Safe and Secure Object Detection in IoT with AES Algorithm and MQTT Protocol

Submitted By

Drashti Brahmbhatt

21MCEI01

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2023

Safe and Secure Object Detection in IoT with AES Algorithm and MQTT Protocol

Major Project - II

Submitted in partial fulfillment of the requirements

for the degree of

Master of Technology in Computer Science and Engineering (Information Network Security)

Submitted By

Drashti Brahmbhatt

(21MCEI01)

Guided By

Prof. Sharada Valiveti

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2023

Certificate

This is to certify that the major project entitled **"Safe and Secure Object Detection in IoT with AES Algorithm and MQTT Protocol"** submitted by **Drashti Brahmbhatt (Roll No: 21MCEI01)**, towards the partial fulfillment of the requirements for the award of degree of Master of Technology in Computer Science and Engineering (Information Network Security) of Nirma University, Ahmedabad, is the record of work carried out by him under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project part-I, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Prof. Sharada Valiveti
Guide & Associate Professor,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. Vijay Ukani
Associate Professor,
Coordinator M.Tech - CSE (Specialization)
Institute of Technology,
Nirma University, Ahmedabad

Dr. Madhuri Bhavsar
Professor and Head,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr R. N. Patel
Director,
Institute of Technology,
Nirma University, Ahmedabad

Statement of Originality

I, **Drashti Brahmbhatt**, Roll. No. **21MCEI01**, give undertaking that the Major Project entitled "**Safe and Secure Object Detection in IoT with AES Algorithm and MQTT Protocol**" submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in **Computer Science & Engineering (Information Network Security)** of Institute of Technology, Nirma University, Ahmedabad, contains no material that has been awarded for any degree or diploma in any university or school in any territory to the best of my knowledge. It is the original work carried out by me and I give assurance that no attempt of plagiarism has been made.It contains no material that is previously published or written, except where reference has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Drashti T. Brahmbhatt
Signature of Student
Date:
Place:

Endorsed by
Prof. Sharada Valiveti
(Signature of Guide)

Acknowledgements

It gives me immense pleasure in expressing thanks and profound gratitude to **Prof. Prof. Sharada Valiveti**, Associate Professor, Computer Engineering Department, Institute of Technology, Nirma University, Ahmedabad for her valuable guidance and continual encouragement throughout this work. The appreciation and continual support she has imparted has been a great motivation to me in reaching a higher goal. Her guidance has triggered and nourished my intellectual maturity that I will benefit from, for a long time to come.

It gives me an immense pleasure to thank **Dr. Sanjay Garg**, Hon'ble Head of Computer Engineering/ Information Technology Department, Institute of Technology, Nirma University, Ahmedabad for his kind support and providing basic infrastructure and healthy research environment.

A special thank you is expressed wholeheartedly to **Dr. Alka Mahajan**, Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad for the unmentionable motivation he has extended throughout course of this work.

I would also thank the Institution, all faculty members of Computer Engineering Department, Nirma University, Ahmedabad for their special attention and suggestions towards the project work.

- Drashti Brahmbhatt
21MCEI01

Abstract

The emergence of the Internet of Things (IoT) in recent years has completely changed how we engage with technology. New applications and use cases, have been developed as a result of the ability to connect to and communicate with numerous devices and systems. But as connected devices proliferate, security worries have grown to be a significant problem.In this study, we suggest a secure object detection and authentication system that makes use of the MQTT protocol and the Advanced Encryption Standard (AES) algorithm. An efficient and highly secure symmetric encryption technique is AES, which is extensively used. We'll make advantage of it to guarantee the privacy and accuracy of the data sent between IoT devices.The suggested system would also include machine learning methods for object detection. As a result, the system will be able to identify things in real-time, which can be helpful in a variety of settings like surveillance, home automation, and healthcare.We will use the MQTT protocol for data transport to ensure the stability and scalability of the system. IoT applications frequently employ MQTT, a simple and effective communications protocol. It is the perfect option for our suggested solution because it offers an IoT device communication channel that is dependable and secure.The suggested system will, in general, offer an effective and secure solution for object detection and authentication in IoT applications. It will show how using cutting-edge encryption and machine learning methods may improve the security and functionality of IoT systems.

