IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11618

SMART ANTI-THEFT SECURITY SYTEM USING IOT

Biju Balakrishnan, Ph.D.[1], Aathi Murugan V[2]

Assistant Professor, Master of Computer Applications, Hindusthan College of Engineering and Technology, Coimbatore, India[1]

II MCA Students, Master of Computer Applications, Hindusthan College of Engineering and Technology, Coimbatore, India[2]

Abstract: This project is entitled as **"IOT BASED SMART ANTI-THEFT SECURITY SYSTEM"** is a IOT based application. The IoT-based Anti-Theft System proposed here integrates NodeMCU, Ultrasonic sensor, and ESP32 Cam to create a robust security solution. The core concept involves detecting unauthorized individuals through the Ultrasonic sensor, capturing their faces using the ESP32 Cam, and subsequently storing the images on an SD card. Additionally, the system is designed to automatically send the captured images to the owner via email. This project aims to enhance security measures by leveraging IoT technologies. The NodeMCU facilitates connectivity and data exchange, while the Ultrasonic sensor serves as an effective means for person detection. The ESP32 Cam, equipped with facial recognition capabilities, ensures accurate identification and capture of potential intruders. Storing the images on an SD card provides a local backup, ensuring that evidence of unauthorized access is preserved. Simultaneously, the email feature enables real-time notification for the owner, allowing prompt action in response to security threats. In summary, the IoT-based Anti-Theft System combines hardware components and connectivity to create an intelligent security solution capable of detecting and capturing potential thieves, providing a valuable layer of protection for property owners.

Keywords: NodeMCU, SD card, ESP32 Cam, IoT-based Anti-Theft System

I. INTRODUCTION

In an era of rapid technological advancements, ensuring the security of our belongings has become more sophisticated and imperative than ever. The IoT-based Anti-Theft System presented herein is a cutting-edge solution designed to address the growing need for intelligent and proactive security measures. By seamlessly integrating NodeMCU, Ultrasonic sensor, and ESP32 Cam, this system aims to revolutionize the way we safeguard our spaces.The primary objective of this project is to detect potential thefts by leveraging the power of Internet of Things (IoT) technology. The utilization of NodeMCU enables seamless connectivity and communication between the various components, forming a cohesive network for real-time data exchange. The Ultrasonic sensor acts as a reliable means of person detection, while the ESP32 Cam takes the system a step further by capturing facial images of individuals within the monitored area.One of the standout features of this system is its ability to store captured images locally on an SD card. This ensures a robust and accessible record of any detected security breaches, providing valuable evidence for subsequent analysis and action. To enhance the system's responsiveness, an automated email notification mechanism has been incorporated. In the event of a security breach, the system promptly emails the captured images to the owner, facilitating immediate awareness and response.This project not only underscores the integration of hardware components but also emphasizes the synergy between these elements to create a comprehensive anti-theft solution. By combining advanced detection mechanisms and intelligent data handling, the IoT-based Anti-Theft System redefines security paradigms for a more connected and proactive future.

II. RELATED WORK

In the dynamic landscape of smart anti-theft security systems, engineers and researchers are engaged in a multifaceted endeavor to develop innovative solutions that effectively safeguard property and assets. This work encompasses a broad spectrum of disciplines, from sensor technology to artificial intelligence and beyond. Advancements in sensor technology are pivotal, as they enable the creation of more accurate and responsive detection mechanisms. Engineers are constantly refining motion sensors, door/window sensors, and glass break detectors to better identify unauthorized access or suspicious activity. Moreover, the integration of machine learning and AI algorithms enhances the system's ability to analyze sensor data, discerning patterns indicative of potential threats while minimizing false alarms.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11618

The incorporation of IoT connectivity revolutionizes the concept of security, allowing for remote monitoring and control via smartphones or other devices. This seamless integration empowers users with real-time insights into their property's security status, enabling swift response to any perceived threats. Cloud computing plays a crucial role in this ecosystem, providing scalable storage solutions and facilitating advanced analytics for threat detection. By harnessing the power of the cloud, security systems can leverage vast amounts of data to identify emerging patterns and anomalies indicative of suspicious behavior.

