IoT Embedded Smart Glasses for the Visually Impaired

Ming Rui Lim[1] , Muhammad Hassan Majeed[2] , Manzoor Hussain[3] ,Angel Chian Ni Jee[4] ,Jasmine Hwee Ying Lai[5] , Kavesha Kanagasundaram[6], Sumathi Balakrishnan[7] Imdad Ali Shah[8]

[1,2,4,5,6,7,8] School of Computer Science Taylors' University Lakeside Campus, No. 1, Jalan Taylors, 47500 Subang Jaya, Selangor Darul Ehsan, Malaysia

[3] Computing Department Faculty of Computing & Information Technology, Indus University, Karachi Pakistan

Article History: Received: 02.10.2022 **Revised:** 23.12.2022 **Accepted:** 17.01.2023

Abstract. There are many people around the world losing their eyesight or have already lost them. Thus, it is impeccable to have a solution for that. In this project, the project team aimed to develop a device that would let blind individuals recognize obstacles at any height level and assure their safety while walking along the street. The project team has decided to use an Arduino UNO, ultrasonic sensor, ambient light sensor, potentiometer, GPS module, camera module and etc. to create a smart glass device. Moreover, the IoT architecture proposed is a five-layer architecture that has protocols that are interoperable with each other. Based on the design of the sensors and actuators, a prototype circuit of the proposed device is created as well as a prototype mobile application. Moreover, resource and potential risk management of the IoT product has been discussed to ensure the system can be able to provide services by overcoming the underlying risks and challenges. Additionally, limitations and suggestions were brought up and analyzed for future enhancements. This project has included detailed information regarding the proposed IoT device as well as matching market demands for current and future use.

1. INTRODUCTION

Approximately 40 million people are blind permanently. Meanwhile, there are about 250 million people who have been visually impaired in the world. According to a research report [1], the number of blind people will be increasing in the elder population because being visually impaired is an age-related disorder. People who get visually impaired might often experience physical, economic, and psychological changes that influence their daily life. Thus, they need some assistance tools to assist them to complete the tasks easier, and then gain confidence from fulfilling the tasks. To do so, the evolution of technology could contribute to the effort of building their confidence by creating an innovative product that could assist blind people to complete their daily tasks. Physical movement is one of the difficulties faced by blind people [2-4] They are using a white cane when walking on the street to identify obstacles. However, there are some weaknesses in using the white cane. For example, the user might be tired of their hands if they keep moving the white cane frequently. Besides, the white cane could not sense other obstacles at the high level, such as branches, notice boards, etc. Followed by the user might need to take a long time to figure out the way if there is a huge obstacle, such as a wall. Next, it could not sense the approaching object, which could lead to accidents. All of these have pointed out the several weaknesses of using a normal white cane. By using the normal white cane, it could expose the user to danger, and it is inefficient to find out the way. Therefore, the project team decided to create a product that could assist blind people to identify obstacles from any height level efficiently and ensure their safety when walking on the street[5-7]. Based on the problem statement and objectives, the project team decided to build smart glasses to solve the major problem of blind people, as well as help them to build confidence by adapting themselves to the environment.

[1,2,4,5,6,7,8] School of Computer Science Taylors' University Lakeside Campus, No. 1, Jalan Taylors, 47500 Subang Jaya, Selangor Darul Ehsan, Malaysia

[3] Computing Department Faculty of Computing & Information Technology, Indus University, Karachi Pakistan

2. LITERATURE REVIEW

In recent years, several technologies and system architecture models have been proposed for visually impaired people with IoT devices. In this section, the general architecture in healthcare-related IoT and the technologies and the underlying system architecture used in the IoT related devices for the visually impaired are investigated and analyzed.

The architecture model proposed in medicine is divided into four layers: device and sensor layer, network layer, cloud layer and application layer [8-10]. It includes most of the wearable sensors and devices in the first layer. Moreover, development boards, microcontrollers and programming languages are also included in this layer. Communication technologies such as Bluetooth, Wi-Fi, and cellular networks, as well as network protocols commonly used in smart health systems, are included in the network layer. Wi-Fi is found to be better than Bluetooth in terms of availability and accessibility, whereas Bluetooth is more frequently used for short ranged wireless communication. Besides that, the most explored network in medical IoT applications is 4G due to its higher speed and bandwidth. In the cloud server layer, centralized data and computing centers are needed for storage and computation [11-13]. Cloud benefits storage management due to it could provide a high capacity of virtual storage. However, there are some shortcomings of the cloud which is handling data traffic. The existence of fog or edge computing can be used to reduce the latency problem. MQTT, REST, and CoAP protocol are examples of network protocols that are used to communicate data between IoT devices. The application layer, which is the last layer, provides the user interface for the smart application's services. Since Android is an open-source platform with minimal cost and high flexibility, it is said to be the most popular operating system for designing IoT devices.

To achieve obstacle recognition and real-time GPS tracking, several sensors are needed. The Raspberry Pi and PIC microcontroller are used to connect the sensors and actuators [14-16]. Ultrasonic sensor, infrared sensor, and sonar sensor are some of the obstacle detection sensors addressed. As a conclusion, ultrasonic sensors appear to be a better fit for the suggested system. The ultrasonic sensor, unlike the IR sensor, is not affected by light or other elements such as moisture, dust, or smoke. Wi-Fi is used to send the obtained data, such as location, to the database. The application is connected to the database, allowing data to be accessible via the mobile app.

Another proposed system architecture [17-19] that uses IR and RFID sensors instead of the ultrasonic sensor and GPS module to achieve the similar goal as the previous system. Only the object to which the RFID tags are attached will be detected in this scenario. The Bluetooth controller is connected to the PCB unit and is used to deliver location information to the server. MedGlasses, a deep-learning-based wearable smart glasses for medicine recognition that intends to provide healthcare support for visually impaired chronic patients is proposed in paper. [21] The system consists of a drug pill recognition box with an embedded AI-based edge computing module at the perception layer, a cloud management platform at the processing layer, and a mobile device app at the application layer, which is built with a Raspberry Pi Zero W, image sensor, battery charging module, boost converter module, and a drug pill recognition box with an embedded AI-based edge computing module at the perception layer, a cloud management platform at the processing layer, and a mobile device app at the application layer. The patient's family can access medical information from the drug package using the QR code scanning capability. The medical data will be extracted first and then uploaded to the cloud over 4G, followed by the recognition box. The patient's smart glasses will snap a photo of the pills at medication time, which will be transmitted to the recognition box, and the medication records will subsequently be transferred to the cloud through Wi-Fi. Family members can check the patient's medication status using the smartphone app.

3. TECHNICAL DIAGRAM

The technical diagram of the overall proposed system is shown in Figure 1. The resources and

technologies [7,20,21] covered in the proposed system are discussed in terms of the five layers of IoT architecture: Perception Layer, Transport Layer, Processing Layer, Application Layer, and Business Layer.