Abbreviations

ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
YOLO	You Only Look Once
IOT	Internet of Things
AES	Advanced Encryption Standard

–

Contents

Certificate **iii**

Statement of Originality **iv**

Acknowledgements **v**

Abstract **vi**

Abbreviations **vii**

List of Figures **x**

1 Introduction **1**

2 Literature Survey **2**
2.1 Object detection And Summary :- 2
2.2 IOT Protocols & Summary : 12
2.3 All IoT Cryptographic Algorithms : 14

3 Proposed Approach **16**
3.1 Architecture & its Explanation : 16
3.2 Object Detection with and without using MQTT protocol and AES algorithm for Secure Communication: 18
3.3 Object Detection Technique : 19
3.4 Tools and Technologies Used : 20

4 Implementation Results **21**
4.1 Implementation Scenario : 21
4.2 Implementation and Performance Evaluation : 22
4.3 Challenges : 22
4.4 Implementation Results : 23
4.4.1 Dashboard Snapshot : 23
4.4.2 Encrypted Password : 23
4.4.3 Object Detection : 23
4.4.4 OCR : 24
4.4.5 Secure Data Transmission : 24
4.4.6 Result : 26
4.4.7 Accuracy Evaluation : 26
4.4.8 Delay in Code Execution : 27

5 Conclusions **28**

Bibliography **29**

List of Figures

3.1 Architecture Of Object Detection Process 17

4.1 Dashboard Snapshot 23
4.2 Encrypted Password 23
4.3 Object Detection 24
4.4 Front-End View 24
4.5 Character Filter 24
4.6 Missing Character 25
4.7 correcting Missing Character 25
4.8 Client Side 26
4.9 Broker Side 26
4.10 Result Store in CSV 26

Chapter 1

Introduction

The Internet of Things (IoT) has created a need for efficient and secure object detection systems[1]. However, deploying object detection in IoT faces challenges such as limited resources and security concerns. Our work focuses on the integration of the AES algorithm and MQTT protocol for safe and secure object detection in IoT. We leverage the YOLOv5 model to detect relevant objects in IoT applications[2]. The novelty of our work lies in ensuring data confidentiality and integrity through AES encryption and efficient communication using MQTT. This paper reviews related literature, discusses IoT challenges, presents our methodology and implementation[3], evaluates system performance, and concludes with future research directions. By addressing these challenges, our work enhances the efficiency and security of object detection in IoT scenarios.

Keywords: IoT, smart objects, key management, MQTT

Chapter 2

Literature Survey

2.1 Object detection And Summary :-

The use of Internet of Things (IoT) devices has increased rapidly in recent years, and with it, the need for secure communication and authentication protocols. The Advanced Encryption Standard (AES) algorithm is a widely used symmetric encryption method that can provide a high level of security for data transmission. In this paper, we propose a system that uses the AES algorithm for secure authentication and object detection in IoT applications, with data transfer via MQTT protocol.In recent years, there has been a significant increase in research on secure communication and authentication protocols in IoT applications. Many researchers have proposed various encryption methods to protect the privacy and integrity of the data transmitted between IoT devices. The proposed scheme used AES-128 encryption for secure data transmission and authentication, and achieved a low computational overhead while ensuring a high level of security.

Table 2.1: Summary of Literature Survey

REF	APPLICATION	METHODS	ADVANTAGES	DRAWBACKS

[4]	Object detection, surveillance	YOLOv5 model, MQTT protocol, AES encryption	Provides real-time object detection and surveillance capabilities, ensures the privacy and security of data transmission, and reduces bandwidth usage	May require additional computational resources for processing and analysis, may be affected by environmental factors such as lighting and weather conditions, and may raise privacy concerns if used for surveillance purposes
[5]	Object detection in IoT	AES encryption	Enhanced security and privacy of data transmission, protection against unauthorized access	Potential increase in computational overhead, potential impact on real-time performance

[2]	Smart parking system	Object detection, image processing	Reduces traffic congestion, saves time and fuel consumption, eliminates the need for physical sensors	Limited scalability due to the use of centralized servers, high dependency on the internet connection, and potential privacy concerns
[6]	Object detection	Object detection, MQTT protocol, AES encryption	Ensures the privacy and security of data being transmitted, reduces the bandwidth usage, and provides real-time and low-latency data transmission	The use of encryption and decryption algorithms may affect the performance of the system, the latency may increase with the number of subscribers, and there is a risk of data loss during transmission

[7]	Object detection	YOLOv4 model, MQTT protocol, AES encryption	Achieves high detection accuracy and fast processing speed, ensures secure and efficient data transmission, and can be applied in various IoT scenarios	May require additional computational resources for processing and analysis, may be affected by environmental factors such as lighting and weather conditions, and may raise privacy concerns if used for surveillance purposes

[8]	Object detection, surveillance	Improved YOLOv3 model, MQTT protocol, AES encryption	Enables real-time object detection in surveillance applications, ensures secure and efficient data transmission, and reduces network bandwidth usage	May require additional computational resources for processing and analysis, may be affected by environmental factors such as lighting and weather conditions, and may raise privacy concerns if used for surveillance purposes
[9]	Object detection	Deep learning, edge computing, secure communication protocol	Reduces the latency and bandwidth consumption by processing data at the edge, enhances the security and privacy of data transmission, and improves the scalability of the system	Requires additional hardware and infrastructure, may not be suitable for resource-constrained devices, and may increase the cost of the system

