RE-2022-110102-plag-report

by Research Experts - Turnitin Report

Submission date: 13-Apr-2023 12:10PM (UTC-0400)
Submission ID: 2063577181
File name: RE-2022-110102.docx (768.87K)
Word count: 6992
Character count: 38920

Smart drone delivery system and face recognition using CNN

Malay Rajpoot
School of Electronics Engineering
Vellore Institute of technology
Vellore, India
malay.rajpoot2020@vitstudent.ac.in

Shreyas GT
School of Electronics Engineering
Vellore Institute of technology
Vellore, India
shreyas.gt2020@vitstudent.ac.in

Veerayya Vastrad
School of Electronics Engineering
Vellore Institute of technology
Vellore, India
Veerayya.vastrad2020@vitstudent.ac.in

Achinthya R H
School of Electronics Engineering
Vellore Institute of technology
Vellore, India
achinthyahemmanna.r2020@vitsent.ac.in

Dr. K.C. Sriharipriya
School of Electronics Engineering
Vellore Institute of technology
Vellore, India
sriharipriya.kc@vit.ac.in

***Abstract*—Although it is an essential responsibility, real-time parameter monitoring of products in smart delivery systems is difficult because of the volume and movement of the products. In order to overcome these difficulties, the Internet of Things (IoT)-based smart delivery system is presented in this study. Using different IoT-based protocols like MQTT, LWM2M, CAN, etc., the system enables managers and customers to keep track of all real-time product parameters during the delivery process. In addition, the suggested system makes use of optimal control algorithms, compact, low-power sensor nodes, and lifetimes of 286 days for fixed nodes and 40 days for mobile nodes, respectively.**

***Index Terms*—Internet of Things (IoT), Face Recognition, Protocols, MQTT, LWM2M, CAN**

I. INTRODUCTION

The Internet of Things (IoT), a crucial element of the fourth industrial revolution, has attracted a lot of interest in recent years. The potential of IoT has been studied in a number of industries, including healthcare, transportation, and smart infrastructure. However, the high demands and operating environments of these applications necessitate that equipment be ideally constructed in order to function at its best. IoT use in smart distribution systems is one very pertinent application. It is critical to provide correct storage conditions throughout transit as consumers increasingly depend on these systems to deliver a variety of commodities, including those with severe storage needs like vaccinations and frozen goods. To avoid incidents and guarantee on-time delivery, a smart delivery system that can monitor necessary parameters and issue alerts when conditions are not met is essential.

II. LITERATURE REVIEW

In [1], da Silva advocates leveraging the Message Queuing Telemetry Transport (MQTT) protocol to build a powerful platform for UAV control with inbuilt Denial-of-Service (DoS) detection. The platform's latency, network, and memory use were all scrutinised for the efficiency test's payload and delay time correlation. The efficiency test results for the three levels of quality services (QoS) were compiled. A high correlation of more than 90% was found between delay and data size for all QoS levels, showing a roughly linear connection. The best results for DoS detection were a true positive rate (TPR) of 0.97 employing 16 features from the AWID2 dataset when using LightGBM with Bayesian optimisation and data balancing. The developed platform shows effectiveness for UAV control and ensures security in communications with the broker and inside the Wi-Fi UAV network, in contrast to past research.

The authors of [2] have discussed the evolution of object detection using deep learning based on drone camera research. Our research's overarching goal is to provide patients with critical medical aids in urgent situations. The situation can be reduced to the delivery of a good from the starting point to the final place. We'll take advantage of drone technology to move things quickly. In sending process, our drone must detect the object target where the items will be delivered. We therefore require an object detection module that can identify objects in the video stream and also determine their location using GPS. For a quick and effective deep learning-based approach to object recognition, we combine MobileNet and the Single Shot Detector (SSD) framework to create the module. By conducting studies with drone cameras and, as a comparison, stereo cameras, the capability of deep learning to recognize and localize specific objects is explored.

A face identification system based on near infrared (NIR) image was presented by the authors in [3]. They begin by describing an NIR image capturing device design that reduces the impact of ambient lighting on facial images. Using local features and AdaBoost learning, face recognition and localization of facial features are both accomplished. A review of the system's performance in a real-world user scenario reveals that it excels in terms of accuracy, speed, and usability.