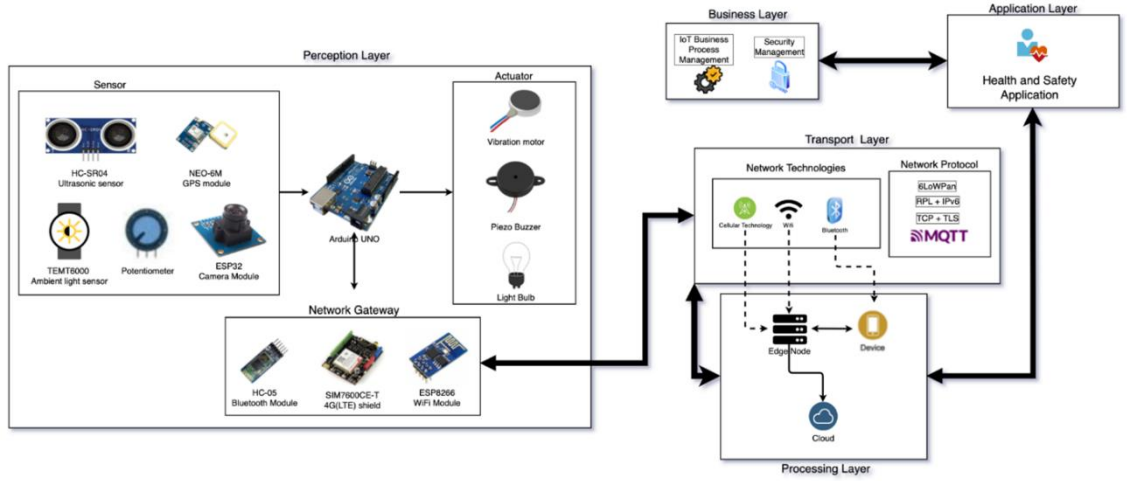


FIGURE 1. Technical Diagram of the Overall Proposed System

3.1 Perception Layer

The first layer in IOT architecture is the perception layer, also known as the physical layer. This layer contains sensors and actuators for sensing and gathering data from the environment, as well as other hardware components that are required by the proposed system. The five sensors used in the proposed system are described below.

"HC-SR04 Ultrasonic sensors": The HC-SR04 ultrasonic sensor is used to detect objects. The sensor offers a low-cost and simple way to measure distance. The working principle of the sensor is to send an ultrasonic [8,22,23] pulse from the unit to the target and measure the time required for the echo to return to measure the distance.

- **"TEMT6000 Ambient Light sensor"**: As a photodetector, the TEMT6000 ambient light sensor can detect the total amount of ambient light present in the environment. In low-light situations, the combination of ambient light sensor and LED will be used as a flashlight, assisting users in being seen by other pedestrians and ensuring user's safety while walking.
- **"Potentiometer"**: The potentiometer is used to monitor the condition of each component. The voltage flow for each component in the circuit will be read by the potentiometer.
- **"NEO-6M GPS Module"**: Since the emergency functions in the proposed system require the use of a satellite navigation system, the NEO-6M GPS module is used to determine the user's ground position to collect the user's location coordinates.
- **"ESP32 Camera Module"**: The ESP32 camera is a small-sized camera module, which is widely used in IoT applications such as smart sticks and smart home devices. The camera is used to capture real-time video that is then saved to the cloud.

All the sensors are connected to the Arduino UNO, which is a microcontroller module based on the microcontroller Microchip Atmega328P. [2,9,24] Because of the low cost, ease in the implementation, and suitability for real-time hardware, Arduino Uno is preferred over Raspberry Pi or PIC microcontrollers. The board has a collection of digital and analogue input/output pins for connecting sensors and actuators. Three actuators are used in the proposed system: a vibration motor, a piezo buzzer, and an LED. When an object is detected, the vibration motor and piezo buzzer work together with ultrasonic sensors to produce sound and vibration to alert the user. The LED can also be used as an alert component when combined

with the ambient light sensor. The required functions will be programmed in C++ in a sketch, which will then be uploaded and executed on the Arduino board [25-26]. To send and receive data in the proposed system, a network gateway is required. External shields, including HC-05 Bluetooth module, SIM7600CE-T 4G(LTE) Arduino Shield and ESP8266 Wi-Fi module, are attached to the board to build the network that allows data exchange between system components such as sensors, edge nodes, and cloud.

3.2 Transport Layer

The transport layer is responsible for transmitting data from the perception layer to the processing layer and vice versa through network technologies. Bluetooth, Wi-Fi and 4G are the network technologies used in the proposed system.

- **"Bluetooth"**: This technology is used to connect the user's mobile device to smart glasses. When the emergency button is pressed, the user's location data is collected, which will be sent to the mobile phone through Bluetooth. The reason for implementing Bluetooth technology is due to the low power consumption and cheap cost. [10,27,28] Aside from that, Bluetooth is suitable for exchanging data over short distances.
- **"Wi-Fi and 4G"**: These technologies are used to transmit data to edge nodes and cloud. If Wi-Fi is unavailable, 4G can be used for transmitting and receiving data.

The network protocol is utilized to establish the connection between IoT devices and cloud-based services over the Internet. This is to provide a secure communication channel between them for sending or receiving data. The selected network protocols are classified in OSI (Open Systems Interconnection) reference model that provides the guideline for the technology vendors and developers to enable the interoperability of the digital communications products and software programs. The OSI also helps the project teams to have a clear conceptual framework of their networking functions or telecommunication system. [11,29,30] There are 7 layers in the OSI reference model that are describing the breakdown of the communication process between two network endpoints. The data transmission would start from the application layer. On the other hand, data gathering would start from the physical layer. The description of OSI model for the reference system is shown in Figure 2.

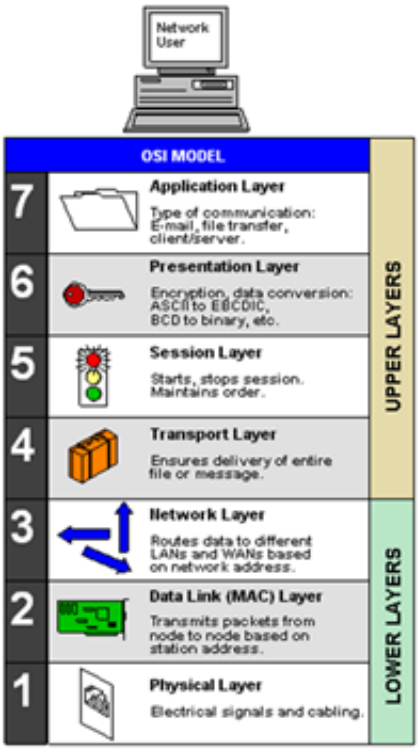


FIGURE 2. Description of OSI Model [11]

Based on the reference system, an OSI model for this IoT project is constructed and defined with every layer of IoT Architecture in Table 1. The description of selected network technology and protocol is shown in Table 2.

