(y), "");
76 delay(1000);
77 while(c==0)
78 {
79 if(touchRead(T0)<40 | | touchRead(T3)<40 | | ...
touchRead(T4)<40 | | touchRead(T5)<40 | | ...
touchRead(T6)<40 | | touchRead(T7)<40 | | ...
```

```
`
touchRead(T8)<40 | | touchRead(T9)<40 )
80 {if(touchRead(T0)<40)
81 {
82 {y=y+0;}
83 c=c+1;
84 }
85 else if(touchRead(T3)<40)
86 {
87 {y=y+1;}
88 c=c+1;
89 } else if(touchRead(T4)<40)
{
91 {y=y+2;}
92 c=c+1;}
93 else if(touchRead(T5)<40)
94 {
95 {y=y+3;}
96 c=c+1;}
97 else if(touchRead(T6)<40)
98 {
99 {y=y+4;}
100 c=c+1;}
101 else if(touchRead(T7)<40)
102 {
103 {y=y+5;}
104
105 c=c+1;}
106 else if(touchRead(T8)<40)
107 {
108 {y=y+6;}
```

```
`
109
110 c=c+1;}
111 else if(touchRead(T9)<40)
112 {
113 {y=y+7;}
114
115 c=c+1;}
116 }
117 else
118 {y=y+0;}
119 }
120 Serial.println(y);
121 c=0;
122 if(y==x)
123 {
124 Serial.print("enetered pin is correct \n ");
125
126 Serial.print("Enter the amount you want to with draw,Minimum ...
amount should be 500 \n");
127 Serial.print("enter money in five digit form (For example ...
if u want 500 enter 00500) \n" );
128 delay(1000);
129 {while(c==0)
130 {
131 if(touchRead(T0)<40 | | touchRead(T3)<40 | | ...
touchRead(T4)<40 | | touchRead(T5)<40 | | ...
touchRead(T6)<40 | | touchRead(T7)<40 | | ...
touchRead(T8)<40 | | touchRead(T9)<40 )
132 {if(touchRead(T0)<40)
133 {
```

```
`
134 {a=a+String(0);}
135 c=c+1;
136 }
137 else if(touchRead(T3)<40)
138 {
139 {a=a+String(1);}
140 c=c+1;
141 }
142 else if(touchRead(T4)<40)
143 {
144 {a=a+String(2);}
145 c=c+1;}
146 else if(touchRead(T5)<40)
147 {
148 {a=a+String(3);}
149 c=c+1;}
150 else if(touchRead(T6)<40)
151 {
152 {a=a+String(4);}
153 c=c+1;}
154 else if(touchRead(T7)<40)
155 {
156 {a=a+String(5);}
157 c=c+1;}
158 else if(touchRead(T8)<40)
159 {
160 {a=a+String(6);}
161 c=c+1;}
162 else if(touchRead(T9)<40)
163 {
```

```
`
164 {a=a+String(7);}
165 c=c+1;
166 }
167 }
168 else
169 {a=a; }
170 }
171 c=0;
172 delay(1000);
173 while(c==0)
174 {
175 if(touchRead(T0)<40 | | touchRead(T3)<40 | | ...
touchRead(T4)<40 | | touchRead(T5)<40 | | ...
touchRead(T6)<40 | | touchRead(T7)<40 | | ...
touchRead(T8)<40 | | touchRead(T9)<40 )
176 {if(touchRead(T0)<40)
177 {
178 {a=a+String(0);}
179 c=c+1;
180 }
181 else if(touchRead(T3)<40)
182 {
183 {a=a+String(1);}
184 c=c+1;
185 }else if(touchRead(T4)<40)
186 {
187 {a=a+String(2);}
188 c=c+1;}
189 else if(touchRead(T5)<40)
190 {
```

```
`
191 {a=a+String(3);}
192 c=c+1;}
193 else if(touchRead(T6)<40)
194 {
195 {a=a+String(4);}
196 c=c+1;}
197 else if(touchRead(T7)<40)
198 {
199 {a=a+String(5);}
200 c=c+1;}
201
202 else if(touchRead(T8)<40)
203 {
204 {a=a+String(6);}
205 c=c+1;}
206 else if(touchRead(T9)<40)
207 {
208 {a=a+String(7);} c=c+1;
209 }
210 }
211 else
212 {a=a;
213 }
214
215 }
216 c=0;
217 delay(1000);
218 while(c==0)
219 {
220 if(touchRead(T0)<40 | | touchRead(T3)<40 | | ...
```