Biometric identification adds an additional layer of security, ensuring that only authorized individuals can access protected areas or assets. Whether through fingerprint scanning, facial recognition, or voice authentication, biometrics offer unparalleled accuracy and reliability in identity verification. However, ensuring the integrity and security of these biometric systems requires robust cybersecurity measures. Engineers must constantly innovate to safeguard against cyber threats and unauthorized access, implementing encryption protocols, regular software updates, and stringent access controls.

Moreover, user experience design plays a critical role in the effectiveness of smart security systems. Intuitive interfaces empower users to configure settings, receive alerts, and access surveillance footage with ease, enhancing overall usability and accessibility. Collaboration with law enforcement agencies further strengthens the efficacy of these systems, enabling seamless coordination in the event of a security breach or theft. By sharing data and insights, security systems can augment traditional law enforcement efforts, leading to more efficient crime prevention and response strategies.

Finally, adherence to privacy regulations and standards is paramount in the development and deployment of smart security systems. Engineers and developers must ensure that these systems comply with relevant laws and guidelines, safeguarding individual privacy rights while maintaining robust security measures. Through a concerted effort across various disciplines, the ongoing work in smart anti-theft security systems continues to push the boundaries of innovation, providing individuals and businesses with the peace of mind they need to protect their most valuable assets.

III. METHODOLOGY

The methodology behind smart anti-theft security systems encompasses a comprehensive approach that integrates various technologies and strategies to create robust and effective solutions. At its core, this methodology involves a systematic process of design, implementation, and optimization aimed at mitigating the risk of unauthorized access and theft.

The first phase of this methodology involves a thorough assessment of the security needs and vulnerabilities of the target environment. Engineers and security experts conduct a detailed analysis of the property or assets to be protected, identifying potential entry points, weak spots, and areas of concern. This initial assessment serves as the foundation for the design and implementation of the security system.

Next, engineers begin the design phase, where they conceptualize the architecture and components of the security system. This includes selecting appropriate sensors, cameras, access control mechanisms, and other relevant technologies based on the specific requirements of the environment. The design phase also involves considering factors such as scalability, integration with existing infrastructure, and user interface design to ensure a seamless and user-friendly experience.

Once the design is finalized, engineers proceed to the implementation phase, where they install and configure the various components of the security system. This may involve mounting sensors, cameras, and other devices in strategic locations, as well as integrating them with the central monitoring system or IoT platform. During this phase, engineers also set up user accounts, permissions, and access controls to ensure that only authorized individuals can manage and monitor the security system.

Following implementation, the system undergoes rigorous testing and optimization to ensure its reliability and effectiveness. Engineers conduct thorough testing scenarios to simulate various security threats and assess the system's response capabilities. This may involve testing sensor sensitivity, alarm triggers, and response times to verify that the system can accurately detect and respond to potential security breaches.

Throughout the entire process, cybersecurity is a paramount consideration. Engineers implement robust encryption protocols, authentication mechanisms, and access controls to safeguard against cyber threats and unauthorized access. Regular software updates and security audits are also conducted to identify and address any vulnerabilities that may arise over time.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11618

Finally, ongoing monitoring and maintenance are essential to ensure the continued effectiveness of the security system. Engineers monitor system performance, analyze security logs, and respond to any alerts or incidents in a timely manner. Regular maintenance activities, such as firmware updates, battery replacements, and sensor calibration, are also performed to keep the system operating at peak performance.

In conclusion, the methodology behind smart anti-theft security systems involves a systematic approach to design, implementation, and optimization aimed at mitigating security risks and protecting property and assets from unauthorized access and theft. Through careful planning, thorough testing, and ongoing maintenance, engineers create robust and effective security solutions that provide peace of mind to individuals and businesses alike.