TABLE 1. Define the Selected Network Technology and Protocol with OSI model and IoT architecture

OSI	IoT Architecture	Selected Network Technology & Protocol
Physical Layer Data-link Layer	Perception Layer	Bluetooth, Wi-Fi, Cellular Technology (4G)

Network Layer Transport Layer	Transport Layer	6LowPan (IPv6 over Low-Power Wireless Personal Area Network), IPv6, RPL (Routing Protocol for Low-Power and Lossy Networks), TCP (Transmission Control Protocol)
Session Layer Presentation Layer Application Layer	Processing Layer Application Layer Business Layer	MQTT (Message Queuing Telemetry Transport)

TABLE 2. Description of Selected Network Technology and Protocol

Network Technology & Protocol	**Description**
Bluetooth	Used to establish the connection between the IoT product and phone. It uses Bluetooth Low Energy (BLE) standard to provide a short range of network communication between the smart devices with low energy consumption.
Wi-Fi	Used for sending or receiving the data to or from edge nodes or Cloud. It uses IEEE 802.11 LAN protocols and defines a set of MAC and PHY protocols for creating wireless local area networks (WLAN) with various frequency bands.
4G	Used whenever the network connectivity is difficult. Each cellular technology generation is using different standards to construct cellular networks. For example, 3G is using the UMTS standard, but 4G is using the LTE standards that provide faster data transmission speed than 3G.
6LowPAN	Combination of the IPv6 and Low-Power Wireless Personal Area Network (LoWPAN). It enables wireless data packet transmission in the form of IPv6 protocol for the low power wireless sensor network, such as Bluetooth, IEEE 802.15.4, etc.
IPv6	Latest version of Internet Protocol which is developed by Internet Engineering Task Force (IETF) to resolve the long-underlying problem of IPv4 address limitation. It provides a mechanism for identifying and locating machines on networks, as well as routing traffic across the Internet.
RPL	A standardized IPv6 routing protocol. The objective function (OF) is used in the RPL routing protocol for low-power and lossy networks to construct a Destination Oriented Directed Acyclic Graph (DODAG) based on a set of metrics and constraints. The OF is responsible to choose and specify the best parent nodes or the best path to the destination to minimize the latency.
TCP	A reliable protocol for establishing and maintaining network communication to allow data packets exchanged between the machines. TCP is used in conjunction with the Internet Protocol (IP), which specifies how machines exchange data packets.
MQTT	A lightweight publish/subscribe messaging transport runs over the TCP for communications with remote places that

demand a limited network bandwidth. MQTT has client/broker architecture. The client connects to the broker, acting as an edge node to mediate communication between the two devices. The MQTT broker is responsible for managing subscriptions as well as authenticating the client for security purposes by using TLS (Transport Layer Security) protocol. When another client publishes a message on a subscribed topic, the broker forwards it to all clients and appropriate destinations which have subscribed to that topic such as users, cloud, etc. Here, the IoT device could send the data to the broker by using MQTT, then the broker forwards the data to all the subscribers, such as cloud and user's family.

3.3 Processing Layer

Raw data that are collected from the physical world and transmitted over various network technologies usually come in a variety of sizes and forms. To ensure high data quality, pre-processing tasks are carried out in the third layer, the processing layer. Sensor data from the prior transport layer must go through a series of processing procedures including conversion of data format and removal of unwanted information. In the proposed system, data pre-processing takes place in multiple places, including the mobile device, edge nodes and cloud. Since edge nodes are located closer to the data source, they can provide substantially faster response time and more reliable data processing. With the edge nodes available in the proposed system, workload of the cloud can be significantly reduced, time efficiency can also be improved as the edge nodes use zero latency in-house analysis. [12],[31-33] Because the cloud is positioned far away from the data source, several challenges such as latency and connectivity issues needed to be overcome to transmit data. Therefore, only the processed data is transmitted from the edge nodes to the private cloud. Private clouds could ensure high data integrity as it is isolated from other organizations. When it comes to storing video data that has large storage requirements, private clouds can ensure storage scalability. In the case of public clouds, they are less expensive compared to on premise storage when processing small amounts of data, but the user's sensitive data could be accessible by the CSP (Cloud Service Provider), so the public cloud is not suitable for the proposed project. Additionally, the data would be transmitted to the cloud by using MQTT connections.

3.4 Application Layer

The application layer, also known as the abstraction layer, illustrates the user's interaction with the system. In other words, it is responsible for serving specific services to the user. The services provided differ for every application as they are based on the collected sensor data from the physical world. [13],[34-36] The proposed system, which is a health and safety system, is specially designed for visually impaired individuals and attempts to assist them in performing daily tasks that are difficfor the low-sighted people. The proposed smart glasses can serve as a smart navigating guidance, alerting users when sensors detect objects and obstacles and allowing them to be more vigilant in outdoor situations with a lot of movements. The data access of the proposed smart glasses mobile application is limited to authenticated and authorized users. The user, also known as the device owner, has the right to view and modify data, as well as the ability to grant authorization but limited data access to other subscribers, such as the user's family members. More specifically, the device owner can use the mobile application to access all video recordings and modify emergency contact list through mobile application, while other subscribers, the user's family, can only view limited data, such as the user's location data.

3.5 Business Layer

The business layer, which is the fifth layer, is defined as the manager of the entire system, from business process management to security management. This layer contains all the business logic including business guidelines and policies, application data management, data integrity and validity assurance. If the information generated by the previous layer solves a problem and aids in the achievement of business goals, it is said to be useful. [13] After performing data analysis in the cloud, business insights can be generated in the proposed system. For example, the number of approaching objects with time is collected and analysed, and the data is used to inform the user of the peak time for overcrowding [37-39]. In terms of security management, network security in the proposed system is guaranteed by integrating MQTT as messaging protocols. In the MQTT infrastructure, the perception layer of the system is protected by VPN (Virtual Private Network), which isolates the layer from external connections. For infrastructures using public networks, TLS (Transport Layer Security) with security certificate credentials form CA (Certificate Authority) are employed in the transport layer. TCP/IP protocol is used to establish the connection between the sender and receiver to assure the encapsulated packet is delivered and received by the receiver. Username and password authentication alongside Access Control Lists (ACLs) is then applied in the application security. [14] Additionally, regular system updates and upgrades are essential for the long-term operation of the proposed system. In fact, outdated software contains security vulnerabilities and the hackers searching for ways to access sensitive business data often target these vulnerabilities. As a result, system updates are required to ensure that these security flaws are addressed and fixed as soon as possible. The system updates for the proposed system are always scheduled and completed in a timely manner [40]. To prevent malicious attacks from unreliable sources, only authenticated sources are allowed to provide security updates. On the other hand, system upgrades for the proposed system are scheduled on a one-year interval basis. The goal of the upgrades is to expand the available features in the mobile application while also improving existing ones in response to user feedback.

4. RESULT AND FINDINGS

The technical circuit and mobile prototype have been built based on the requirements. The technical circuit diagram is built by using Tinkercad application, meanwhile, the mobile application prototype is designed by using the Figma application. A prototype circuit of the proposed smart glasses is shown in Figure 3.

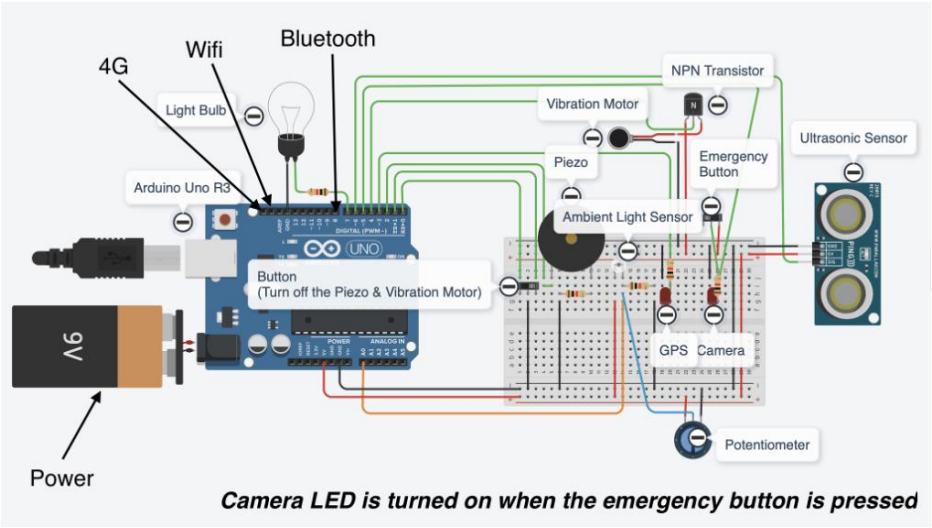


FIGURE 3. Smart Glasses Circuit in Tinkercad

The mechanism of the circuit is described below.