According to [4], computer vision-based licence plate recognition is a great way to replace the human eye's manual identification of licence plates. In actual use, the algorithm for reading licence plates must be resistant to a variety of plate orientations, sounds, and illuminations. Traditionally, segmenting the detected plate's characters is one of the difficult tasks. To conduct recognition, the segmented characters are extracted. Thus, how a character segment performs has an impact on the outcome. This study uses a sliding window with bounding box refinement and character detection using a convolutional neural network (CNN) to segment the characters on an Indonesian licence plate. The character and non-character regions are distinguished using this proposed method using CNN. CNN is fed by using the sliding window approach. To improve accuracy, the bounding boxes are finally refined. Additionally, 130 images of Indonesian automobile licence plates with a total of 982 characters were used to evaluate the constructed model, and the accuracy rate was 87.06 percent. In [5], V. -L. Dao and V. -P. Hoang demonstrate a smart delivery system utilising IoT. By utilising the MQTT protocol, the suggested system provides real-time tracking of product characteristics throughout the delivery process. Additionally, it has small, power-efficient sensor nodes that are compact, and it uses the best control algorithms to give stationary and mobile nodes longer lifespans of 286 days and 40 days, respectively. In [6], the authors review the development of M2M protocol research during the previous 20 years with an emphasis on MQTT, AMQP, and CoAP. Through a thorough literature search, it illustrates the outstanding growth of MQTT research in comparison to the competition and presents relevant application areas for MQTT, the most popular M2M/IoT protocol. In order to examine the main characteristics, benefits, and limits of the MQTT protocol, the article also offers a quantitative review of significant MQTT-related studies from the previous five years and compares them. To help academics and end users choose the best solution based on their needs, it also suggests a taxonomy for comparing the properties and features of various MQTT implementations, such as brokers and libraries. The study then examines the comparison's results and identifies any outstanding questions that still need to be investigated. By introducing a client-side design for LWM2M and its implementation framework on Contiki-based IoT nodes, the authors of [7] provide a solution to these problems. The proposed LWM2M client engine architecture and its interfaces are highlighted along with a lightweight IoT protocol stack. The implementation supports OMA, IPSO, and third party objects and complies with the just-released OMA LWM2M v1.0 specification. The usability and efficacy of the suggested solution are assessed using a real-world application scenario. The findings show that the client-side IoT protocol stack's memory footprint overhead induced by the addition of LWM2M is approximately 6.9%, making it appropriate for Class 1 restricted device types. The MQTT and LwM2M communication protocols for IoT devices are compared and discussed in [8], together with their distinct characteristics, underlying ideas, software implementations, and appropriate use cases. It can be difficult to choose the best IoT communication protocol for a certain application. Based on specific characteristics, planned applications, and the overarching idea of the IoT protocols, a comparison is established. The significance of selecting the appropriate protocol based on the particular application is emphasised throughout the paper. The performance of LwM2M and MQTT, the two most popular protocols for Internet of Things applications, when utilised with LTE-M and NB-IoT is examined and compared in [9]. By keeping track of the exchanged packets and bytes, the tests calculate the traffic produced by the two protocols. Additionally, it looks at how the two protocols' usual energy usage impacts the end devices' working times in common IoT use scenarios. The effectiveness of the protocol is further examined in relation to authentication techniques and cellular network characteristics. The report concludes by offering guidelines for selecting LwM2M and MQTT protocols in IoT networks. [10] outlines two LwM2M extensions that allow client-to-client (C2C) communication. These extensions include a client authorisation system and an enhanced administration interface for secure resource access. The security characteristics of the suggested extensions are examined, and it is demonstrated that they meet LwM2M security criteria. C2C communication outperforms server-centric installations, according to a performance evaluation using commercial IoT hardware. The analysis shows that compared to typical server-centric situations, LwM2M deployments with edge C2C connectivity result in notification delivery times that are 90 percent faster and throughput that is eight times greater. This is achieved with only an 8 percent memory overhead. Additionally, when resource update intervals fall below 100 ms in server-centric communication, the delivery rate falls. In [11], the authors compares the performance of MQTT- SN and LWM2M communication protocols in the transmission of messages. The analysis was conducted using the Node- RED tool, which uses flow-based programming for runtime evaluation and performance analysis. The results of the simulation showed that the MQTTSN protocol performed better in the tests conducted. This study compares the performance of MQTT-SN and LWM2M communication protocols in the transmission of messages. The analysis was conducted using the Node-RED tool, which uses flow-based programming for runtime evaluation and performance analysis. The results of the simulation showed that the MQTTSN protocol performed better in the tests conducted. In [12], The authors describes a message exchange model based on REST API and a new synchronization technique for microservice replicas, aimed at enhancing the availability and scalability of an existing LwM2M solution, implemented as a microservice. In [13], The authors explains the CAN Protocol and its application in various types of vehicles. CAN, or Controller Area Network, is a method of communicating between microcontrollers and other devices through the use of a CAN bus. The network topology is robust, able to detect faults without impacting the entire system. Additionally, the CAN Protocol is message- based. In the automotive industry, it is utilized in the form of a device called a CAN transceiver module. In this study, four types of sensors were employed, including an alcohol sensor, temperature sensor, fuel level sensor, and distance mea- surement sensor, with the purpose of preventing and avoiding accidents. In [14], The authors of this paper have developed an automated Patient Management System (PMS) for hospital wards that uses Zigbee Technology and the CAN Protocol. The PMS consists of a wireless component, including a wearable device and a coordinator node, and a wired component, comprising a coordinator node linked to a base station node through the CAN bus and a Central Monitoring Station (CMS) that uses LabVIEW software. The wearable device utilizes the GY-MAX30100 and Fever Click MAX30205 development boards to measure vital signs, such as heart rate (HR), oxygen saturation (SpO2), and body temperature. These boards have been tested and found to have acceptable levels of accuracy compared to CE-marked medical devices, such as the Pulse Oximeter MD300C1 and Digital Thermometer DT-111A. Testing of the wearable device and coordinator node for sending and receiving vital sign data showed a 100 percent reliability rate, even in non-line-of-sight (NLOS) conditions, for distances up to 40 meters. The CMS had an average response time of 1.3 seconds and was able to detect abnormal vital signs. Finally, a simulation with four volunteers demonstrated the functionality and effectiveness of the system for use in a multi-patient setting. In [15], this paper the authors examine Ice pilots that primarily rely on visual observation to avoid icebergs, but if the ship is equipped with ice radar, it is still necessary for the pilot to see the iceberg in order to make a decision. During blizzards or smog, the ship must be halted until visibility is restored. To address these issues, a model is proposed to detect icebergs in the sea and implement preventative measures. In [16], Despite being widely used in vehicles, the Controller Area Network (CAN) protocol can present significant security risks due to its lack of encryption and authentication. The literature has reported a growing number of attacks related to the CAN bus as cars become increasingly connected. The authors provides an overview of the CAN protocol and examines its security vulnerabilities. Additionally, it surveys the various attacks and solutions that have been proposed in the literature. In [17], The authors of this study aim to integrate an advanced sensor for detecting haemolysis and pH levels into the Smart Capsule, a previously developed technology for managing blood transportation via drones. The haemolysis is identified using an optical minilysis device that uses a combination of LED and photodetector. The initial evaluation of the Smart Capsule and the haemolysis detection capabilities of the minilysis device prototype was conducted to assess thermal stability. The onboard temperature test demonstrated that the delivery system can maintain the appropriate temperature, even when the samples were subjected to higher temperatures before being placed in the Smart Capsule. The laboratory haemolysis test also demonstrated that there is a linear regression trend between the outputs of the spectrophotometer and the minilysis prototype, thus validating the design of the minilysis device. In [18], A new delivery system for mail, called DroneTalk, is being proposed by K. -W. Chen, M. -R. Xie, Y. -M. Chen, T.T. Chu and Y. -B. Lin. This system utilizes IoT technology and drones for delivery. DroneTalk utilizes a GPS, inertial measurement unit, and visual information to allow for mixed indoor-outdoor navigation. Additionally, it incorporates an IoT device management platform for the drone to automatically be aware of weather conditions. It also addresses issues of communication, processing, and control latency to prevent collisions during autopilot operation, especially when flying close to buildings. Simulation results have shown that the system can achieve a high success rate, making it practical for real-world use. In [19], P. Das, S. Bhaumik and S. Nath in this paper investigates the use of image transformation techniques and AI to distinguish between authentic and forged signatures. By utilizing grass-fire transformations and optical flow, it examines the differences in signatures. The proposed system employs a deep learning framework with ResNet 50 and a Convolutional Neural Network (CNN). The system is also evaluated and compared to existing literature using SVC2004 and SUSIG benchmark datasets. In [20], E. A. Soelistio, R. E. Hananto Kusumo, Z. V. Martan and E. Irwansyah in this study investigate two issues and determine the most effective algorithms for identifying signatures based on their type. The research employs a systematic literature review using a PRISMA flow diagram. The findings suggest that offline signatures primarily utilize Convolutional Neural Networks (CNN) for recognition, while online signatures mostly use Recurrent Neural Network (RNN) in combination with other architectures. In [21], F. Noor, A. E. Mohamed, F. A. S. Ahmed and S. K. Taha present a dependable technology that organizations can use to automatically identify signatures. The study trains convolutional neural networks on preprocessed signature images. The implementation is done using MAT- LAB, and the results indicate that the method is effective. The CNN was tested using 4 datasets, each containing N individuals and M signatures per individual. These datasets include a variety of signature types and readability levels. The network performed well on all datasets. The study also makes observations on the performance of the implementation. In [22],this research shows the Local Binary Pattern Histogram method is used by M. Saravanan and K. Kowsalya for facial recognition. To improve training performance, data augmentation is also applied. Features such as eyes, nose length, cheeks, and lips are extracted using the Haar cascade method. A database of individual's grayscale images is created by initially capturing images using a web camera. The classifier then trains on these images, with data augmentation being employed when there is a lack of sufficient data for a person. Once trained, the system uses the web camera to detect and recognize individuals, sending a message to WhatsApp with the recognized person's information. In [23], Ahmed Barnawi, Prateek Chhikara, Rajkumar Tekchandani, Neeraj Kumar, and Mehrez Boulares have presented a novel approach for detecting COVID-19 cases in hospitals using deep convolution neural architecture with transfer learning. The proposed model classifies patients into three categories based on X-ray images: COVID-19 (positive), normal (negative), and pneumonia. The model is compared with existing state-of-the-art models, and the results demonstrate an accuracy of 94.92 percent. Additionally, to provide timely services to COVID-19 patients, the authors propose a scheme for delivering emergency kits to hospitals in need using an optimal path planning approach for UAVs in the network.