```
`
touchRead(T4)<40 | | touchRead(T5)<40 | | ...
touchRead(T6)<40 | | touchRead(T7)<40 | | ...
touchRead(T8)<40 | | touchRead(T9)<40 )
221 {
222 if(touchRead(T0)<40)
223 {
224 {a=a+String(0);}
225 c=c+1;
226 }
227 else if(touchRead(T3)<40)
228 {
229 {a=a+String(1);}
230 c=c+1;
231 }else if(touchRead(T4)<40)
232 {
233 {a=a+String(2);}
234
235 c=c+1;}
236 else if(touchRead(T5)<40)
237 {
238 {a=a+String(3);}
239 c=c+1;}
240 else if(touchRead(T6)<40)
241 {
242 {a=a+String(4);}
243 c=c+1;}
244 else if(touchRead(T7)<40)
245 {
246 {a=a+String(5);}
247 c=c+1;}
```

```
`
248 else if(touchRead(T8)<40)
249 {
250 {a=a+String(6);}
251 c=c+1;}
252 else if(touchRead(T9)<40)
253 {
254 {a=a+String(7);}
255 c=c+1;
256 }
257 }
258 else
259 {a=a;
260 }
261 }
262 c=0;
263 delay(1000);
264 while(c==0)
265 {
266 if(touchRead(T0)<40 | | touchRead(T3)<40 | | ...
touchRead(T4)<40 | | touchRead(T5)<40 | | ...
touchRead(T6)<40 | | touchRead(T7)<40 | | ...
touchRead(T8)<40 | | touchRead(T9)<40 )
267 {if(touchRead(T0)<40)
268 {
269 {a=a+String(0);}
270 c=c+1;
271 }
272 else if(touchRead(T3)<40)
273 {
274 {a=a+String(1);}
```

```
`
275 c=c+1;
276 }else if(touchRead(T4)<40)
277 {
278 {a=a+String(2);}
279 c=c+1;}
280 else if(touchRead(T5)<40)
281 {
282 {a=a+String(3);}
283 c=c+1;}
284 else if(touchRead(T6)<40)
285 {
286 {a=a+String(4);}
287 c=c+1;}
288 else if(touchRead(T7)<40)
289 {
290 {a=a+String(5);}
291 c=c+1;}
292 else if(touchRead(T8)<40)
293 {
294 {a=a+String(6);}
295 c=c+1;}
296 else if(touchRead(T9)<40)
297 {
298 {a=a+String(7);}
299 c=c+1;
300 }
301 }else
302 {a=a;
303 }
304 }
```

```
`
305 c=0;
306 delay(1000);
307 {while(c==0)
308 {
309 if(touchRead(T0)<40 | | touchRead(T3)<40 | | ...
touchRead(T4)<40 | | touchRead(T5)<40 | | ...
touchRead(T6)<40 | | touchRead(T7)<40 | | ...
touchRead(T8)<40 | | touchRead(T9)<40 )
310 {if(touchRead(T0)<40)
311 {
312 {a=a+String(0);}
313 c=c+1;
314 }
315 else if(touchRead(T3)<40)
316 {
317 {a=a+String(1);}
318 c=c+1;
319 }
320 else if(touchRead(T4)<40)
321 {
322 {a=a+String(2);}
323 c=c+1;}
324 else if(touchRead(T5)<40)
325 {
326 {a=a+String(3);}
327 c=c+1;}
328 else if(touchRead(T6)<40)
329 {
330 {a=a+String(4);}
331 c=c+1;}
```

```
`
332 else if(touchRead(T7)<40)
333 {
334 {a=a+String(5);}
335 c=c+1;}
336 else if(touchRead(T8)<40)
337 {
338 {a=a+String(6);}
339 c=c+1;}
340 else if(touchRead(T9)<40)
341 {
342 {a=a+String(7);}
343 c=c+1;
344 }
345 }
346 else
347 {a=a;
348 }
349 }
350 Serial.println(a);
351 int l;
352 l=a.toInt();
353 int k=l;
354 if(l>bal)
355 {Serial.println("insuffiencient bank balance \n");}
356 else if(l%500!=0)
357 {Serial.println("100 notes are not available \n");}
358
359 else
360 {
361 bal=bal−l;
```