1. Power will be given to the Arduino via polymer battery.

2. Then the data will be collected from the sensors (ultrasonic sensor and ambient light sensor) continuously and will be matched with the threshold/set values. If the values are out of range of set values, then an action would be taken at the actuators (vibration motor, piezo and light bulb).
3. If the object is less than 0.5 meters, then a notification sound will be produced via piezo and if the object's distance varies from 0.5 meter to 1.0-meter vibration would be produced via vibration motor. The vibration would start when the distance between the object and device is 1.0m and would be increasing gradually. The vibration would be maxed at 0.5m.
4. The device has Wi-Fi and 4G to store emergency contacts in cloud, these emergency contacts will be alerted via SMS in case the emergency button is pressed. 4G/Wi-Fi will also be used to store device owner's and family members' information in a database (usernames and passwords). Recorded videos will also be stored in the cloud through 4G/Wi-Fi. The device also uses Wi-Fi for the same purposes which will operate in case of unavailability of 4G as it consumes less battery.
5. Bluetooth is used to connect with the mobile application to perform various functions as described in the previous section.
6. The device also has several other features which are described below:
    - The device also has a button to turn off the vibration motor and piezo so if the user is intentionally close to certain objects.
    - The device also has a flashlight (light bulb) which would be controlled by an ambient light sensor which means in case of a dark environment the light will turn on to alert people or vehicles passing by.
    - The device includes an emergency button which performs specific actions. The device starts the recording via the camera module and sends the current location to the emergency contacts of the device owner when the emergency button is pressed.
    - The device also has a GPS module so that it can give live locations to clouds and can be used by the family members of the user to track the user's location.
    - The device also has a potentiometer for repairing purposes as it can detect the voltage flow towards the sensors which can assist the technician in fixing if the product has any sort of issues.
    -

4.1 Mobile Application Prototype

The Mobile Application will be connected to the smart glasses via Bluetooth to perform various functions. Mobile Application will first require the user to select between the device owner and family member. If the user selects the device owner option, then the user will be prompted to the device owner homepage and if the user selects the family member option, then the user will be prompted to the family member homepage.

The interface of device owner's homepage is shown in Figure 4. On the device owner's homepage, the user first needs to create an account using a username and password [41-43]. Every user must have a unique username so that the device can store the user's data corresponding to that specific username. Later, the device owner can log in using the username and password. After registering/logging in, additional assistance features such as Bluetooth and voice assistance are enabled automatically. The user can perform multiple functions such as emergency features, allowing users to connect with the account feature, PIN generation, video recording, help functions and feedback submission features.

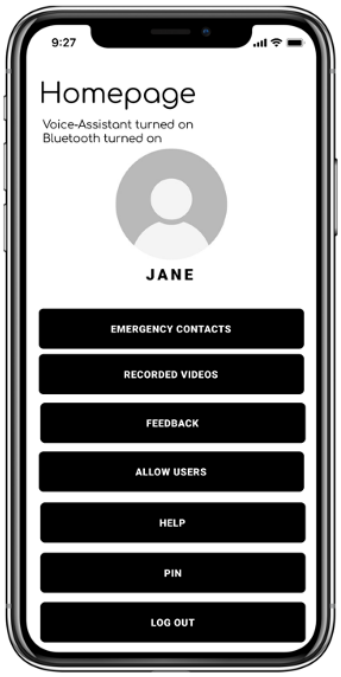


FIGURE 4. Device Owner Homepage

The interface of the family member homepage is shown in Figure 5. On the family member homepage, the user first needs to create an account using a username, password, and phone number. The username should be the same as the username of the specific user of the device so that both applications will be linked with each other. Then, the user is required to authenticate in order to connect with the device owner via a PIN generated from the device owner's account. Later, the family member [44] can log in using the username and password. The user can perform multiple functions such as location tracking, managing linked device owners' accounts and feedback submission features.

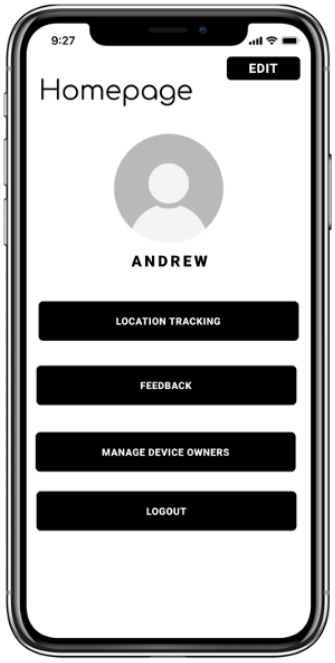


FIGURE 5 Family Member Homepage

5. DISCUSSION

Smart glasses are built with the aim of assisting blind men to perform their daily activities, then they could gain more confidence from completing those activities. Besides, the project team put the family concerns into consideration to create functionality that allows the user's family to monitor and keep track of the user's data with the user's permission. The requirements, resources and potential risks of the IoT product are analyzed to ensure it can meet the user and market demands. In addition, the current IoT products could be modified or added other functionalities to provide a better user experience and meet the evolving market demands [45-47]. The IoT product – Smart Glasses' strengths and weaknesses have been analyzed, then discussed and provided multiple suggestions to address or improve its limitation in future work.

5.1 Resource and Potential Risk Management

Due to the resource constraint of the IoT device, resource management must be discussed in order to ensure the system would not be affected adversely by insufficient resource allocation. In addition, the potential risk management plan is built to identify the underlying risks and threats, as well as to mitigate the effects of the risks once it happens.

5.2 Wireless Capability

The potential risk in wireless capability would be that user privacy can be compromised. Bluetooth provides low-level security, which means that it is an open network system that could allow for data collection by people other than the owner [48,49] of the device. While Using Wi-Fi and cellular network, an attacker can utilize sniffers to capture data packets sent between IoT devices and the cloud without having physical access to them. This attack can be used to track down or monitor the users' locations as it is being transmitted to the cloud. The solution to this is to install patches and updates to enhance its security. Specifically, for BLE, the BLE link layer encryption algorithm (AES-128 block cypher protocol) would be used. The data within the payload can be encrypted, ensuring confidentiality. [15] Similar to Wi-Fi, the implementation of the WPA2/ WPA3 protocol will be used so that the data would be encrypted during transmission. Other than that, the wireless communication capabilities on IoT devices may not be sufficient for continuous operation. A loss of connectivity may occur due to a Wi-Fi signal being lost when the device moves away from the access point, Bluetooth being limited by range, or the cellular network being adversely affected by weather conditions or electromagnetic interference from other devices. The solution to this would be to embed an SD card into the smart glasses, to store the data when the connection is unstable [50]. Once it is stable, the data can be sent to the cloud for storing. It is ensured that the data in the memory card is cleared every week by the program to prevent any leakage of sensitive data. In addition to that, the last saved status of the user would be included in the application so, that the family member and/or emergency contacts will know what is happening.