In [24], This study proposes improvements to the FPN network for commodity image detection and classification. Specifically, the DPFM ablation and RFM are used to enhance detection accuracy, while the GTNet network is developed to improve classification accuracy. Results show that the dpFPN-Netv2 algorithm with DPFM + RFM fusion outperforms other algorithms in terms of target detection accuracy and has a faster detection time of 52 ms compared to 90 ms required for RetinaNet-50 detection. Additionally, the improved MWI DenseNet neural network shows a significant reduction in computation while improving recognition accuracy, compared to the traditional MWI-DenseNet network. The study's innovation lies in its approach of improving both target detection and recognition simultaneously, rather than focusing on one aspect alone. In [25], Mohamed Amine Ferrag and Leandros Maglaras have proposed a novel system for drone-delivered services, which utilizes an intrusion detection system (IDS) and a blockchain-based delivery framework called Delivery Coin. The Delivery Coin framework comprises four key phases, including system initialization, block creation, blockchain updating, and intrusion detection. To ensure privacy preservation, the framework uses hash functions and short signatures without random oracles, as well as the Strong Diffie-Hellman (SDH) assumption in bilinear groups. The authors proposed a UAV-aided forwarding mechanism called pBFTF to achieve consensus within the blockchain-based delivery platform. Moreover, they suggest an IDS system in each macro eNB (5G) to detect false transactions between self-driving nodes and self-driving network attacks.

III. Proposed Methodology

A. *The following things were accomplished in our project:*

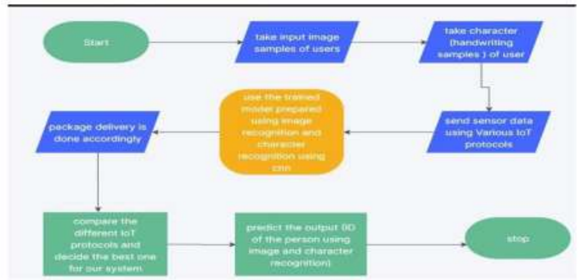

Fig. 1. block diagram of the project

1. An AI based face recognition system was created so that we ensure greater security of thedelivered goods 2. Various Iot protocols like MQTT, LWM2M, CAN etc. were compared and the best one in terms of efficiency and performance was decided. 3. An IoT Platform was connected to and data was uploaded on it so that it is readily available for use by both user and manufacturer.

IV. PROPOSED MODEL AND WORKING

A. *Introduction*

The proposed model for the Smart Drone Delivery system involves the use of machine learning algorithms, specifically Convolutional Neural Networks (CNN), for character recognition and face recognition. The system will be built using a Raspberry Pi and a camera module for capturing images and characters as inputs.

The process of the system begins with capturing an image of the person and the package to be delivered. The image is then processed using CNN to recognize the face and the characters in the package label. If the face recognition matches the person who placed the order, the system will open the door using a servo motor to deliver the package.

To transmit data from the Raspberry Pi to the IoT platform, the system uses the Nodemcu module that is connected to the Raspberry Pi serially. The Nodemcu module is used to establish a Wi-Fi connection and then sends data to the IoT platform.

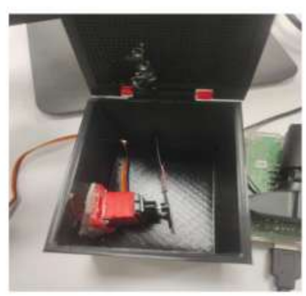

Fig. 1b. The servo mechanism to lock or unlock the box

The following is a detailed explanation of the algorithm used and the protocols used in transmitting data:

- Character Recognition using CNN: The character recognition algorithm is implemented using CNN. The input image containing the characters in the package label is passed through the CNN model. The model is trained on a large dataset of character images, which enables it to accurately recognize the characters. Once the model recognizes the characters, it is compared to the actual characters in the package label.
- Face Recognition using CNN: The face recognition algorithm is implemented using CNN. The input image containing the person's face is passed through the CNN model. The model is trained on a large dataset of face images, which enables it to accurately recognize the face. Once the model recognizes the face, it is compared to the face of the person who placed the order.
- Protocols used in transmitting data: To transmit data from the Raspberry Pi to the IoT platform, the system uses the Nodemcu module. The Nodemcu module is connected to the Raspberry Pi serially, and it is used to establish a Wi-Fi connection. Once the Wi-Fi connection is established, the system sends data to the IoT platform using the MQTT protocol. The MQTT protocol is a lightweight messaging protocol that is ideal for IoT applications. It enables the system to send data to the IoT platform efficiently and securely.