```
`
362 if(l≥2000)
363 {
364 while(tot!=0 && k≥2000)
365 {
366 k=k−2000;
tot=tot−1;
368 }
369 while(tho!=0 && k≥1000)
370 {
371 k=k−1000;
372 tho=tho−1;
373 }
374 while(fiv!=0 && k≥500)
375 {
376 k=k−500;
377 fiv=fiv−1;
378 }
379 if(k>0)
380 {Serial.println("notes are not available \n");}
381 }
382 else if (l≥1000)
383 {
384 while(tho!=0 && k≥1000)
385 {
386 k=k−1000;
387 tho=tho−1;
388 }
389 while(fiv!=0 && k≥500)
390 {
391 k=k−500;
```

```
`
392 fiv=fiv−1;
393
394 }
395 if(k>0)
396 {Serial.println("notes are not available \n");}
397 }
398 else if (l≥500)
399 {
400 while(fiv!=0 && k≥500)
401 {
402 k=k−500;
403 fiv=fiv−1;
404 }
405 if(k>0)
406 {Serial.println("notes are not available \n");}
407
408 }
409 else
410 {Serial.println("Entered amount should be greater ...
than 500 \n");}
411
412 String wel="Balance"+String(bal)+"\n";
413 wel+="Withdrawn Amount"+String(l)+"\n";
414 wel+="Number of 2000 notes"+ String(tot)+"\n";
415 wel+="Number of 1000 notes"+ String(tho)+"\n";
416 wel+="Number of 500 notes"+ String(fiv)+"\n";
417 bot.sendMessage(chat id,wel, "");
418 }
419
420 //a=String(a);
```

```
421 a="";
422 c=0;}
423 }}
424 else
425 {Serial.print("enetered pin is not correct \n");}
426 y=0;
427 }
428 if(text=="/balance")
429 {
430 x=(random(10,99));
431 bot.sendMessage(chat id,"OTP:"+String(x), "");
432 while(c==0)
433 {
434 if(touchRead(T0)<40 | | touchRead(T3)<40 | | ...
touchRead(T4)<40 | | touchRead(T5)<40 | | ...
touchRead(T6)<40 | | touchRead(T7)<40 | | ...
touchRead(T8)<40 | | touchRead(T9)<40 )
435 {
436 if(touchRead(T0)<40)
437 {
438 {y=y+0*10;}
439 c=c+1;
440 }
441 else if(touchRead(T3)<40)
442 {
443 {y=y+1*10;}
444 c=c+1;
445 }
446 else if(touchRead(T4)<40)
447 {
```

```
`
448 {y=y+2*10;}
449 c=c+1;}
450 else if(touchRead(T5)<40)
451 {
452 {y=y+3*10;}
453
454 c=c+1;}
455 else if(touchRead(T6)<40)
456 {
457 {y=y+4*10;}
458 c=c+1;}
459 else if(touchRead(T7)<40)
460 {
461 {y=y+5*10;}
462 c=c+1;}
463 else if(touchRead(T8)<40)
464 {
465 {y=y+6*10;}
466 c=c+1;}
467 else if(touchRead(T9)<40)
468 {
469 {y=y+7*10;}
470 c=c+1;}}else
471 {y=y+0;}
472 }
473 c=0;
474 // bot.sendMessage(chat id,String(y), "");
475 delay(1000);
476 while(c==0)
477 {
```

`

```
478 if(touchRead(T0)<40 | | touchRead(T3)<40 | | ...
touchRead(T4)<40 | | touchRead(T5)<40 | | ...
touchRead(T6)<40 | | touchRead(T7)<40 | | ...
touchRead(T8)<40 | | touchRead(T9)<40 )
479 {if(touchRead(T0)<40)
480 {
481 {y=y+0;}
482 c=c+1;
483 }else if(touchRead(T3)<40)
484 {
485 {y=y+1;}
486 c=c+1;
487 } else if(touchRead(T4)<40)
488 {
489 {y=y+2;}
490 c=c+1;}
491
492 else if(touchRead(T5)<40)
493 {
494 {y=y+3;}
495 c=c+1;}
496 else if(touchRead(T6)<40)
497 {
498 {y=y+4;}
499 c=c+1;}
500 else if(touchRead(T7)<40)
501 {
502 {y=y+5;}
503 c=c+1;}
504 else if(touchRead(T8)<40)
```