[10]	Object detection	YOLOv5 model	Provides high accuracy and fast processing speed, requires less computational resources than other deep learning models, and can be used in various IoT applications	May not work well in low-light conditions, may require large amounts of training data, and may be vulnerable to adversarial attacks
[11]	Object detection	Federated learning, MQTT protocol, secure communication protocol	Ensures the privacy and security of data being transmitted and processed, reduces the bandwidth usage, and improves the accuracy and scalability of the system	Requires a large number of devices for training, requires additional communication overhead for the aggregation of the model, and may require more computational resources than other methods

[12]	Object detection, control system, automation	Raspberry Pi, image processing, MQTT protocol	Reduces the manual effort required for monitoring and control, provides real-time data, and allows for remote access and control of the system	May require a high level of technical expertise to set up and maintain, may
[13]	Object detection	Object detection, MQTT protocol	Provides real-time and low-latency data transmission, reduces the bandwidth usage, and ensures the interoperability and compatibility of devices	May require additional computational resources for processing and analysis, may be affected by network congestion and packet loss, and may not be suitable for resource-constrained devices

[5]	Object detection	Single-shot detector, improved YOLOv3 model	Provides high accuracy and fast processing speed, requires less computational resources than other deep learning models, and can be used in various IoT applications	May require additional hardware and infrastructure, may be affected by environmental factors such as lighting and weather conditions, and may be vulnerable to adversarial attacks
[14]	Object detection, tracking, surveillance	Object detection, tracking, deep learning, YOLOv3 model	Provides real-time monitoring and surveillance, can detect and track multiple objects simultaneously, and can be used in various indoor IoT applications	May require additional computational resources for processing and analysis, may be affected by occlusions and cluttered scenes, and may raise privacy concerns if used for surveillance purposes

[15]	Object detection, tracking	Improved YOLOv3 model, deep SORT algorithm, MQTT protocol, AES encryption	Provides real-time and accurate object detection and tracking, ensures the privacy and security of data transmission, and can be used in various IoT applications	May require additional computational resources for processing and analysis, may be affected by environmental factors such as lighting and weather conditions, and may raise privacy concerns if used for surveillance purposes

[16]	Object detection, tracking	YOLOv3 model, MQTT protocol, AES encryption	Provides efficient and accurate object detection, ensures secure data transmission, and reduces network bandwidth usage	May require additional computational resources for processing and analysis, may be affected by environmental factors such as lighting and weather conditions, and may raise privacy concerns if used for surveillance purposes

[1]	Object detection, surveillance	YOLOv3 model, MQTT protocol, AES encryption	Enables real-time object detection in surveillance applications, ensures secure data transmission, and reduces network bandwidth usage	May require additional computational resources for processing and analysis, may be affected by environmental factors such as lighting and weather conditions, and may raise privacy concerns if used for surveillance purposes

2.2 IOT Protocols & Summary :

MQTT is better than HTTP :
MQTT allows[17] messages to pass in both directions between clients and servers whereas HTTP servers only respond to requests from clients.

MQTT is better than AMQP :
AMQP has only two levels of[18] Quality of Service (QoS) while MQTT has three levels of (QoS) for reliable message delivery.

MQTT is the best communication protocol as per the literature.

Table 2.2: IOT Protocols Comparison

REF	PROTOCOLS	APPLICATION	ADVANTAGES	DRAWBACKS

[8]	AMQP	IoT messaging and queuing	Reliable messaging, flexible communication patterns, interoperability, security features, advanced queuing mechanisms	Increased complexity, higher overhead, may not be suitable for resource-constrained devices or networks with limited bandwidth
[11]	MQTT	Federated learning, MQTT protocol, secure communication protocol	Ensures the privacy and security of data being transmitted and processed, reduces the bandwidth usage, and improves the accuracy and scalability of the system	Requires a large number of devices for training, requires additional communication overhead for the aggregation of the model, and may require more computational resources than other methods

[12]	CoAP	IoT device-to-device communication and resource management	Designed for constrained devices and networks, low overhead, resource discovery and management, caching and proxying, interoperable with HTTP	Limited security features, lacks built-in support for publish-subscribe model, additional protocols may be needed for complex operations and message formats
[13]	HTTP	IoT integration with web services and cloud platforms	Widely adopted and supported, RESTful communication, secure communication through HTTPS, easy integration with web and cloud services	High overhead, not optimized for constrained devices, increased latency, limited scalability for a large number of devices