5.3 Functionality

The potential risk in functionality would be that the user will not know if the battery were to run out. The solution to this is to use an indicator, a speaker is implemented to inform the user when the battery life is at 20%. And it will repeatedly inform the user every time the battery life drops 5% for immediate charging. In addition to the battery life indicator, another risk would be if the user will not know whether the sensors and/or actuators are disabled or broken. Functionality risk comes from not having one or more sensors or actuators working properly and providing the related data to the system which [51] in turn uses this information to control an operation. The solution to this is to use a potentiometer. The potentiometer is used to measure the voltage of the sensors. So, if a sensor is not working, which means there is no voltage flow, the program will send a notification to the technician to check on the functionality of the smart glasses.

5.4 Interoperability

There are three potential risks for interoperability which are the technical, semantic, and pragmatic challenges. The technological issue here is interconnection at the physical layer/data link layer. For this project, the team implemented the use of LAN, Wi-Fi, Bluetooth, and 6LoWPAN. This is due to ensure the interoperability needs are addressed among the smart glass connectivity to the cloud and edge node as they address the heterogeneity at the MAC layer. [16] The semantic issue is that it has a concern with the capabilities of various IoT components that are responsible for processing and interpreting the exchanged data. For this, the team implemented edge nodes for processing real-time data, therefore they are responsible for extracting the semantic meaning from the data and converting it into information for the system to display on either the Smart Glass or store in the cloud. Lastly, the pragmatic challenges, it is not much of a risk since as mentioned the data is processed in the edge nodes before storing in the cloud thus, the information provided is what the smart glass needs.

5.5 Immediate Boot Capacity

The potential risk for the immediate boot capacity is that the storage space will be quickly used up due to the numerous amounts of data being saved. When IoT devices are heavily used, the storage space on it may be quickly used up. It will become slower and slower until it does not work anymore, so there must have a backup plan. The solution is to use cloud services to store data rather than local storage space. However, in this project, the cloud is the primary storage for the proposed IoT device's data [17]. Therefore, this risk does not pose a major threat to the system.

But there are a few cloud backup solutions available such as Rsync, Restic and duplicity that are commonly used as backup solutions.

- **"Rsync"**: Rsync is one of the most commonly used backup solutions. It has many features that are specifically designed for backups, such as there being no file size limit, unlimited versions of each file, and it is fast. Each time a file is copied, only the differences are saved so it saves disk space, which makes it suitable for backing up files.
- **"Restic"**: Restic is a modern backup tool based on the rsync protocol. It can use both rsync and duplicity, which have been proven to have excellent encryption capabilities. It has a comparatively simple configuration and can be used to quickly create a backup repository that is compatible with the Restic protocol.
- **"Duplicity"**: duplicity is a backup tool with excellent encryption capabilities, which has been widely used by the OpenBSD project since 2002. It does not have a problem with setting up encrypted backups for many different BSD distributions.

Another potential risk would be if the user encounters problems with the smart glass. For this the solution is to ensure that they are able to contact customer service for assistance. The team implemented a button in the application to call customer service.

5.6 Secure Storage

The potential risk for secure storage is that large amounts of data saved can be compromised. In this proposed IoT device, the team uses the cloud service to store data. However, it is vulnerable because of the lack of privacy. The solution to this is to use a private cloud Private clouds on IoT devices are an effective means for securing data generated locally. The private cloud on an IOT device has advantages in terms of security and privacy protection. Security is enhanced because it can be easily implemented to protect the sensitive data generated by the IoT device against unauthorized access [52,53]. Moreover, the private cloud can provide authentication, authorization, encryption and decryption capabilities that prevent intruders from accessing the sensitive data generated by the IoT device. This is a service that can be accessed by authorized persons only. Once the user has given permission, the user's family members or emergency contacts will be able to access the data in the cloud. To ensure that the data being stored is verifiably secure, each node should have sufficient storage space to collect data as well as process the information from other nodes to provide value for the user. An additional layer of security can be added to each device by signing and encrypting information as it is passed from node to node, in which is that the device will allow for private access to those with access rights such as the user's family members and emergency contacts.

5.7 Device Categorization

The potential risk for device categorization is insecure data transmission if not properly designed and implemented. As devices become increasingly interconnected with each other and the internet, there is a need to evaluate the security risks that these IoT devices could cause. [18] These evaluation results will allow the team to be more proactive in protecting valuable information from malicious attacks such as hacking and ransomware. One approach is to categorize the IoT device into three types: gateway, edge or cloud device. This categorization will allow the team to further evaluate the security risks of these devices by focusing on one type of device at a time. The focus will be on the edge and cloud device since it sends real-time sensor data gathered by the sensors. If this data was intercepted by an unauthorized person, they could potentially manipulate it to create adversaries [55]. For the case of the cloud device, if an attacker compromised it, an adversary can redirect information so that it is sent to the wrong server or falsify information that is stored in the cloud. The solution to this is to educate customers about how to properly implement secure IoT devices by ensuring that proper security measures are implemented. The team can educate them by providing them guidelines and standards on how to properly categorize the IoT device into three types: gateway, edge or cloud device.

5.8 Bandwidth

The potential risk for the bandwidth would be the increase in data traffic causing slow network performance. Bandwidth indicates the maximum amount of data can be transmitted over an internet connection in a given time period. There are numerous types of data would be gathered from the device's sensor and transmitted to the edge nodes or cloud. For example, location data from GPS module, data from ultrasonic sensor, recorded video from video camera, etc. This could increase the data traffic and might cause slow network performance. [19] Firstly, reduce the workload of the bandwidth by collecting the data with a given time interval. For example, the user's location data is collected and transmitted every 1 minute to reduce the amount of data being transfer in the network. Moreover, consider about the latency issues and to enhance the network performance, the real-time data will be sent to the edge node for pre-processing the data, such as the location data and ultrasonic data would be sent to the edge node for pre-processing the data by using MQTT protocol, then the data will be sent to its subscribers or cloud.

5.9 Cryptographic Controls

The potential risk in cryptographic controls would be the insecure data transmission as MQTT does not provide security enhancements over TCP to ensure that the protocol is as lightweight as possible for resource-constrained IoT edge devices. As a result, MQTT communications that rely on TCP are unencrypted and vulnerable to attacks. As a solution, the project team implements TLS protocol to perform encryption for establishing a secure and reliable connection between the sender and receiver through the three-way handshake. TLS protocol is using both symmetric and asymmetric encryptions [56]. The TLS protocol consist of two layers. At the lowest layer, it is using a reliable transport protocol, such as TCP. It's also known as the TLS Record Protocol. The TLS Record Protocol is responsible to establish a secure and reliable connection between the sender and receiver. Then, it proceeds to the next layer, that is encapsulating the data packet by using TLS Handshake Protocol. TLS Handshake Protocol is used for the authentication between the client and server, as well as to establish a secure negotiation communication for executing a cryptographic algorithm and generating cryptographic keys before the data packet is being transmitted or received. [20] There are many encryption algorithms being used in TLS protocol, some algorithms are listed down below:

- **"ECDHE (Elliptic curve Diffie–Hellman)"**: is an algorithm for cryptographic key exchange.
- **"ECDSA ((Elliptic Curve Digital Signature Algorithm**)": is an algorithm for authentication.
- **"AES_128_GSM (Elliptic Curve Digital Signature Algorithm)"**: is an algorithm for data encryption.
- **"SHA256 (Secure Hash Algorithm 256 bit)"**: is an algorithm for Message Authentication code to ensure the integrity of the data and information.