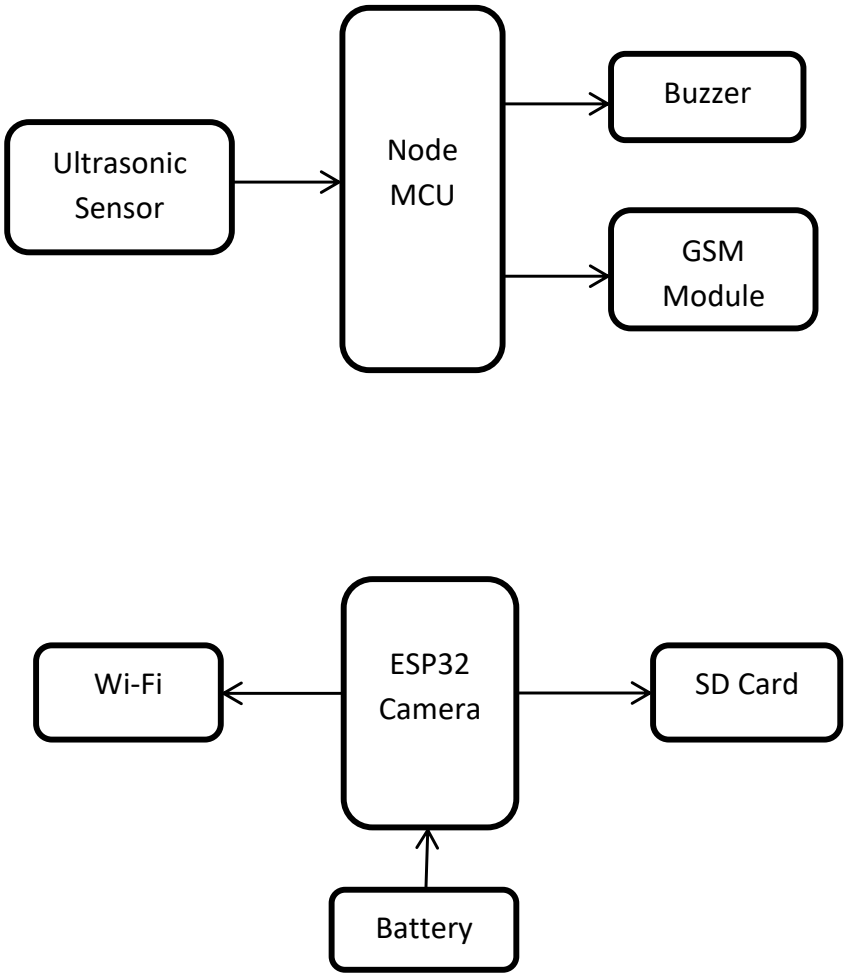

Fig 3.1 Block diagram

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11618

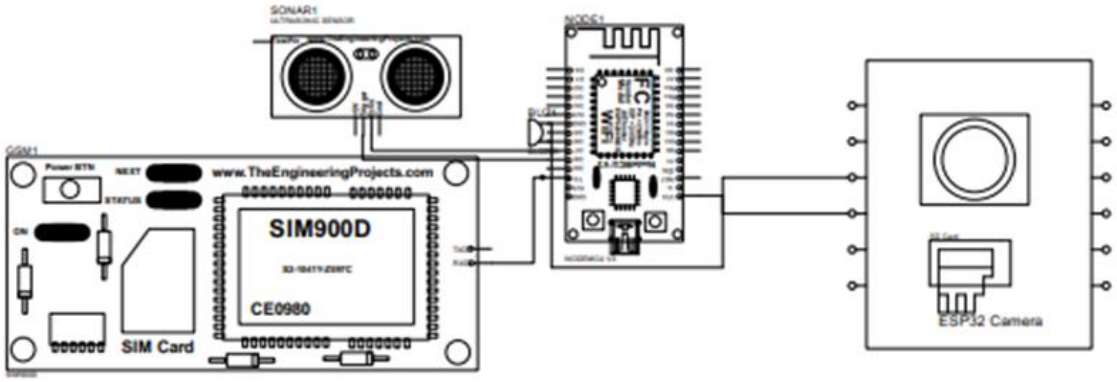

Fig 3.2 Circuit diagram

IV. IMPLEMENTATION

To implement a smart anti-theft security system effectively, a systematic approach is crucial. It begins with a thorough assessment of the property, identifying vulnerabilities and critical areas for protection. Once the components are selected, they are installed strategically, ensuring optimal coverage and connectivity. Integration into a central monitoring system or IoT platform follows, allowing for seamless communication and control. Configuration and testing ensure that the system operates as intended, with proper sensitivity and response mechanisms. Cybersecurity measures are implemented to safeguard against threats, while user training ensures efficient operation. Ongoing monitoring and maintenance are essential to keep the system functional, with procedures in place for incident response and management. Regular evaluation and improvement guarantee the system remains effective in deterring theft and unauthorized access, adapting to evolving security needs. Through this comprehensive implementation process, a smart anti-theft security system can effectively protect property and assets.