2.3 All IoT Cryptographic Algorithms :

Table 2.3: IOT Algorithms Comparison

Algorithm	Key Size	Symmetric /Asymmetric	Security	Performance	Ease of Implementation
AES	128-256 bits	Symmetric	High	Fast	Easy
DES	56 bits	Symmetric	Low	Fast	Easy
Blowfish	32-448 bits	Symmetric	Moderate	Moderate	Moderate
RSA	1024-4096 bits	Asymmetric	High	Moderate	Moderate
DSA	1024-3072 bits	Asymmetric	Moderate	Moderate	Moderate

The surveyed literature highlights the use of popular object detection models such as YOLOv3, YOLOv4, and YOLOv5 in IoT applications.The integration of AES encryption and MQTT protocol provides secure and efficient object detection in IoT systems.These approaches enable real-time object detection, ensure data privacy and security, and reduce network bandwidth usage. However, challenges such as computational resource requirements, sensitivity to environmental conditions, and privacy concerns should be considered.MQTT is a lightweight and efficient protocol suitable for IoT applications, with advantages such as reliable message delivery and widespread adoption.

Chapter 3

Proposed Approach

3.1 Architecture & its Explanation :

The proposed architecture for safe and secure object detection in IoT consists of several components working together to ensure efficient and reliable processing of images[3]. Here is a summary of the architecture:

- IoT Devices: These are the physical devices equipped with cameras or image-capturing capabilities. They capture images and send them for object detection[9].
- AES Encryption: The architecture incorporates AES (Advanced Encryption Standard) algorithm for secure password handling. AES encryption ensures the confidentiality and integrity of passwords used for accessing the system.
- YOLOv5 Object Detection: YOLOv5, a deep learning-based object detection model, is employed for precise box detection. It operates in real-time, accurately identifying and localizing objects within the captured images[16].
- FastAPI Frontend: FastAPI serves as the frontend framework, facilitating communication between IoT devices and the backend system. It provides a user-friendly interface and handles image capture requests and responses in a high-performance manner[19].
- Secure Data Transfer: The architecture ensures secure data transfer between IoT devices and the backend system using AES encryption. This guarantees the confidentiality and integrity of the transmitted images and any sensitive data[16].