5.10 Power Management

For power management, the potential risk would be that the energy consumption increases as the device is operating for long periods of time. Most sensors that are mounted in the smart glass would keep functioning until the user turns off the device, such as data gathering and data transmission from the device to the edge node and cloud already consume much energy. If the user also turns on the emergency function, it will consume more power to support the function. This would cause the energy consumption to increase. The solution to this, is to develop a specific program in the device that could diminish the power consumption, as well as to notify the user earlier so the user could get to charge the device before the battery runs out. As transmitting the data to the cloud might consume more power because the distance between the IoT device and the cloud might be far, especially the video because it contains more data, it would consume even more power and take longer time to transmit the video data to cloud. For this, the project team decided to prior send the data to the edge nodes for pre-processing, then once its processed, it would send to the cloud [57]. This could save up the energy because the data is being transmitted to the nearby edge nodes instead of

the cloud. In addition, the device would start alerting the user when the battery life goes down as mentioned. In addition, data transmission can happen because of network connection. There are 3 wireless network connections being used in the IoT device, they are Bluetooth, Wi-Fi and cellular network (4G). Using cellular network to establish the connection consumes more power, so Wi-Fi is recommended to be used when the user enters the Wi-Fi network connection area to reduce the power consumption. The Wi-Fi has been modified to Low-power Wi-Fi to accommodate the IoT demand. As well as Bluetooth has been modified to BLE.

5.11 Limitation

The following points are the limitation of the current IoT project that identified by the project team, they are component limitation, annoying disturbance, high power consumption and less features.

- **"Component Limitation"**: There are a few components that have their limitations, which would be affected by the external/ environmental factors, such as weather. This could affect the diagnosis of the sensor and lead the actuator to perform the wrong action.
- **"Annoying Disturbance"**: When there's an object approaching the user within the 1-meter range, the vibration motor will start vibrating [2-4]. If the object is approaching the user closer, within a 0.5-meter range, the vibration motor will be stopped but the piezo (speaker) would start producing the sound to alert the user. The continuous alert would annoy the user if the user were having a conversation with others.
- **"High Power Consumption"**: As the device's sensors keep sensing, gathering and sending the data when the user turns on the device, such as ultrasonic sensor, GPS module, ambient light sensor, etc. The device did not offer battery saving mode but there are others approaches for mitigating this issue, for example, the device would keep informing the user when the battery is about to run out and if the device stays at a static location for about 15 minutes, inactive movement will lead the device to automatically shut down itself for saving battery.
- **"Less feature"**: The product is only executing the primary functions. Adding advanced features are adding value to the product, such as object recognition, hole detection, etc. to assist the user to perform the daily activities easier, more convenient and safer.

6. Future Enhancement

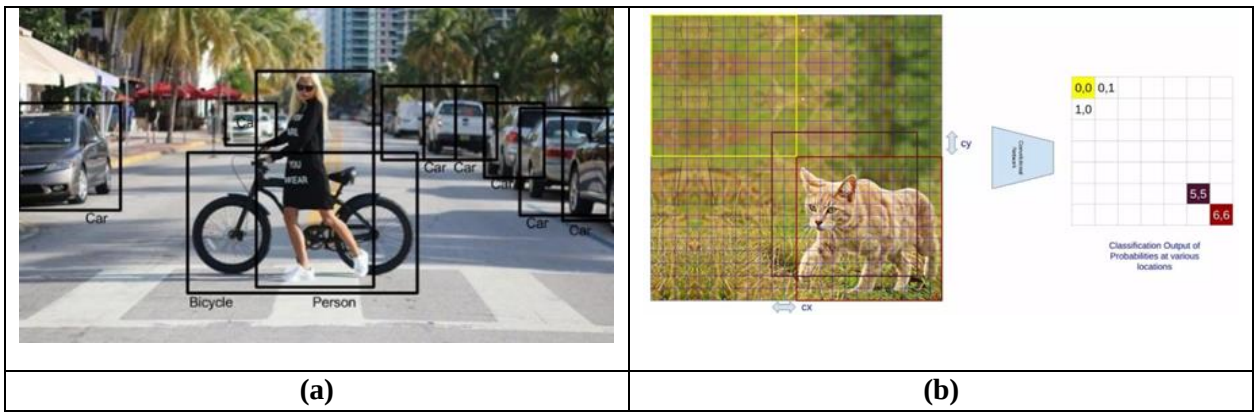
The project team did research on the number of blind men in the world, and the report [1] indicates the elder population is at higher risk to get visually impaired. The elder population might not be familiar with the latest technology, so the IoT product design must be user-friendly for the elder people to be familiar with using the IoT product easily. Besides, the project team provides multiple suggestions for future enhancement in order to enhance the user experience and the overall functionalities. The project team recommended the next project team could concentrate more on building new and advanced functionalities.

The advanced functionalities should be prominently concentrated on the user's safety and assisting the user to perform daily tasks. It would be added value and meet the market demands as those functionalities would excel the IoT product amongst other competitors in the market, as well as could assist the user to perform the tasks effectively in their daily life. The functionalities below are the suggestions or the part for future projects to focus on.

- **"Improve Notification Alerting"**: If an object is approaching the user within 1-meter area of the user, the vibration motor and piezo would start alerting the user until the object is leaving the range of area. Continuous alerting would lead to the user feeling annoyed if the user is having a conversation with the approaching object. In this case, the project team only recommends the user to turn off the device if they are having a conversation in a static place. It is recommended to have a better solution for improving functionality.
- **"Battery Saving Mode"**: As the proposed IoT device consumes more power for data transmission and the age of the battery could adversely affect the battery life, so it leads to

the device often running out of battery and the user might be frustrated of often recharging the device. Therefore, to ensure the system quality, it is recommended to embed a battery saving mode in the device, then trigger the mode when the battery is about to run out, such as 20%.

- **"Hole Detection"**: Hole detection is recommended to be included in the proposed IoT device as it could enhance the IoT device capability in user safety protection.
- **"GPS Navigation"**: It would be adding value to the device if they could navigate the user to the destination since the current device could track the user location and only a few similar IoT products in the market provide the GPS navigation function.
- **"Voice Recognition"**: Implementing voice recognition service, such as Google assistant, Siri, Amazon Alexa, etc. allows the user to interact with the IoT device better.
- **"Object Recognition"**: Implement the Single Shot Detector for high-accuracy object detection, such as transactions, traffic sign detection, etc. It is used to identify an object that is captured as an image by referring to the bounding box of the object repetitively and predicting their labels. The Figure 6 is showing how does the Single Shot Detector detect and identified the objects.
- **"Virtual Reality (VR)"**: People who get visually impaired might often experience the physical, economic and psychological changes that influence their daily life. Implementing VR is prominent for assisting the low vision user to run their daily routine independently, such as going outside, walking, reading, cooking, etc., and so rebuild their confidence and help them to be more independent. This could also ease the burden of the family members. [22] Figure 7 is showing how VR works.



