Kufa Journal of Engineering
Vol. 16, No. 3, July 2025, P.P. 132-145
Article history: Received 21 June 2024, last revised 15 October 2024, accepted 15 October 2024

THE DRIVING LICENSE AUTHORIZED BASED ON IOT

Ahmed. A. Abdel Hussein [1], Asaad. S. Daghal [2], and Nasir Hussein Selman[3]

[1] Al-Furat Al-Awsat Technical University, Iraq, Email: aaaau90@gmail.com.

[2] Al-Furat Al-Awsat Technical, Iraq. Email: ad466kent@atu.edu.iq.

[3] Al-Furat Al-Awsat Technical, Iraq. Email: Coj.nas@atu.edu.iq.

https://doi.org/10.30572/2018/KJE/160309

ABSTRACT

Driving without a valid driver's license is considered illegal and causes endangers the safety of people, as well as vehicles. Necessary measures should therefore be taken to ensure that vehicles are operated and driven only by those with the appropriate licences. This paper proposes an authentication framework to operate the vehicles. It uses biometric devices together with the Internet of Things (IoT) technologies, where the system verifies the validity of the driver's license before allowing the vehicle to operate, guarantee that the only authorized person can control it. Other than simply detecting drivers' presence, the system provides a practical solution to ensure that drivers comply with the requirements to obtain a valid driver's license through regulations that focus on the nature of effective biometric authentication tackling the issue of unlicensed driving by integrating internet-related technologies. This approach can go a long way in reducing accidents and improving overall vehicle safety. The proposed system used Raspberry Pi, Firebase, and program in C# language for the matching fingerprint authentication process. The main results show that the average time for each verification process is 6 seconds, indicating constant up time. In addition, the system has a success rate of 65% (13 out of 20 attempts) for authentic fingerprints.

KEYWORDS

IoT, Driving license, Raspberry PI, Fingerprint, Driver's identity.

1. INTRODUCTION

Driving without a valid license is a common issue worldwide, with significant impacts on road safety. This concern is particularly evident in two populations: individuals under the age of 18 and individuals who commit crimes. These groups often drive without licenses, posing a serious threat to public safety (Boulagouas, et al., 2020).

Many people have not their own license driver that may not have the basic training, testing, and knowledge to operate a vehicle safely. The statistics that if one gets a driver's license, these people ignore traffic rules, increase the chance of accidents, and endanger themselves and others on the road Furthermore, a license lack of eligibility means that unlicensed drivers for traffic violations are not subject to the same penalties normally imposed on license holders, which exacerbates the problem

Fortunately, advances in Internet of Things (IoT) technologies have opened up new ways to address this issue. The IoT enables billions of devices, including cars, to be seamlessly connected to the Internet, providing opportunities for innovative solutions for automotive control (Rahim, et al., 2021; Athab, et al., 2020; Daghal, et al, 2022., and Hemalatha, 2020).

The main objective of this paper is to propose and implement a fingerprint authentication system as a key tool to cope with unlicensed driving. Integrating fingerprint sensors enables biometric driver identity verification. Fingerprints obtained by this sensor must be compared with data stored in law enforcement databases such as police servers.

Fingerprint recognition is a widely accepted technique for security due to its high specificity and non-replication by others (Sawant, et al., 2021., and Rahmat, et al., 2019). The advantages of this technology, together with IoT developments, offer a promising solution to the problem of unlicensed driving. The main contributions of this paper include improved driver verification capabilities, practical measures aimed at reducing cases of unlicensed driving, and enforcement capabilities to improve legality These developments have significant relevance in road safety and vehicle safety and underscore the key role they play in strengthening overall safety measures.

2. RELATED WORKS

In (Ali, et al., 2021), researchers proposed an integrated in-car gear system that uses an RFID sensor with fingerprint sensor to identify personals authorization. The fingerprint authentication is used to start ignition process, but if the fingerprint sensor fails, the RFID tag can be used as an alternative. This addition of RFID authentication enhances the vehicle's security system.

In (Selvi, et al., 2021), the vehicle detection system including facial recognition were introduced, where the system uses principal component analysis for facial recognition to detect the persons who are not authorized to prevent vehicle entry in.

A cost-effective system has been presented in (Hegde, N., et al., 2022), where the vehicles are protected from theft and address unlicensed driving. The system utilizes an Arduino microcontroller, a driver's license card (DL), an RFID reader, a fingerprint module (FP), and a GSM modem. When a driver's license is inserted into the RFID reader, the system checks its authorization. If authorized, the fingerprint is verified. If both credentials match, the ignition system is activated; otherwise, an SMS is sent to the vehicle owner and the ignition is blocked. Additionally, an SMS reminder is sent for DL renewal before expiration. The system aims to enhance road security, minimize unlicensed driving, reduce fraud, and increase DL functionality.