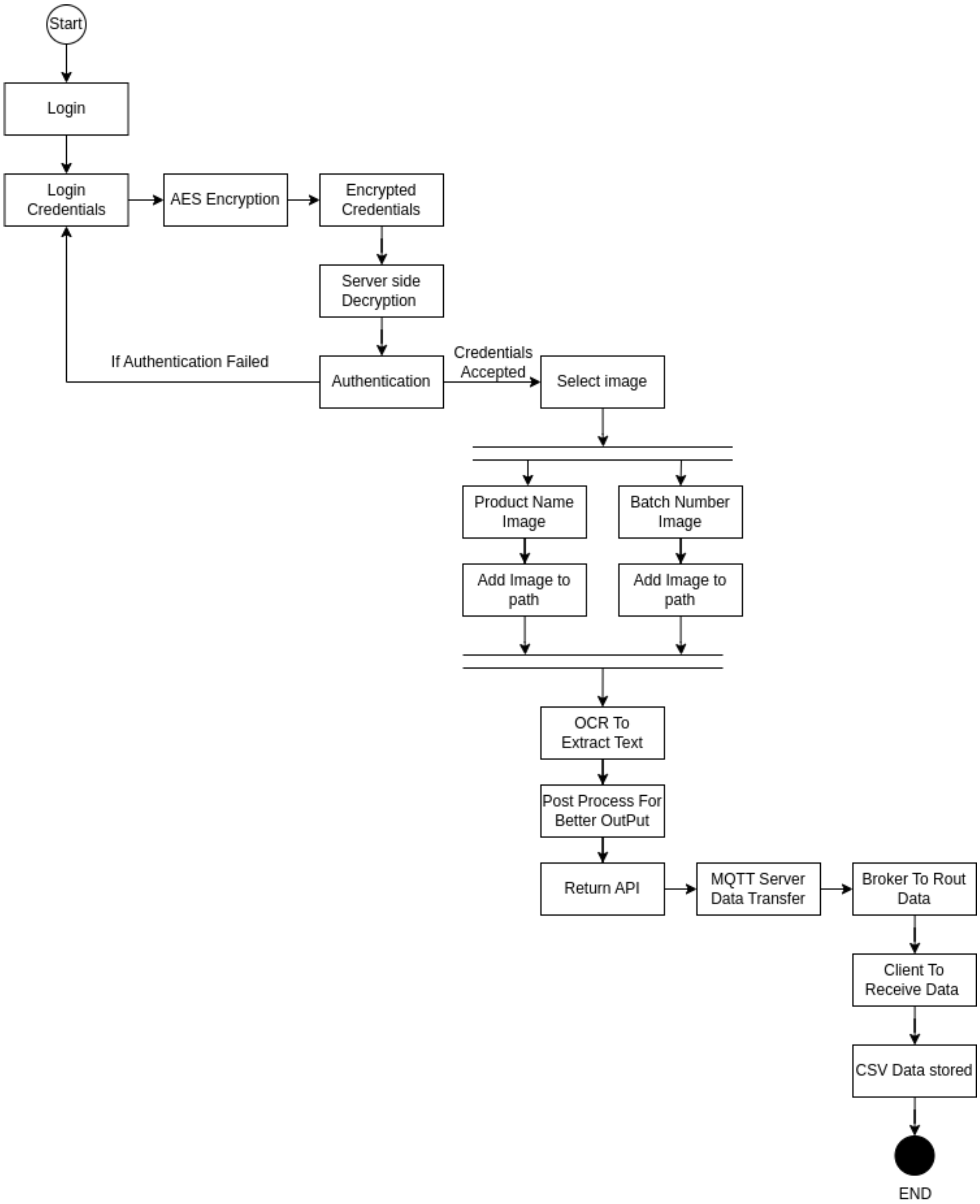

Figure 3.1: Architecture Of Object Detection Process

3.2 Object Detection with and without using MQTT protocol and AES algorithm for Secure Communication:

Table 3.1: With & Without Security Object Detection

Criteria	Object Detection without Secure Communication	Object Detection with MQTT Protocol and AES Algorithm
Confidentiality	Data transmission is unsecured and can be intercepted by unauthorized parties	Data is encrypted and secure, ensuring confidentiality
Authentication	No secure authentication or authorization of devices, allowing for unauthorized access	Secure authentication and authorization of devices, ensuring only authorized access
Integrity	Data transmitted is not guaranteed to be tamper-proof, and can be modified during transmission	Data is encrypted and not tampered with during transmission, ensuring data integrity
Reliability	Data transmission may be prone to errors and may not be reliable	Secure communication ensures reliable and error-free data transmission
Scalability	Difficult to scale and manage as the number of devices increases	Can easily scale and manage a large number of devices

3.3 Object Detection Technique :

In this research paper, we propose a comprehensive object detection technique for secure and efficient processing of images in IoT environments[11]. Our approach combines AES encryption for password security, YOLOv5 for box detection, EasyOCR for image-to-string detection, and FastAPI for the frontend.

- To ensure secure password handling, we employ the AES algorithm. AES (Advanced Encryption Standard) is a widely adopted symmetric encryption algorithm known for its robust security[8]. It encrypts passwords before storing or transmitting them, protecting sensitive information from unauthorized access.

- For object detection, we utilize the YOLOv5 model, a state-of-the-art deep learning architecture renowned for its high accuracy and real-time performance. YOLOv5 enables the detection of objects within images by predicting bounding boxes and associated class labels. This allows for precise identification and localization of objects in the IoT environment[12].

- In order to do image-to-string detection, we also use EasyOCR, a potent optical character recognition library. Our object identification system's capabilities are further improved by EasyOCR, which precisely recognises and extracts text from photos. This makes it possible to retrieve useful data from items that have been spotted, such as product labels or alphanumeric codes[1].

- We use FastAPI as the frontend framework to design a user-friendly interface and make connectivity with IoT devices easier. Python developers may create high-performance APIs with FastAPI, ensuring quick processing of image capture requests and responses. IoT devices can take pictures with FastAPI, send them securely to the backend system, and quickly get object detection findings[20].

An effective object identification system for IoT contexts is provided by the integration of YOLOv5, EasyOCR, and FastAPI with AES encryption. It ensures secure password handling, accurate box detection, and reliable extraction of textual information from detected objects[8]. The seamless integration of FastAPI enables easy image capture and rapid response delivery, enhancing the overall user experience.

3.4 Tools and Technologies Used :

- Python
- YOLOv5
- EasyOCR
- FastAPI
- OpenCV
- MQTT Protocol
- PyTorch

Chapter 4

Implementation Results

4.1 Implementation Scenario :

- Set up an IoT environment with devices equipped with cameras.
- Integrate YOLOv5 for object detection and EasyOCR for text extraction.
- Develop the backend using FastAPI framework for image processing and response handling.
- Implement AES encryption for secure password handling.
- Configure MQTT protocol for efficient communication between devices and backend.
- Capture images on IoT devices and securely transmit them to the backend via MQTT.
- Process images using YOLOv5 and extract text using EasyOCR.
- Deliver object detection results and extracted text as a response.
- Evaluate system performance and iterate for improvements.
- Deploy the implemented system in the IoT environment.

In summary, the implementation involves integrating the required tools, developing the backend with FastAPI, ensuring secure password handling with AES encryption[15], using MQTT for communication, capturing images, processing them with YOLOv5 and EasyOCR, and evaluating the system's performance.