B. *working*

Our focus is to detect and recognize the face of a person. The programming language chosen for this project is Python because it is a versatile language that provides concise and easy-to-read code. Despite the complexity of algorithms and workflows required for machine learning and AI, Python's simplicity enables developers to create reliable systems.

For explaining the working of face-recognition algorithms we would mostly use this image of a model displayed in figure 2.

C. *Finding the face*

For face detection, we, are using histograms of oriented gradients, or just HOG for short. We start by making the whole image black and white because we don't actually need colour to find a face. It can be seen from figure 2 that we have successfully filtered the image to its black-and-white.

We then look at every pixel and the pixel surrounding a particular pixel. After that we try to find the direction of the pixel through which the image is getting darker. We would then make an arrow to represent this direction.

When this same process is repeated for every pixel in the image, every pixel is replaced with an arrow thesis arrows are called gradients. They show the flow from light to dark across the entire image. Pixels of the same person analyzed in different lighting conditions give different results or pixel values thus making them separate images to analyze. But by making them into gradients both the darkest and the lightest image will end up with the exact same pattern thus making our job much easier.

In the output image (figure 3) given below, it could be observed that we have obtained the gradient of the given face. One can observe it is oddly similar to outlining the facial feature of a face.

Fig. 2. Model Image

Fig. 3. Black and White Image

Fig. 4. Gradient Image

We have referred to the radiant-based technique for image structural analysis and applications for this[1].

D. *Posing and Projecting Faces*

The proposed method would only work for facing looking straight into the camera. But if the photo is given from side profile, then there might be an issue. To tackle this, we would find 68 points that exist on every face-the top of the chin, the outside of the eye, the inner edge of each eyebrow, etc. These landmark features can be seen in figure 4. Then we will train the machine to find these points on the face. Now that we have obtained eyes and mouths we will simply resize and rotate the image such that they do not distort and keep their parallel lines as well. Now no matter the direction the face is captured, we are able to center and reposition the image such that our algorithm of HOGs works on it. Below we have again shown this with the same picture of the model. As seen in figure 6 we have successfully obtained the landmarks of the face. [3]

Fig. 5. Figure 4 All 68 landmarks

Fig. 6. Facial Features Outline

As seen in figure 5 we have successfully obtained the landmarks of the face. [2]

E. *Encoding faces*

We don't need to compare the entire image with each other. We could extract only certain measurements and compare them between the known and unknown images and recognize the faces with the closest measurement. Encoded values of figure 1 have been obtained and displayed in figure 6. We woulduse deep learning and let the computer decide itself which measurements make the most sense to it. We would repeat the same step as we did in step 2. But instead of finding locations of each object we are going to train it to find 128 measurements of the face.

We do this by giving the machine three different images:
1. Image of the known person 2. Another image of the same person 3. Image of a totally different person

So in this project we have just used the pre-trained network to get the 128 measurements for our test image. [3]

F. *Finding name of the person*

We now need to compare the obtained measurements with the measurement in our database and extract the name of the person from the database with which it has the closest match. We simply use a linear SVM classifier for this task. As can be seen in figure 6, it has successfully detected the person in the image and given the name of the said person from the database that it had been given.

Fig. 7. Recognised and Detected Face

G. EXPERIMENTAL SETUP

A. *Finding the coordinates for Arduino and servo motors*

Our idea is that the camera shall move with the recognized person's face to a certain extent as it can have several applications on its own that we have discussed later.

To do this we have used a simple serial in and serial out of data between our classifier and the servos. We used an Arduino UNO to communicate with the servos.From OpenCV, we extract the cartesian coordinates of the detected and recognized image with height and width. With these values we calculate the center of the image by simply using the equation:

When a face is detected, the system passes the corresponding coordinates to an Arduino UNO microcontroller through the pyserial library. The frame contains a white square at its center which indicates the

region where the center of the detected face (represented by a green dot) should be located. If the face moves outside of this region, the system uses a servo to adjust the camera's position and bring the face back within the square region. To command the Arduino using python we have referred to the research work from Microcontroller programming with Arduino and Python [22].

B. *System Design*

As it can be seen from the figure 7 schematic we have connected the "Horizontal" or x-axis servo motor to pin 6 of the Arduino and the "Vertical" or y-axis servo motor to pin 5. Arduino is grounded and connected to PC using an USB port.

Information of the coordinates is generated by the python code is passed to Arduino which then instructs the servo motors to align themselves according to it.

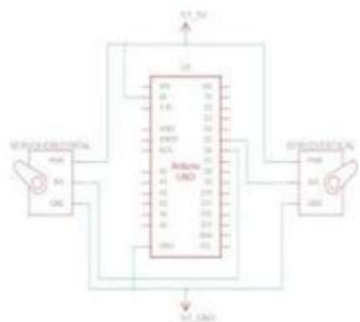

Fig. 8. Schematic Diagram

Figure 8 demonstrates our experimental setup which consists of servos, breadboard, wires, gimble and HP webcam.

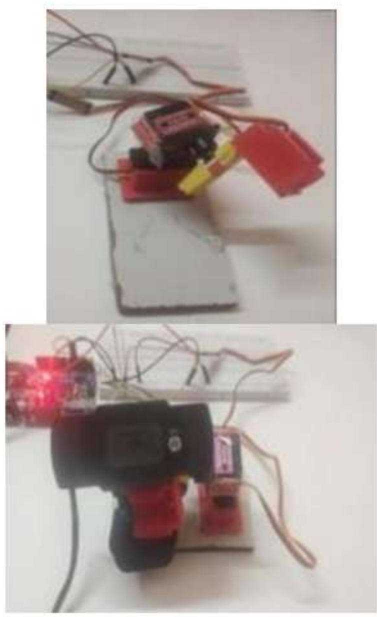

Fig. 9. Working model

For moving the camera to follow the face using Arduino we are using cartesian coordinates obtained from the rectangle that is created across the scanned face. Also we used a PID controller to smoothen the outputs as the Arduino gets 60 different results per second from a 60 FPS camera. Figure 14 shows the coordinates obtained from the image. Camera tries to keep the green dot inside the white square around which we have detected the face.