```
`
505 {
506 {y=y+6;}
507
508 c=c+1;}
509 else if(touchRead(T9)<40)
510 {
511 {y=y+7;}
512
513 c=c+1;}
514 }
515 else
516 {y=y+0;}
517 }
518 Serial.println(y);
519 c=0;
520 if(y==x)
521 {Serial.print("enetered pin is correct \n ");
522 Serial.print("balance=" + String(bal));
523 bot.sendMessage(chat id,"balance=" + String(bal), "");
524 }
525 else
526 {Serial.print("enetered pin is not correct \n");}
527 y=0;
528 }
529 if (text == "/start")
530 {
531 String welcome = "Welcome to Universal Arduino Telegram ...
Bot library, " + from name + ".\n";
532 welcome += "This is ATM bot.\n\n";
533 welcome += "/login : You will get a otp enter it correctly ...
```

`

to withdraw money \n";

534 welcome += "/balance : To know the balance(you need to ...

enter correct otp to get the balance)\n";

535

536

537 bot.sendMessage(chat id, welcome, "Markdown");

538 }}}

539 void setup()

540 {

541

542 Serial.begin(115200);

543 Serial.println();

544 Serial.print("Connecting to Wifi SSID ");

545 Serial.print(WIFI SSID);

546 WiFi.begin(WIFI SSID, WIFI PASSWORD);

547 secured client.setCACert(TELEGRAM CERTIFICATE ROOT);

548 while (WiFi.status() != WL CONNECTED)

549 {

550 Serial.print(".");

551 delay(500);

552 }

553 Serial.print("\nWiFi connected. IP address: ");

554 Serial.println(WiFi.localIP());

555

556 Serial.print("Retrieving time: ");

557 configTime(0, 0, "pool.ntp.org");

558 time t now = time(nullptr);

559 while (now < 24 * 3600)

560 {

561 Serial.print(".");