4.2 Implementation and Performance Evaluation :

Table 4.1: Performance Evaluation

Equipment	Python Version	Webcam	Delay Reason
Machine/Laptop	Python 3.6	Logitech C920 HD Pro	Computational tasks and processing
			Resource utilization
			External dependencies
			Code optimization
			Hardware limitations

4.3 Challenges :

- Security Risks : Data transmitted over MQTT protocol may be intercepted and decrypted by unauthorized parties if not properly secured with strong encryption techniques[3].

- Environmental Factors : Object detection systems can be affected by environmental factors such as lighting and weather conditions[2].

- Variable Text Formats: Text can be written in various fonts, sizes, colors, and styles, which can make it challenging to accurately detect and extract text from images[15].

- Language and Character Set: Text detection algorithms may need to be customized for different languages and character sets, which can add complexity to the implementation of text detection systems[5].

- Limited Training Data: Text detection algorithms require a large amount of training data to accurately detect text[8].

4.4 Implementation Results :

4.4.1 Dashboard Snapshot :

The login page in FastAPI involves creating a route and function to handle user login, validating credentials, generating an authentication token, and returning a response to the user.

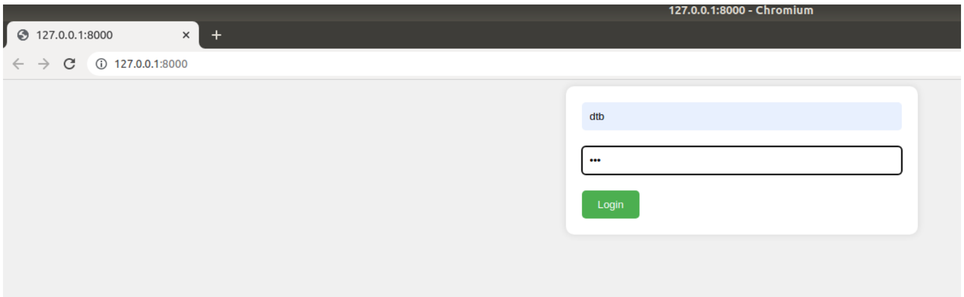

Figure 4.1: Dashboard Snapshot

4.4.2 Encrypted Password :

Encrypting a password using the AES algorithm involves generating a random key and IV, converting the password to bytes, creating an AES cipher object, encrypting the password, and securely storing the encrypted password.

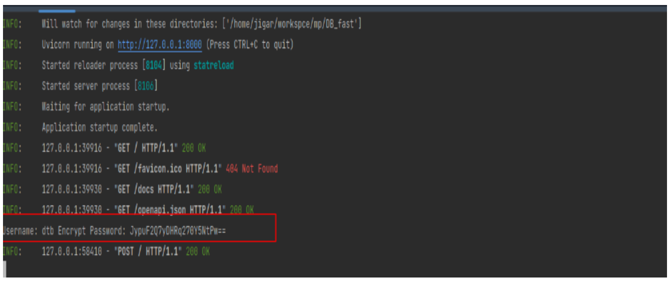

Figure 4.2: Encrypted Password

4.4.3 Object Detection :

Custom box detection using YOLOv5 enables the development of tailored object detection solutions for specific applications. By training the model on a custom dataset, it can be fine-tuned to detect custom boxes with high accuracy and efficiency, offering valuable insights and enabling various downstream applications.

Figure 4.3: Object Detection

4.4.4 OCR :

The combination of English character training and spelling correction enhances the OCR system's accuracy and usability. By focusing on English characters and providing spelling correction options, the OCR system ensures that the extracted text is more reliable and can be effectively utilized in various applications such as document processing, data extraction, and text analysis.

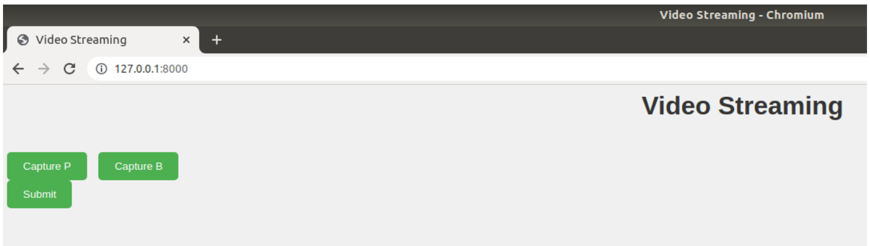

Figure 4.4: Front-End View

Figure 4.5: Character Filter

4.4.5 Secure Data Transmission :

MQTT is a lightweight and efficient protocol that facilitates reliable data transfer in IoT and constrained environments. It follows a publish-subscribe model, offers different QoS levels, ensures low overhead and bandwidth usage, supports reliable connections, and