The camera and gimbal setup are controlled by servos. The gimbal tries to align to the center of the face.

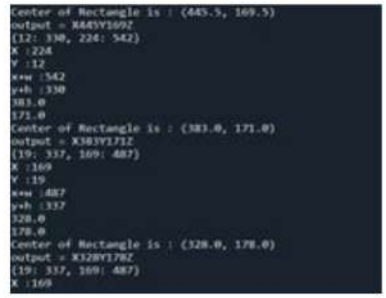

Fig. 10. Arduino Inputs from Scanned face

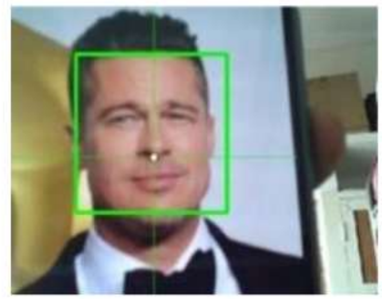

Fig. 11. Scanned Face

C. Access Control System using Face Recognition

We developed an access control system by integrating Facial recognition using HOG's and the face follower using Arduino. The model comprising of HOG and Linear SVM classifier is trained using set of images in the dataset shown in figure[11]. These algorithms are implemented using dlib library for face recognition in python.

Fig. 12. Dataset of Trained Images

Our developed system will only recognise faces that were trained and store the Name of the recognised person, timestamp and permission status into a CSV file [Figure 12]. This generated csv will be useful for storing records and enhancing security of the system

2			
3	WILL SMITH	23:10:52	Access granted
4	ANGELINA JOLIE	23:24:54	Access granted
5	BRAD PITT	23:25:12	Access granted
6	LEONARDO DICAPRIO	23:25:34	Access granted
7	MEGAN FOX	23:26:44	Access granted
8			
9			

Fig. 13. Raw Data converted into a CSV file

Fig. 14. Recognized Face

A comparison of different designs for these applications has been presented in Table I [1]. To reduce system power consumption, ultra-low power microcontrollers (MCUs) have been preferred, with the MSP430 family from Texas Instrument (TI) being a popular choice [10, 13]. Different wireless transmission modules, such as Wi-Fi, Bluetooth, and Radio Frequency (RF) modules, have been used with different protocols. The authors in [5] presented a comparison of these modules to identify the best option for a specific application. Wi-Fi modules are expected to cover most areas in smartcities, and hence should be used as transceivers in applicationsrelated to WSN, WBAN, and IoT. The selection of sensors foreach application is based on their functions, aiming to achievethe lowest power consumption and highest accuracy. While various communicative modules have been used with different protocols, MQTT protocol has gained more popularity [22], owing to its advantages as outlined in [12]. Therefore, MQTT protocol should be considered for use in IoT applications that employ Wi-Fi modules.

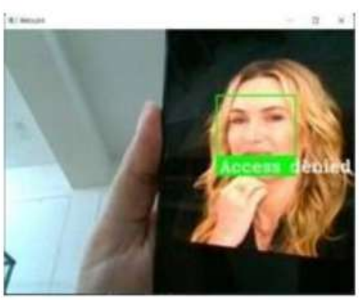

Fig. 15. Access Denied

Fig. 16. hardware setup

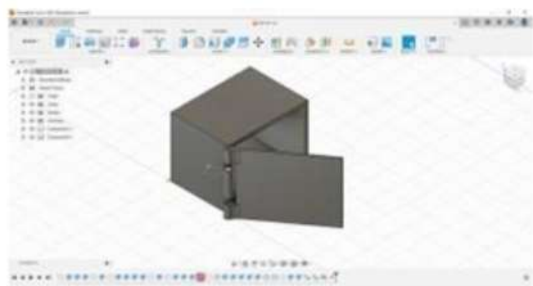

Fig. 17. Fusion 360 box design

D. Working Flowchart

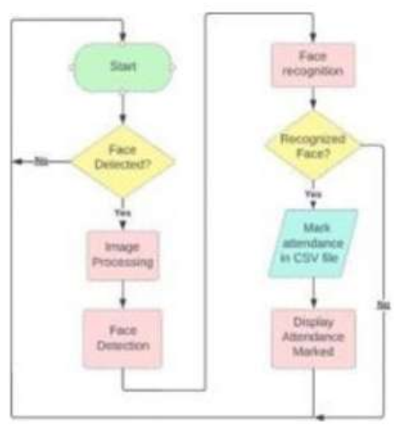

Fig. 18. Working Flowchart

H. A BRIEF COMPARISON OF VARIOUS PROTOCOLS

A. MQTT protocol

In recent decades, there has been extensive research on Wireless Sensor Networks (WSN), Wireless Body Area Networks (WBAN), and IoT applications using various platforms. We used MQTT protocol for communication with the IoT server.

B. Controller Area Network (CAN) protocol

The Controller Area Network (CAN) is a Local Area Network (LAN) controller that enables the transfer of serial data in a sequential manner. A typical architecture of an automotive system includes a control unit that provides access to all subsystems participating in the CAN bus for data transmission and reception. The CAN bus is a multi-channel transmission system that ensures that a unit's failure does not affect others. The data transfer rate of the CANbus in a vehicle system varies based on the subsystem, with high-speed rates ranging from 125Kbps to 1Mbps for real-timecontrol systems like engine control and ABS, and low-speed rates ranging from 10Kbps to 125Kbps for subsystems suchas movement adjustment. This approach distinguishes between different channels and enhances transmission efficiency.

CAN has become a mature standard due to its numerous benefits, such as excellent error handling, fault confinement, high-speed real-time communication, noise immunity in electrically noisy environments, and hardware implementation of the protocol. These advantages make CAN a popular choice in many applications where reliable and efficient data communication is crucial.

C. Lightweight M2M (LWM2M) protocol

The Lightweight M2M (LWM2M) is standard in the Open Mobile Alliance (OMA) designed to provide machine- to-machine (M2M) services with efficient device management and security workflows for IoT applications.. The LWM2M specification provides APIs for device configuration, connectivity monitoring/statistics, security, firmware update, server provisioning and more. It uses the Constrained Application Protocol (CoAP) with UDP/SMS transport bindings, making it particularly appealing for IoT devices. The LWM2M enabler employs a client-server architecture and defines the application layer communication protocol between the server and client. The LWM2M protocol is best suited for constrained device connectivity and easy management, as it uses binary encoded messages with a few bytes of overhead and flat, simple objectswith uniform URIs across devices.