(a) **(b)**

FIGURE 6 Image Showed in Single Shot Detector. [21]

FIGURE 7 VR Functionality.[22]

Moreover, collecting the data from the device and collecting the feedback from the user are the must after adding the new functionalities to perform the data analysis. The result could help in improving the IoT product and system for providing a better user experience. For example, keep track of the user voice recognition data to diagnose the frequency of using those functionalities. If the functionality is being used

frequently by the user, then the project team could concentrate on improving the functionality to gain the user loyalty [58,59]. Otherwise, the project team could carry out a survey and investigation about the functionality that is less frequent being used by the user. Finally, the future project also needs to investigate the entire IoT system with the contemporary challenges, then make an improvement on the IoT system to address those challenges. This is to enhance the security of the IoT system, the most important is to protect the user's personal and sensitive data against cyberattack.

7. CONCLUSION

The proposed IoT project is to build a smart glass that can assist blind users to accomplish everyday tasks easily. The proposed IoT product will be an extension of the user's senses, so it is crucial to consider the requirements of the users in terms of accessible design. Besides, it needs to be compatible with other devices that are designed for the blind and visually impaired to support their daily life. In this paper, the project team has illustrated research ideas and design specifications for the proposed IoT smart glasses. Through discussing the core capabilities of the IoT system, and detailing the hardware architecture and software architecture of the proposed device, the project team has synthesized a mockup of a smart glass device to show the design concepts. As innovative as it is, the proposed IoT solution is still facing some challenges: limitations and input methods. Due to the limitations having adverse effects on the proposed system and input methods requiring more sophisticated designs for easy use, suggestions have been made to solve those two problems. Success factors for achieving three years of technology milestone have been listed and analyzed so that the next project team could take them into consideration in changing or improving these smart glasses. Lastly, the project team suggested multiple suggestions for future enhancements of this product so that this product can meet market demands and become popular among users. The report has shown comprehensive information about the proposed IoT product, so the project team believes that the product could meet market demands and become popular among users.

REFERENCES

[1] U. o. BATH, "How blind people see the world", 2021. [Online]. Available: https://www.bath.ac.uk/case-studies/how-blind-people-see-the-world/.

[2] M. Adil, T. Rafa, J. Ferdoush, M. A. Mahmud and A. Pathak, "An IoT based Voice Controlled Blind Stick to Guide Blind People", International Journal of Engineering Inventions, Vol. 9, pp 09-14, 2020.

[3] A. Behmanesh, N. Sayfouri, and F. Sadoughi, "Technological Features of Internet of Things in Medicine: A Systematic Mapping Study", Journal of Electrical and Computer Engineering, 2020.

[4] N. Sahoo, W.L. Hung, and H.C. Yeong, "Design and Implementation of a Walking Stick Aid for Visually Challenged People", ResearchGate (2019).

[5] Kher Chaitrali S., Dabhade Yogita A., Kadam Snehal K., Dhamdhere Swati D. and Deshpande Aarti V, "An Intelligent Walking Stick for the Blind", ISSN 2091–2730, 2015.

[6] W.-J. Chang, L.-B. Chen, C.-H. Hsu, J.-H. Chen, T.-C. Yang, and C.-P. Lin, "MedGlasses: A Wearable Smart-Glasses-Based Drug Pill Recognition System Using Deep Learning for Visually Impaired Chronic Patients", IEEE Access (2020).

[7] P. Sethi and S.R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", Journal of Electrical and Computer Engineering, Vol. 2017, 2017.

[8] G. V. N. S. K. Sravya and N. Harini, "Third Eye for Blind Using Ultrasonic Sensor", International Journal of Advanced Science and Technology, Vol. 29, No. 12s, pp. 1222-1230, 2020.

[9] The Arduino Team, "Read Analog Voltage", 2018. [Online]. Available: https://www.arduino.cc/en/Tutorial/BuiltInExamples/ReadAnalogVoltage/

[10] Polytechnic Hub, "Advantages and disadvantages of Bluetooth", 2017. [Online]. Available:

https://www.polytechnichub.com/advantages-disadvantages-bluetooth/

[11] A. Froehlich and K. Gattine, "OSI model (Open Systems Interconnection)", 2021. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/OSI

[12] G. Immerman, "The Importance of Edge Computing for the IoT", 2020. [Online]. Available: https://www.machinemetrics.com/blog/edge-computing-iot

[13] A. Patel, "5 Layer Architecture of IoT", 2021. [Online]. Available: https://belkiot.in/5-layer-architecture-of-iot/

[14] Cirrus Link, "MQTT Security Best Practices", 2018. [Online]. Available: https://cirrus-link.com/mqtt-security-best-practices/

[15] H. Chaskar, "IoT Security Using BLE Encryption", 2017. [Online]. Available: https://www.networkcomputing.com/wireless-infrastructure/iot-security-using-ble-encryption

[16] S. Hasseb, A. H. A. Hashin and O. O. Khalifa, "Connectivity, interoperability and manageability challenges in internet of things", AIP Conference Proceedings 1883, 020004, 2007.

[17] A. Berry, "Backup Strategies for 2018", 2018. [Online]. Available: https://www.lullabot.com/articles/backup-strategies-for-2018

[18] S. Hammed, F. I. Khan and B. Hammed, "Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review", Journal of Electrical and Computer Engineering, Vol. 2019, 2019.

[19] C. Keller, "Low Bandwidth Means Slow Network Performance", 2018. [Online]. Available: https://www.tribuscomputer.com/low-bandwidth-means-slow-network-performance/

[20] A. Prodromou, "TLS Security 5: Establishing a TLS Connection", 2019. [Online]. Available: https://www.acunetix.com/blog/articles/establishing-tls-ssl-connection-part-5/

[21] CV-Tricks.com, "Object Detection using Single Shot Multibox Detector", 2017. [Online]. Available: https://cv-tricks.com/object-detection/single-shot-multibox-detector-ssd/.

[22] getvisionbuddy.com, "How Virtual Reality (VR) headsets help visually impaired people regain vision and transform the way they see the world", 2020. [Online]. Available: https://getvisionbuddy.com/blogs/the-vision-buddy-blog/how-virtual-reality-vr-headsets-help-visually-impaired-people.

[23] Ali, S., Hafeez, Y., Jhanjhi, N. Z., Humayun, M., Imran, M., Nayyar, A., ... & Ra, I. H. (2020). Towards pattern-based change verification framework for cloud-enabled healthcare component-based. *Ieee Access*, *8*, 148007-148020.

[16] Khan, N. A., Brohi, S. N., & Jhanjhi, N. Z. (2020). UAV's applications, architecture, security issues and attack scenarios: A survey. In *Intelligent Computing and Innovation on Data Science: Proceedings of ICTIDS 2019* (pp. 753-760). Springer Singapore.

[24] Zaman, N., Low, T. J., & Alghamdi, T. (2014, February). Energy efficient routing protocol for wireless sensor network. In *16th international conference on advanced communication technology* (pp. 808-814). IEEE

[25] Gaur, L., Afaq, A., Solanki, A., Singh, G., Sharma, S., Jhanjhi, N. Z., ... & Le, D. N. (2021). Capitalizing on big data and revolutionary 5G technology: Extracting and visualizing ratings and reviews of global chain hotels. *Computers and Electrical Engineering*, *95*, 107374.

[26] Diwaker, C., Tomar, P., Solanki, A., Nayyar, A., Jhanjhi, N. Z., Abdullah, A., & Supramaniam, M. (2019). A new model for predicting component-based software reliability using soft computing. *IEEE Access*, *7*, 147191-147203.