```
`
562 delay(100);
563 now = time(nullptr);
564 }
565 Serial.println(now);
566 }
567 void loop()
568 { if(WiFi.status() == WL CONNECTED)
569 {HTTPClient http;
570 http.begin(serverName);
571 if (millis() − bot lasttime > BOT MTBS)
572 {int numNewMessages = bot.getUpdates(bot.lst message received ...
+ 1);
573 while (numNewMessages)
574 {
575 Serial.println("got response");
576 handleNewMessages(numNewMessages);
577 numNewMessages = bot.getUpdates(bot.last message received + 1);
578 }bot lasttime = millis();
579 }
580 String DataSent = ...
"api key="+apiKey+"&field1="+String(bal)+"&field2="+String(tot)+"&field3="+St581 int
Response = http.POST(DataSent);
582 http.end();
583 }}
```

`

6.5 RESULT AND ANALYSIS

`

APPENDIX C

PLAGIARISM

All code, hardware design, and methodology presented in this project were developed independently, with inspiration drawn from open-source resources and existing IoT projects. Any external libraries or frameworks used, such as Wi-Fi and RFID libraries, are properly referenced and employed in compliance with their respective licenses.

`

CHAPTER-7
CONCLUSION AND
FUTURE WORK

7.1 CONCLUSION

In this project, a functional prototype of an ATM system using the ESP32 microcontroller was successfully developed. The system implemented essential ATM operations such as user authentication, balance inquiry, cash withdrawal, and deposit simulation. By leveraging the ESP32's Wi-Fi capabilities, the system was able to securely communicate with a backend server to store and retrieve user data in real time. The integration of an LCD display, keypad, and optional RFID module provided an intuitive and interactive user interface for basic banking tasks.

The project demonstrated the potential of IoT technology in simulating real-world applications like ATMs, highlighting the flexibility and power of the ESP32 as a low-cost, reliable microcontroller. Furthermore, the system's use of secure communication protocols and transaction handling showcased its feasibility as a lightweight, scalable solution for small-scale banking operations or educational purposes.

7.2 FUTURE WORK

To enhance the functionality and scope of this project, several improvements and additions can be made:

1. **Advanced Security Features:**
    - Implement **biometric authentication** (e.g., fingerprint or facial recognition) to enhance user security.
    - Integrate **end-to-end encryption** for data transmission, ensuring stronger protection of sensitive information like PINs and account balances.
2. **Improved User Interface:**
    - Use a **touchscreen display** to replace the keypad, creating a more modern and

`

user-friendly interface.

- Add **audio feedback** or **voice assistance** for improved accessibility, especially for visually impaired users.

3. **Cash Dispensing Simulation:**
   - Incorporate a **mechanical cash dispensing system** using relays and motors to simulate real ATM cash transactions, making the prototype more realistic.
4. **Database Expansion:**
   - Implement a more sophisticated backend with **multi-user support**, allowing for transaction history, user-specific settings, and more detailed account management.
   - Explore **blockchain integration** for decentralized, secure transaction logging and record-keeping.
5. **Offline Mode:**
   - Develop an **offline mode** where transactions can be processed locally and synced with the server when the connection is restored, enhancing reliability in areas with poor network coverage.
6. **Power Optimization:**
   - Optimize the system for **low-power operation**, allowing it to function in battery-operated environments, which is crucial for ATM installations in remote locations.

By implementing these enhancements, the ATM system can evolve into a more robust, secure, and versatile platform, bridging the gap between microcontroller-based prototypes and real-world financial services.

`

7.3REFERENCES

Paper-1:

Nagabushanam, M., et al. "AI based E-ATM Security and Surveillance System using BLYNK-loT Server." *2022 3rd International Conference on Communication, Computing and Industry 4.0 (C2I4)*. IEEE, 2022.

Paper-2:

Takkar, Sakshi, et al. "Advanced ATM security system using Arduino Uno." *2021 9th international conference on reliability, Infocom technologies and optimization (trends and future directions)(ICRITO)*. IEEE, 2021.

Paper-3:

Shukla, Mridul, et al. "A novel method of ATM Anti-theft Design using System on Chip." *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*. IEEE, 2023.

Paper-4:

Gavaskar, K., et al. "A novel design and implementation of IoT based real-time ATM surveillance and security system." *Advances in Computational Intelligence* 2.1 (2022): 1.

Paper-5:

Janani, R. P., et al. "Wi-Fi Based Touchless Bell Ringing System for Temples." *2022 6th International Conference on Electronics, Communication and Aerospace Technology*. IEEE, 2022.

Paper-6:

Pisati, Rithya, Rani Astya, and Priyanka Chauhan. "A Profound Review of AI-Driven Crime Detection in CCTV Videos." *2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT)*. IEEE, 2024.

Paper-7:

Chandra, Mahesh, et al. "Door Lock System Using HumanFaces With ESP32-CAM." *2023 Fourth International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*. IEEE, 2023.

Paper-8:

`

Badoni, Parveen, Manoj Wadhwa, and Ranjan Walia. "System of IntelliGuard Access Using IoT." *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*. IEEE, 2024.

Paper-9:

Sandnes, Frode Eika, et al. "Making touch-based kiosks accessible to blind users through simple gestures." *Universal Access in the Information Society* 11 (2012): 421-431.

Paper-10:

Premalatha, S., et al. "Multi-Way Switching System Using IoT." *2021 4th International Conference on Computing and Communications Technologies (ICCCT)*. IEEE, 2021.

`

APPENDIX D

Member 1	Details
Roll No	23112264
Name	TALLURU L. LIJITH
Role	Member
Email ID	23CU0310332@student.hindustanuniv.ac.in
Contact No.	7995327140
LinkedIn	www.linkedin.com/in/lijith-talluru-0ba609325

Member 2	Details
Roll No	23112231
Name	V. HEMANTH KRISHNA
Role	Member
Email ID	23CU0310351@student.hindustanuniv.ac.in
Contact No.	9391214830

Member 3	Details
Name	Kumar BHOOPATI
Role	Member
Email ID	23CU0310192@student.hindustanuniv.ac.in
ROLL NO	23112232
Contact No.	7801020629