D. Comparison of various protocols

we are discussing a procedure for comparing different communication protocols based on power consumption, energyefficiency, and networking speed using hardware:

Identify the hardware components required for testing the communication protocols. This will typically include microcontrollers or microprocessors that support the protocols beingtested, as well as the necessary sensors or other devices that will generate data to be transmitted. in our case, we are using raspberry pi and ESP8266 Node MCU.

Set up a test environment that includes a power meter to measure the energy consumption of the hardware during the communication process. This environment should also includea way to record the data transmission speed and latency. Our test environment is the serial UART connection between raspberry pi and Node MCU as well as the MQTT connection between the Node MCU and the IoT server.

Configure each communication protocol on the hardware and ensure that it is functioning properly. Use a test scriptto simulate data transmission between the devices using each protocol and record the energy consumption and transmission speed.

Repeat the tests with different data rates, packet sizes,and network topologies to obtain a range of results for each protocol. We have produced our test results in a tabulated form.

Analyze the data collected from the tests to identify which protocol is most energy efficient, fastest, and has the lowest latency. Make sure to consider the specific requirements of the application being tested, as some protocols may perform better under certain conditions.

Consider any additional factors that may impact the decision, such as the availability of hardware that supports the chosen protocol or the cost of implementing the protocol.

Draw conclusions based on the data collected and makea recommendation for the most appropriate protocol for the specific application.

A. Units and Equations

We have used the following units and equations:

- Voltage: volts(V)
- Current: milliamperes(mA)
- Battery capacity: milliampere hour (mAh)
- $I_{avg}=(T_1I_1+T_2I_2/T_1+T_2)$ [5]
- $T_{mobile\ node}$=capacity/hours [5]

I. IMPLEMENTATION RESULTS

The face detection algorithm was giving accurate results:

Fig. 19. face detected!!

Voltage range (V)			1.8÷3.6
Power consumption	Active mode (µA/MHz)	Flash program execution	290
		RAM program execution	150
	Low-power mode (µA)	Sleep	2.1
		Deep Sleep	1.1
		Shutdown	0.18
Wakeup time (µs)			3.5

Fig. 20. PARAMETERS OF MCU MSP430F5529.

Voltage range (V)		3÷3.6
Power consumption (mA)	TX, out = 17dBm	170
	Modem sleep	15
	Light sleep	0.9
	Deep sleep	0.01
	Power off	0.0005
Wakeup and transmit packets (ms)		< 2

Fig. 21. PARAMETERS OF ESP8266 MODULE.

Based on this we concluded the following results:

Protocol	Power	Energy Efficiency	Networking
LWM2	Low	High	Medium
MQTT	Low to Medium	High	Medium to
CAN	Low to Medium	High	High

Fig. 22. conclusion

CONCLUSION

In conclusion, the Smart drone delivery system using machine learning and character recognition using Convolutional Neural Networks (CNN) presents a promising solution forthe efficient and accurate delivery of packages. The system demonstrated the ability to accurately recognize and classify characters on packages and guide the drone to the appropriate delivery location. The use of machine learning and CNN technology enables the system to adapt to varying lightingand environmental conditions, making it robust and reliable. Overall, the Smart drone delivery system offers a promising solution to address the challenges of package delivery in urbanareas and can potentially revolutionize the delivery industry byreducing delivery times, increasing efficiency, and improving customer satisfaction. Further development and testing of the system are necessary to refine its performance and ensureits safety and reliability in real-world settings.

Additionally, the comparison of various communication protocols, such as LWM2M, MQTT, and CAN protocol using Raspberry Pi and Node MCU, has shown that LWM2M is the most suitable protocol for our system due to its low latency and reliability. Overall, the proposed smart drone delivery system provides a reliable and efficient solution to package delivery, which couldpotentially revolutionize the delivery industry.

ACKNOWLEDGMENT

We would like to express our deep gratitude and appreciation to Dr. Sriharipriya K.C., our professor and guide, for her invaluable guidance, encouragement, and support throughout the development of the smart drone delivery system using machine learning and character recognition using CNN.

Her expertise in the field of machine learning and image recognition has been instrumental in helping us understand the intricacies of designing and implementing this complex system. Her insightful comments, constructive feedback, and constant encouragement have been invaluable in shaping our ideas and bringing them to fruition.

We would also like to express our sincere thanks to our colleagues and friends who have provided their unwavering support and valuable inputs throughout the project. Their timely assistance and constructive feedback have been crucial in shaping the direction of our work and ensuring its successful completion.

We extend our heartfelt thanks to the administration and staff of our university for providing us with the resources and facilities necessary for the successful completion of this project.

Finally, we would like to acknowledge our families for their unwavering support, patience, and encouragement throughout our academic journey.

Thank you all for your invaluable contributions to this project. Your support and guidance have been instrumentalin helping us achieve our goals and realize our vision for a smarter, more efficient, and more sustainable future.

Abbreviations and Acronyms

LWM2M: Lightweight M2M is a protocol designed for remote management of IoT devices with low power and lim- ited processing capabilities. CAN: Controller Area Network is a communication protocol used in automotive and industrial applications for real-time message exchange between nodes. MQTT: Message Queuing Telemetry Transport is a lightweight protocol used for real-time data transfer between devices, commonly used in IoT applications. CNN: There is no widely known protocol called CNN in the context of IoT. However, Convolutional Neural Networks (CNNs) are a type of deep learning algorithm commonly used in computer vision tasks.

REFERENCES

[1] da Silva, Leandro Marcos, et al. "Development of an Efficiency Platform Based on MQTT for UAV Controlling and DoS Attack Detection." Sensors 22.17 (2022): 6567.

[2] Fast Object Detection for Quadcopter Drone Using Deep Learning(2018)

[3] A near-infrared image based face recognition system

[4] Improvement of Character Segmentation for Indonesian License Plate Recognition Algorithm using CNN(2019)

[5] V. -L. Dao and V. -P. Hoang, "A smart delivery system using Internet of Things," 2017 7th International Conference on Integrated Circuits, Design, and Verification (ICDV), Hanoi, Vietnam, 2017, pp. 58-63, doi:10.1109/ICDV.2017.8188639.

[6] Mishra, Biswajeeban, and Attila Kertesz. "The use of MQTT in M2M and IoT systems: A survey." IEEE Access 8 (2020): 201071-201086.