[27] Sennan, S., Somula, R., Luhach, A. K., Deverajan, G. G., Alnumay, W., Jhanjhi, N. Z., ... & Sharma, P. (2021). Energy efficient optimal parent selection based routing protocol for Internet of Things using firefly

optimization algorithm. *Transactions on Emerging Telecommunications Technologies*, *32*(8), e4171.

[28] Hussain, S. J., Ahmed, U., Liaquat, H., Mir, S., Jhanjhi, N. Z., & Humayun, M. (2019, April). IMIAD: intelligent malware identification for android platform. In *2019 International Conference on Computer and Information Sciences (ICCIS)* (pp. 1-6). IEEE.

[29] Shafiq, M., Ashraf, H., Ullah, A., Masud, M., Azeem, M., Jhanjhi, N., & Humayun, M. (2021). Robust cluster-based routing protocol for IoT-assisted smart devices in WSN. *Computers, Materials & Continua*, *67*(3), 3505-3521.]23\ https://www.researchgate.net/publication/233823923_Traffic_Monitoring_Using_M2M_CommunicationM2M_tongsin-eul_sayonghan_teulaepig_moniteoling/figures?lo=1

[30] Adeyemo, V. E., Abdullah, A., JhanJhi, N. Z., Supramaniam, M., & Balogun, A. O. (2019). Ensemble and deep-learning methods for two-class and multi-attack anomaly intrusion detection: An empirical study. *International Journal of Advanced Computer Science and Applications*, *10*(9) doi:https://doi.org/10.14569/IJACSA.2019.0100969

[31] Gaur, L., Singh, G., Solanki, A., Jhanjhi, N. Z., Bhatia, U., Sharma, S., ... & Kim, W. (2021). Disposition of youth in predicting sustainable development goals using the neuro-fuzzy and random forest algorithms. *Human-Centric Computing and Information Sciences*, *11*, NA.

[32] Lim, M., Abdullah, A., & Jhanjhi, N. Z. (2021). Performance optimization of criminal network hidden link prediction model with deep reinforcement learning. *Journal of King Saud University-Computer and Information Sciences*, *33*(10), 1202-1210.

[33] Hussain, K., Hussain, S. J., Jhanjhi, N. Z., & Humayun, M. (2019, April). SYN flood attack detection based on bayes estimator (SFADBE) for MANET. In *2019 International Conference on Computer and Information Sciences (ICCIS)* (pp. 1-4). IEEE.

[34] Srinivasan, K., Garg, L., Datta, D., Alaboudi, A. A., Jhanjhi, N. Z., Agarwal, R., & Thomas, A. G. (2021). Performance comparison of deep cnn models for detecting driver's distraction. *CMC-Computers, Materials & Continua*, *68*(3), 4109-4124.

[44] Muhammad Ibrahim Khalil, N.Z. Jhanjhi, Mamoona Humayun, SivaKumar Sivanesan, Mehedi Masud, M. Shamim Hossain, Hybrid smart grid with sustainable energy efficient resources for smart cities, Sustainable Energy Technologies and Assessments, Volume 46, 2021, 101211, ISSN 2213-1388, https://doi.org/10.1016/j.seta.2021.101211

[45] A. Almusaylim, Z., Jhanjhi, N. Z., & Alhumam, A. (2020). Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP. *Sensors*, *20*(21), 5997.

[46] Lim, M., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). Hidden link prediction in criminal networks using the deep reinforcement learning technique. *Computers*, *8*(1), 8.

[47] Fatima-tuz-Zahra, N. Jhanjhi, S. N. Brohi and N. A. Malik, "Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning," 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2019, pp. 1-9, doi: 10.1109/MACS48846.2019.9024821.

[47] Humayun, M., Jhanjhi, N. Z., Alruwaili, M., Amalathas, S. S., Balasubramanian, V., & Selvaraj, B. (2020). Privacy protection and energy optimization for 5G-aided industrial Internet of Things. *IEEE Access*, *8*, 183665-183677.

[48] Lee, S., Abdullah, A., Jhanjhi, N., & Kok, S. (2021). Classification of botnet attacks in IoT smart factory using honeypot combined with machine learning. *PeerJ Computer Science*, *7*, e350.

[49] Zaman, N., Low, T. J., & Alghamdi, T.

(2014, February). Energy efficient routing protocol for wireless sensor network. In *16th international conference on advanced communication technology* (pp. 808-814). IEEE.

[50] Khan, N. A., Brohi, S. N., & Jhanjhi, N. Z. (2020). UAV's applications, architecture, security issues and attack scenarios: A survey. In *Intelligent Computing and Innovation on Data Science: Proceedings of ICTIDS 2019* (pp. 753-760). Springer Singapore.

[51] Ali, S., Hafeez, Y., Jhanjhi, N. Z., Humayun, M., Imran, M., Nayyar, A., ... & Ra, I. H. (2020). Towards pattern-based change verification framework for cloud-enabled healthcare component-based. *Ieee Access*, *8*, 148007-148020.

[52] Shah, I. A., Jhanjhi, N. Z., Humayun, M., & Ghosh, U. (2022). Impact of COVID-19 on Higher and Post-secondary Education Systems. In *How COVID-19 is Accelerating the Digital Revolution* (pp. 71-83). Springer, Cham.

[53] Shah, I. A., Jhanjhi, N. Z., Amsaad, F., & Razaque, A. (2022). The Role of Cutting-Edge Technologies in Industry 4.0. In *Cyber Security Applications for Industry 4.0* (pp. 97-109). Chapman and Hall/CRC.

[54] Shah, I. A. (2022). Cybersecurity Issues and Challenges for E-Government During COVID-19: A Review. *Cybersecurity Measures for E-Government Frameworks*, 187-222.

[55] Shah, I. A., Wassan, S., & Usmani, M. H. (2022). E-Government Security and Privacy Issues: Challenges and Preventive Approaches. In *Cybersecurity Measures for E-Government Frameworks* (pp. 61-76). IGI Global.Shah, I. A. (2022). Cybersecurity Issues and Challenges for E-Government During COVID-19: A Review. *Cybersecurity Measures for E-Government Frameworks*, 187-222.

[56] Shah, I. A., Sial, Q., Jhanjhi, N. Z., & Gaur, L. (2023). Use Cases for Digital Twin. In *Digital Twins and Healthcare: Trends, Techniques, and Challenges* (pp. 102-118). IGI Global.

[57] Shah, I. A., Jhanjhi, N. Z., & Laraib, A. (2023). Cybersecurity and Blockchain Usage in Contemporary Business. In *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications* (pp. 49-64). IGI Global.S Umrani, S Rajper, SH Talpur, IA Shah, A Shujrah - Indian Journal of Science and Technology, 2020

[58] Shah, I. A., Sial, Q., Jhanjhi, N. Z., & Gaur, L. (2023). The Role of the IoT and Digital Twin in the Healthcare Digitalization Process: IoT and Digital Twin in the Healthcare Digitalization Process. In *Digital Twins and Healthcare: Trends, Techniques, and Challenges* (pp. 20-34). IGI Global.

[59] Kiran, S. R. A., Rajper, S., Shaikh, R. A., Shah, I. A., & Danwar, S. H. (2021). Categorization of CVE Based on Vulnerability Software By Using Machine Learning Techniques. *International Journal*, *10*(3)