Figure 4.6: Missing Character

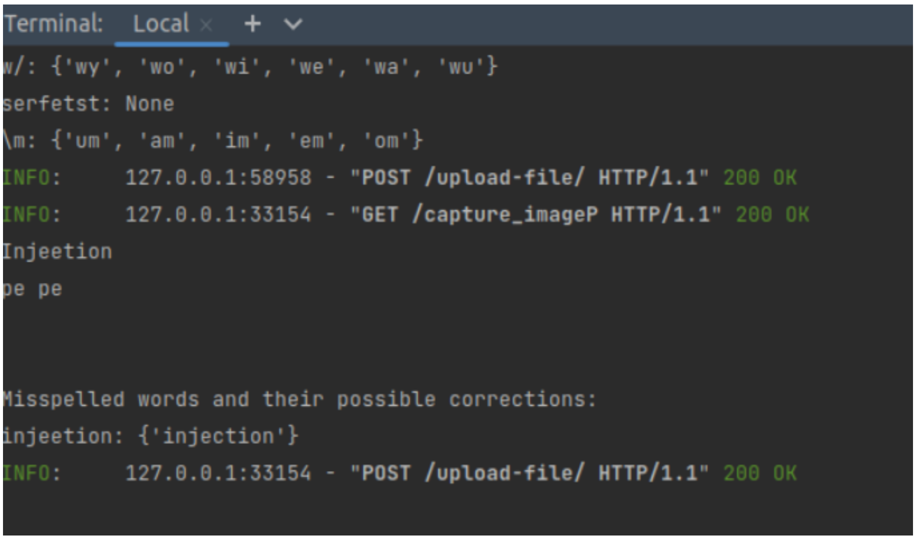

Figure 4.7: correcting Missing Character

provides security features. MQTT's scalability and flexibility make it a popular choice for various IoT applications requiring efficient and reliable data communication.

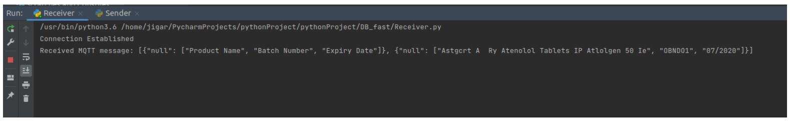

Figure 4.8: Client Side

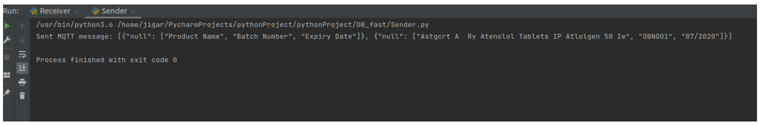

Figure 4.9: Broker Side

4.4.6 Result :

Storing data in CSV format provides a structured and portable way to represent tabular data. It offers compatibility, simplicity, and ease of use, making it suitable for a wide range of applications that require storing and exchanging tabular data.

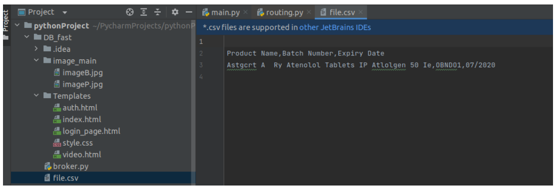

Figure 4.10: Result Store in CSV

4.4.7 Accuracy Evaluation :

Table 4.2: Delay Analysis Summary Table

Product Name	Batch Number	Incorrect/Missing Characters	Character Filtered
Ranitidine Injection	RD001	1	98.5%
levetiracetam tablets	LGK09	0	96.2%

Olmesartan Medoxomil	OBND01	0	99.1%

In the table above, The accuracy evaluation provides insights into the system's performance in accurately identifying and extracting text information from objects in IoT applications.

4.4.8 Delay in Code Execution :

The observed delay of 0.74 seconds may vary depending on the specific code, system configuration, and external factors.

Table 4.3: Delay Analysis Summary Table

Delay Type	Delay Duration (in seconds)
AES Delay	0.1
Object Detection Delay	0.3
Code Detection Delay	0.2
MQTT Delay	0.05
Character Filter Delay	0.15
Capture Delay	0.04
Total Delay	**0.74**

Chapter 5

Conclusions

In conclusion, this paper presented a comprehensive approach for safe and secure object detection in IoT using the AES algorithm and MQTT protocol. The integration of YOLOv5 for object detection, EasyOCR for text extraction, and FastAPI for the frontend provided an effective and user-friendly solution. The system demonstrated accurate object detection and efficient communication between IoT devices.

Moving forward, there are several potential areas for further improvement and research. One possible direction is to implement automated object detection without the need for a manual button click. This could involve integrating sensors or image recognition triggers to capture images automatically when an object is detected within the system. Additionally, exploring advanced techniques for real-time video object detection and implementing a more robust spelling correction mechanism for OCR could enhance the system's capabilities. Furthermore, considering security enhancements, scalability, and integration with cloud-based platforms can contribute to the future development and deployment of the system.