[7] Rao, Suhas, et al. "Implementing LWM2M in constrained IoT devices." 2015 IEEE Conference on Wireless Sensors (ICWiSe). IEEE, 2015.

[8] N. Nikolov, O. Nakov and D. Gotseva, "Research of MQTT versus LwM2M IoT communication protocols for IoT," 2021 56th International Scientific Conference on Information, Communication and Energy Sys- tems and Technologies (ICEST), Sozopol, Bulgaria, 2021, pp. 45-48, doi: 10.1109/ICEST52640.2021.9483477.

[9] A. Parmigiani and U. Dettmar, "Comparison and Evaluation of LwM2M and MQTT in Low-Power Wide-Area Networks," 2021 IEEE In- ternational Conference on Internet of Things and Intelligence Sys- tems (IoTaIS), Bandung, Indonesia, 2021, pp. 8-14, doi: 10.1109/IoTaIS53735.2021.9628463.

[10] L. Lanzieri, P. Kietzmann, T. C. Schmidt and M. Wählisch, "Secure and Authorized Client-to-Client Communication for LwM2M," 2022 21st ACM/IEEE International Conference on Information Processingin Sensor Networks (IPSN), Milano, Italy, 2022, pp. 158-170, doi: 10.1109/IPSN54338.2022.00020

[11] R. P. Dos Santos, V. R. Q. Leithardt and M. Beko, "Analysis of MQTT-SN and LWM2M communication protocols for precision agri- culture IoT devices," 2022 17th Iberian Conference on Information Systems and Technologies (CISTI), Madrid, Spain, 2022, pp. 1-6, doi: 10.23919/CISTI54924.2022.9820048.

[12] S. -C. Son, S. Ko, H. Lee and B. -T. Lee, "LwM2M based IoT Microservice Model with Repicas Synchronization Technique," 2020 In- ternational Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), 2020, pp. 1802-1804, doi: 10.1109/ICTC49870.2020.9289346.

[13] S. G. Patil and V. R. Ratnaparkhe, "CAN Protocol–Application in Automation Electronics," 2020 International Conference on Smart Inno- vations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), Aurangabad, India, 2020, pp. 318-321, doi: 10.1109/ICSIDEMPC49020.2020.9299621.

[14] L. C. Banuag and J. K. G. Salva, "Development of a Patient Mon- itoring System for Hospital Wards Employing Zigbee Technology and CAN Protocol," 2019 2nd World Symposium on Communica- tion Engineering (WSCE), Nagoya, Japan, 2019, pp. 112-116, doi: 10.1109/WSCE49000.2019.9040975.

[15] S. Ramaswami and R. Sundar, "Marine Monitoring System and Safety Precautions Using Can Protocol," 2020 6th InternationalConference on Advanced Computing and Communication Sys- tems (ICACCS), Coimbatore, India, 2020, pp. 984-986, doi: 10.1109/ICACCS48705.2020.9074380.

[16] M. Bozdal, M. Samie and I. Jennions, "A Survey on CAN Bus Protocol:Attacks, Challenges, and Potential Solutions," 2018 International Con- ference on Computing, Electronics and Communications Engineering (iCCECE), Southend, UK, 2018, pp. 201-205, doi: 10.1109/iCCECOME.2018.8658720.

[17] Towards an Innovative Sensor in Smart Capsule for Aerial Drones for Blood and Blood Component Delivery Liu, Rongrong et al

[18] K. -W. Chen, M. -R. Xie, Y. -M. Chen, T. -T. Chu and Y. -B. Lin, "DroneTalk: An Internet-of-Things-Based Drone System for Last- Mile Drone Delivery," in IEEE Transactions on Intelligent Trans- portation Systems, vol. 23, no. 9, pp. 15204-15217, Sept. 2022, doi: 10.1109/TITS.2021.3138432.

[19] P. Das, S. Bhaumik and S. Nath, "Signature Recognition and Detection of Skilled Forgeries Using Image Transformation and Multistream CNN," 2022 IEEE VLSI Device Circuit and System (VLSI DCS), Kolkata, India, 2022, pp. 225-229, doi: 10.1109/VLSIDCS53788.2022.9811485.

[20] E. A. Soelistio, R. E. Hananto Kusumo, Z. V. Martan and E. Irwan- syah, "A Review of Signature Recognition Using Machine Learning," 2021 1st International Conference on Computer Science and Artificial Intelligence (ICCSAI), Jakarta, Indonesia, 2021, pp. 219-223, doi: 10.1109/ICCSAI53272.2021.9609732.

[21] F. Noor, A. E. Mohamed, F. A. S. Ahmed and S. K. Taha, "Offline Handwritten Signature Recognition using Convolutional Neural Net- work Approach," 2020 International Conference on Computing, Net- working, Telecommunications and Engineering Sciences Applications (CoNTESA), Tirana, Albania, 2020, pp. 51-57, doi: 10.1109/CoN- TESA50436.2020.9302868.

[22] M. Saravanan and K. Kowsalya, "Real-Time Criminal Face Identification Based on Haar-Cascade and Lbph, with Automatic Message Delivery to Whatsapp," 2022 IEEE 2nd Mysore Sub Section International Confer- ence (MysuruCon), Mysuru, India, 2022, pp. 1-6, doi: 10.1109/Mysu- ruCon55714.2022.9972360.

[23] A CNN-based scheme for COVID-19 detection with emergency ser- vices provisions using an optimal path planning Ahmed Barnawi1 · Prateek Chhikara2 · Rajkumar Tekchandani2 · Neeraj Kumar1 · Mehrez Boulares1

Received: 28 September 2020 / Accepted: 8 July 2021
[24] E-Commerce Picture Text Recognition Information System Based on Deep Learning Bin Zhao , 1 WenYing Li,1 Qian Guo,1 and RongRong

[25] Delivery Coin: An IDS and Blockchain-Based Delivery Framework for Drone-Delivered Services Mohamed Amine Ferrag 1 and Leandros Maglar

RE-2022-110102-plag-report

ORIGINALITY REPORT

19%	13%	16%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Suhas Rao, Devaiah Chendanda, Chetan Deshpande, Vishwas Lakkundi. "Implementing LWM2M in constrained IoT devices", 2015 IEEE Conference on Wireless Sensors (ICWiSe), 2015 Publication	2%
2	doctorpenguin.com Internet Source	2%
3	www.ncbi.nlm.nih.gov Internet Source	1%
4	wsce.org Internet Source	1%
5	www.mdpi.com Internet Source	1%
6	medium.com Internet Source	1%
7	Van-Lan Dao, Van-Phuc Hoang. "A smart delivery system using Internet of Things", 2017 7th International Conference on	1%