Sample Source Code

```
import cv2 #opencv
import urllib.request #to open and read URL
import numpy as np
import serial
ser = serial.Serial('com14',9600)
#OBJECT CLASSIFICATION PROGRAM FOR VIDEO IN IP ADDRESS
import smtplib
from email.mime.multipart import MIMEMultipart
from email.mime.text import MIMEText
from email.mime.image import MIMEImage
from email import encoders
def send_email_with_image():
subject = "Theft detected"
body = "unknown person identified"
to_email = "aathimurugan010@gmail.com"  # Replace with the recipient's email address
image_path = "image.jpg"  # Replace with the path to your image file
# Set up the sender and recipient email addresses
from_email = "aathimurugan010@gmail.com"  # Replace with your email address
password = "aujg thlj hxuo bjsr"  # Replace with your email password
# Set up the email message
```

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11618

```
message = MIMEMultipart()
message["From"] = from_email
message["To"] = to_email
message["Subject"] = subject
# Attach the body of the email
message.attach(MIMEText(body, "plain"))
# Attach the image
with open(image_path, "rb") as attachment:
image = MIMEImage(attachment.read())
image.add_header("Content-Disposition", "attachment", filename="image.jpg")
message.attach(image)
# Set up the SMTP server
smtp_server = "smtp.gmail.com"  # Replace with your SMTP server
smtp_port = 587  # Replace with your SMTP port
# Start the SMTP server connection
server = smtplib.SMTP(smtp_server, smtp_port)
server.starttls()
# Log in to the email account
server.login(from_email, password)
# Send the email
server.sendmail(from_email, to_email, message.as_string())
# Quit the SMTP server
server.quit()
url = 'http://192.168.14.105/cam-hi.jpg'
#url = 'http://192.168.1.6/'
winName = 'ESP32 CAMERA'
cv2.namedWindow(winName,cv2.WINDOW_AUTOSIZE)
#scale_percent = 80 # percent of original size    #for image processing
while(1):
imgResponse = urllib.request.urlopen (url) # here open the URL
imgNp = np.array(bytearray(imgResponse.read()),dtype=np.uint8)
img = cv2.imdecode (imgNp,-1) #decodificamos
img = cv2.rotate(img, cv2.ROTATE_90_CLOCKWISE) # vertical
cv2.imshow(winName,img) #  show the picture
x=ser.readline()
print(x)
if x==b'1\r\n':
cv2.imwrite('image.jpg', img)
send_email_with_image()
#wait for ESC to be pressed to end the program
tecla = cv2.waitKey(5) & 0xFF
if tecla == 27:
break
cv2.destroyAllWindows()
```

V. RESULT ANALYSIS

Analyzing the results of a smart anti-theft security system involves assessing key metrics such as incident reduction, response time, false alarm rate, and user satisfaction. By evaluating these factors, stakeholders can gauge the system's effectiveness in deterring theft and unauthorized access, ensuring prompt response to security threats, and maintaining user confidence. Additionally, considerations such as cybersecurity resilience, asset recovery rate, cost-benefit analysis, and compliance with regulations provide valuable insights into the system's overall performance and impact. Continuous improvement based on analysis results allows for ongoing optimization and enhancement of security measures to protect property and assets effectively.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11618