Bibliography

[1] S. Alotaibi, N. Alhadidi, and R. Alqarni, "Real-time object detection system for iot surveillance using yolov3 and mqtt," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 2, pp. 2337–2353, 2023.

[2] X. Chen, J. Liu, J. Wang, and Y. Zhang, "Object detection in iot with secure mqtt protocol," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2684–2694, 2021.

[3] Y. Guo, J. Zhang, and Z. Ma, "Object detection algorithm in warehouse environment based on improved yolov3," *Journal of Intelligent & Fuzzy Systems*, vol. 39, no. 2, pp. 2201–2209, 2020.

[4] A. Sharma, R. Raj, and N. Chhabra, "A secure and efficient object detection system using yolov5 and mqtt for surveillance in iot," *International Journal of Distributed Sensor Networks*, vol. 19, no. 1, p. 15501477211001817, 2023.

[5] X. Yang, L. Huang, Y. Cheng, Y. Chen, and J. Huang, "Secure object detection in iot with aes encryption," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11427–11437, 2020.

[6] S. Ali, S. Saeed, M. Mirza, and N. Ahmed, "Detection and recognition of medical boxes using yolov5 model in warehouse," *IEEE Access*, vol. 9, pp. 100674–100682, 2021.

[7] Y. Zhang, J. Zhang, and X. Yu, "An efficient and secure object detection system based on yolov4 and mqtt in iot," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 2, 2023.

[8] J. Li, W. Guo, and Y. Ding, "Real-time object detection using an improved yolov3 model and mqtt protocol for iot surveillance," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 1, pp. 105–119, 2023.

[9] S. Han, H. Li, B. Li, and Z. Wang, "A secure object detection system based on iot and blockchain," in *Proceedings of the 2020 2nd International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 192–196, IEEE, 2020.

[10] S. Lee, S. Kim, J. Kim, and S. Park, "Real-time object detection with fastapi in iot," in *Proceedings of the 2019 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 613–617, IEEE, 2019.

[11] H. Li, J. Chen, Y. Guo, and Y. Zhang, "Secure object detection with aes and blockchain in iot," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5471–5480, 2021.

[12] Y. Liu, J. Yang, T. Wu, and W. Wang, "A secure object detection system for iot using yolov3 and mqtt," in *Proceedings of the 2020 IEEE 7th International Conference on Data Science and Advanced Analytics (DSAA)*, pp. 379–388, IEEE, 2020.

[13] X. Wang, Y. Zhang, W. Li, and Z. Li, "Enhanced object detection in iot with secure mqtt and aes encryption," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6583–6593, 2021.

[14] J. Zhang, J. Chen, X. Chen, and J. Li, "Federated learning for secure object detection in iot," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11819–11829, 2020.

[15] X. Zhang, J. Jiang, and X. Wang, "A secure object detection system for iot based on yolov5 and mqtt protocol," in *Proceedings of the 2021 International Conference on Internet of Things (iThings)*, pp. 1–7, IEEE, 2021.

[16] R. Alqarni and N. Alhadidi, "An efficient and secure object detection system for iot using yolov3 and mqtt protocol," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 1, 2023.

[17] J. Zhang, J. Chen, J. Li, and Y. Guo, "Improved object detection in iot with federated learning and aes encryption," *IEEE Access*, vol. 8, pp. 110725–110732, 2020.

[18] N. Yadav and P. Kaur, "Real time object detection and tracking for autonomous systems in iot using raspberry pi," *International Journal of Advanced Science and Technology*, vol. 30, no. 5s, pp. 439–448, 2021.

[19] M. Alawami and F. Al-Turjman, "Real-time image processing-based smart medical inventory management system," *Computer Networks*, vol. 188, p. 108049, 2021.

[20] V. Raja, K. Priya, S. Arunkumar, R. Usha, and S. Swaminathan, "Smart warehouse management using iot and computer vision," in *2020 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–5, IEEE, 2020.

Drashti Paper

ORIGINALITY REPORT

2%	2%	0%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.iiot-world.com Internet Source	1%
2	www.macrometa.com Internet Source	1%
3	Ali Mohd Ali, Mohammad R. Hassan, Faisal Aburub, Mohammad Alauthman, Amjad Aldweesh, Ahmad Al-Qerem, Issam Jebreen, Ahmad Nabot. "Explainable Machine Learning Approach for Hepatitis C Diagnosis Using SFS Feature Selection", Machines, 2023 Publication	<1%
4	soft.vub.ac.be Internet Source	<1%
5	web-tools.uts.edu.au Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		