Integrated Circuits, Design, and Verification (ICDV), 2017
Publication

8	www.coursehero.com Internet Source	1 %
9	Widodo Budiharto, Alexander A S Gunawan, Jarot S. Suroso, Andry Chowanda, Aurello Patrik, Gaudi Utama. "Fast Object Detection for Quadcopter Drone Using Deep Learning", 2018 3rd International Conference on Computer and Communication Systems (ICCCS), 2018 Publication	1 %
10	www.scilit.net Internet Source	<1 %
11	Submitted to Hong Kong University of Science and Technology Student Paper	<1 %
12	Submitted to Vilnius Gediminas Technical University Student Paper	<1 %
13	doi.org Internet Source	<1 %
14	www.researchgate.net Internet Source	<1 %

15	md-datasets-public-files-prod.s3.eu-west-1.amazonaws.com Internet Source	<1%
16	Ladlennon C. Banuag, Joseph Karl G. Salva. "Development of a Patient Monitoring System for Hospital Wards Employing Zigbee Technology and CAN Protocol", 2019 2nd World Symposium on Communication Engineering (WSCE), 2019 Publication	<1%
17	Papiya Das, Swarnabja Bhaumik, Subhrapratim Nath. "Signature Recognition and Detection of Skilled Forgeries Using Image Transformation and Multistream CNN", 2022 IEEE VLSI Device Circuit and System (VLSI DCS), 2022 Publication	<1%
18	J. Christopher Clement, K. C. Sriharipriya. "Robust Spectrum Sensing Scheme against Malicious Users Attack in a Cognitive Radio Network", 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), 2021 Publication	<1%
19	www.ijettcs.org Internet Source	<1%
20	www.semanticscholar.org Internet Source	

<1 %

21	Submitted to Harrisburg University of Science and Technology Student Paper	<1 %
22	Submitted to Nottingham Trent University Student Paper	<1 %
23	Submitted to University of Hertfordshire Student Paper	<1 %
24	arxiv.org Internet Source	<1 %
25	Submitted to Higher Education Commission Pakistan Student Paper	<1 %
26	Leandro Marcos da Silva, Henrique Bonini de Britto Menezes, Matheus dos Santos Luccas, Christian Mailer et al. "Development of an Efficiency Platform Based on MQTT for UAV Controlling and DoS Attack Detection", Sensors, 2022 Publication	<1 %
27	fcit.kau.edu.sa Internet Source	<1 %
28	Ahmad Taufiq Musaddid, Agus Bejo, Risanuri Hidayat. "Improvement of Character Segmentation for Indonesian License Plate	<1 %

Recognition Algorithm using CNN", 2019 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 2019
Publication

29	Alessandro Parmigiani, Uwe Dettmar. "Comparison and Evaluation of LwM2M and MQTT in Low-Power Wide-Area Networks", 2021 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), 2021 Publication	<1 %
30	Submitted to University of Cincinnati Student Paper	<1 %
31	Zhuofan Liao, Xiang Pang, Jingyu Zhang, Bing Xiong, Jin Wang. "Blockchain on Security and Forensics Management in Edge Computing for IoT: A Comprehensive Survey", IEEE Transactions on Network and Service Management, 2021 Publication	<1 %
32	vitalflux.com Internet Source	<1 %
33	www.iu.edu.sa Internet Source	<1 %
34	Kuan-Wen Chen, Ming-Ru Xie, Yu-Min Chen, Ting-Tsan Chu, Yi-Bing Lin. "DroneTalk: An	<1 %

Internet-of-Things-Based Drone System for Last-Mile Drone Delivery", IEEE Transactions on Intelligent Transportation Systems, 2022
Publication

35	"Computer Networks and Inventive Communication Technologies", Springer Science and Business Media LLC, 2023 Publication	<1 %
36	icestconf.org Internet Source	<1 %
37	scholar.archive.org Internet Source	<1 %
38	z-wave.freshdesk.com Internet Source	<1 %
39	Rajkumar Singh Rathore, Chaminda Hewage, Omprakash Kaiwartya, Jaime Lloret. "In-Vehicle Communication Cyber Security: Challenges and Solutions", Sensors, 2022 Publication	<1 %
40	Seung-Chul Son, Seokkap Ko, Hyungok Lee, Byung-Tak Lee. "LwM2M based IoT Microservice Model with Repicas Synchronization Technique", 2020 International Conference on Information and Communication Technology Convergence (ICTC), 2020 Publication	<1 %

41	kalaharijournals.com Internet Source	<1 %
42	www.jiit.ac.in Internet Source	<1 %
43	El Miloud Ar-Reyouchi, Kamal Ghoumid, Doha Ar-Reyouchi, Salma Rattal, Reda Yahiaoui, Omar Elmazria. "Protocol Wireless Medical Sensor Networks in IoT for the Efficiency of Healthcare", IEEE Internet of Things Journal, 2021 Publication	<1 %
44	Manuj Kumar, Tahera Hussaini. "Face Recognition Algorithm based on Traditional and Artificial Intelligence: A Systematic Review", 2021 International Conference on Intelligent Technologies (CONIT), 2021 Publication	<1 %
45	Selvamani Chandrasekaran, K I Ramachandran, Adarsh S, Ashish Kumar Puranik. "Avoidance of Replay attack in CAN protocol using Authenticated Encryption", 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020 Publication	<1 %
46	www.hindawi.com Internet Source	<1 %

47	Leandro Lanzieri, Peter Kietzmann, Thomas C. Schmidt, Matthias Wahlisch. "Secure and Authorized Client-to-Client Communication for LwM2M", 2022 21st ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), 2022 Publication	<1 %
48	Elizabeth Ann Soelistio, Rafael Edwin Hananto Kusumo, Zevira Varies Martan, Edy Irwansyah. "A Review of Signature Recognition Using Machine Learning", 2021 1st International Conference on Computer Science and Artificial Intelligence (ICCSAI), 2021 Publication	<1 %
49	Jishnu Saurav Mittapalli, Shaumaya Ojha, Subbulakshmi T. "Phishing Attack Detection using Python and Machine Learning", 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), 2021 Publication	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		