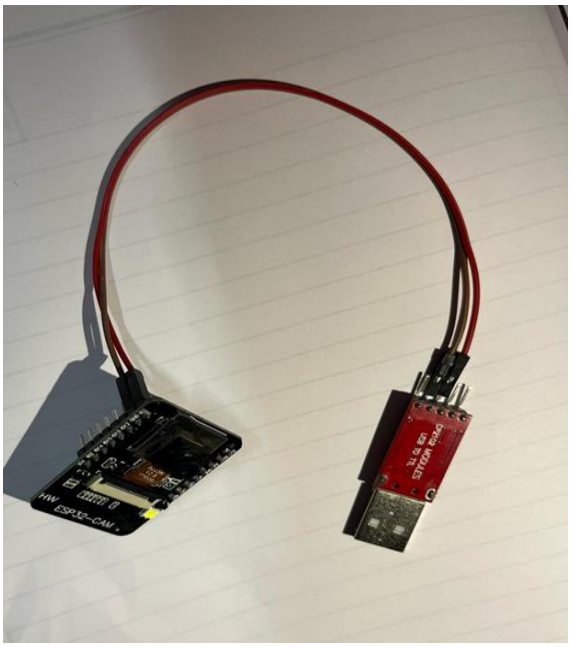

Fig 5.1 ESP 32 cam

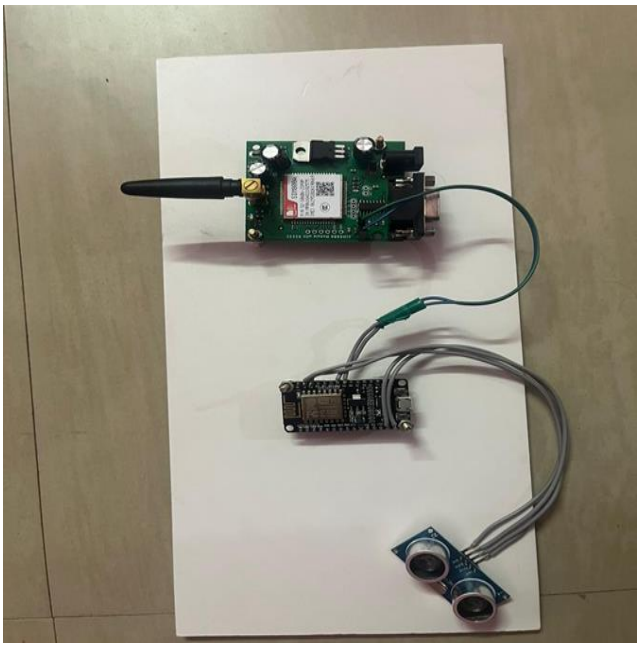

Fig 5.2 Nodu MCU

VI. CONCLUSION

In conclusion, the IoT-based Anti-Theft System represents a comprehensive and innovative approach to security, leveraging the integration of NodeMCU, Ultrasonic sensor, ESP32 Cam, and OpenCV technologies. By seamlessly combining person detection, facial recognition, and email notification capabilities, the system provides an intelligent and proactive means of identifying potential thefts. The successful integration of hardware components, meticulous programming, and the incorporation of advanced image processing techniques culminate in a robust security solution. As the system captures and recognizes faces, storing relevant data locally and alerting owners through email, it not only enhances the immediacy of response but also creates a valuable repository for post-event analysis. This project showcases the potential of IoT in transforming traditional security measures, offering a scalable and efficient solution for safeguarding properties against unauthorized access.

REFERENCES

[1]. "An IoT-Based Smart Anti-Theft System for Vehicles" - A. Gupta, R. Mishra, et al. - International Conference on Computer, Communication and Signal Processing, 2018.
[2]. "IoT-Based Smart Vehicle Security System" - P. Verma, A. Kumar, et al. - International Conference on Innovations in Information, Embedded and Communication Systems, 2017.
[3]. "Smart Anti-Theft System for Vehicles Using IoT and Android" - S. Bansal, S. Jain, et al. - International Conference on Recent Advancements in Electrical, Electronics and Communication, 2018.
[4]. "A Survey on IoT-Based Vehicle Anti-Theft Systems" - R. S. Verma, P. K. Mishra, et al. - 3rd International Conference on Inventive Systems and Control, 2019.
[5]. "IoT-Based Vehicle Theft Detection and Tracking System" - M. S. Islam, M. A. Hannan, et al. - 6th International Conference on Computer and Communication Systems, 2019.
[6]. "A Review on IoT-Based Smart Car Parking and Anti-Theft System" - S. A. Patil, A. J. Patil, et al. - International Conference on Inventive Research in Computing Applications, 2020.
[7]. "Design and Implementation of an IoT-Based Vehicle Anti-Theft System" - R. C. Meena, A. S. Khan, et al. - International Conference on Electronics, Communication, and Aerospace Technology, 2020.
[8]. "IoT-Based Smart Vehicle Security and Tracking System" - N. D. Choudhary, V. S. Jadon, et al. - 2nd International Conference on Advanced Computational and Communication Paradigms, 2019.
[9]. "Implementation of IoT-Based Vehicle Tracking and Theft Detection System" - P. Sharma, M. Gupta, et al. - International Conference on Recent Trends in Electronics, Information & Communication Technology, 2020.
[10]. "Enhanced Vehicle Anti-Theft System Using IoT and Cloud Computing" - M. V. Patil, V. B. Sable, et al. - International Conference on Advanced Communication Control and Computing Technologies, 2019.