In (Akanbi, et al., 2020), researchers developed a software program that combines RFID tags and RFID readers with a central database for efficient university parking slot management. The owner’s and vehicle's information are stored securely in the database of the system. Access to the data is protected and can only be retrieved with the correct vehicle tag number, username, and password. The proposed system is implemented via VASAUCE website, where the security and privacy are enhanced substantially, as well as the server rental time reduces. An authorized individual is responsible for overseeing the VASAUCE website and handling any creation processes. The authorized users must submit a request to the administrator to utilize the parking slot.

Researchers in (Gaspar, et al., 2020) have developed a system to improve vehicle and driver identification in smart cities using an Android-based operating system. This system includes a portable fingerprint sensor module integrated with the Internet of Things, allowing traffic police to quickly check whether a driver holds a legal license. By making use of the devices built into smartphones, the system transmits details of suspicious vehicles over the network to the mobile phones of vehicle owners. This approach not only simplifies the document verification process but also helps identify stolen vehicles and reduces traffic congestion by reducing unnecessary stops.

3. SYSTEM MODEL AND IMPLEMENTATION PROCEDURE

The system model incorporates the driver identification process and traffic law enforcement mechanisms, as illustrated in Fig. 1. During vehicle registration, fingerprints are collected to establish a unique identifier for each driver. This process involves gathering user details, including name, date of birth, address, and occupation, which are then stored in the traffic department's database. These details can be accessed when fingerprint input is required. This procedure enables us to prevent individuals under the age of 18, those without a driver's license, or those with a significant history of traffic violations from operating vehicles, ultimately leading to a reduction in traffic accidents and a more efficient law enforcement process (Rassokhin, 2020).

Source	System Description	Technologies Used	Internet Usage
Sawant, et al., 2021	Integrated in-car gear system with fingerprint and RFID sensors for authorization.	Fingerprint Sensor, RFID Sensor	No
Rahmat, et al., 2019	Stolen vehicle detection system with facial recognition using PCA.	Facial Recognition, PCA	No
Ali, et al., 2021	Cost-effective system using Arduino, RFID reader, fingerprint module, and GSM modem for vehicle security and license management.	Arduino, RFID Reader, Fingerprint Module, GSM Modem	No
Selvi, et al., 2021	University parking slot management system combining RFID tags and readers with a central database.	RFID Tags, RFID Readers, Central Database	No
Hegde, N., et al., 2022	Vehicle and driver identification system for smart cities using Android-based OS and portable fingerprint sensor module integrated with IoT.	Android-based OS, Fingerprint Sensor, IoT	Yes
System Proposed	Fingerprint authentication system for vehicles using Raspberry Pi, Firebase, and C#.	Fingerprint Sensor, Raspberry Pi, Firebase, C#	Yes

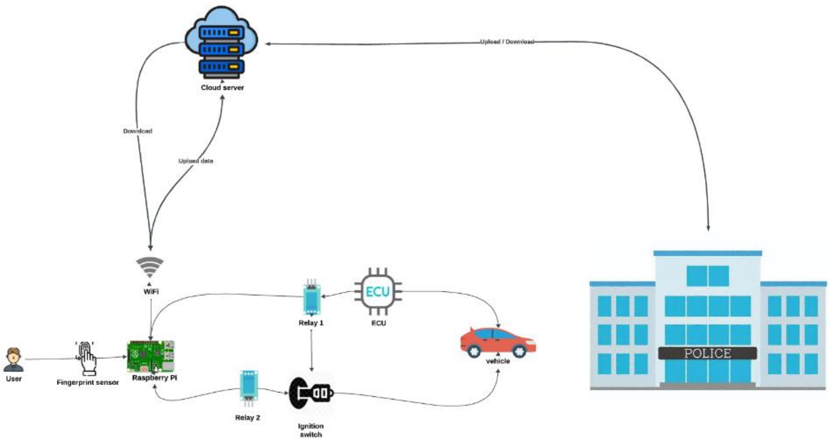

Fig. 1 System model

During the registration process, individuals provide their personal information to the traffic police office for verification, while simultaneously, their fingerprints are collected. Data recorded of the vehicle owner is collected and stored in a system database. To identify individuals, a fingerprint sensor is used. When someone puts his finger on the sensor, it promptly recognizes his identity. This fingerprint serves as the primary means of identification. After successful verification of the user's vehicle details, a unique user identifier is generated. The user's vehicle information is stored in a table of vehicle user details, using the fingerprint as the reference. This table also includes user-specific information. The "Vehicle Document

Details" table comprises a unique identifier as the reference and digital scans of all documents. Fig. 2 outlines the proposed system's flowchart. As depicted in the flowchart, following successful registration, when the driver submits their fingerprint, it undergoes online verification, and the final decision regarding their driving eligibility is displayed.

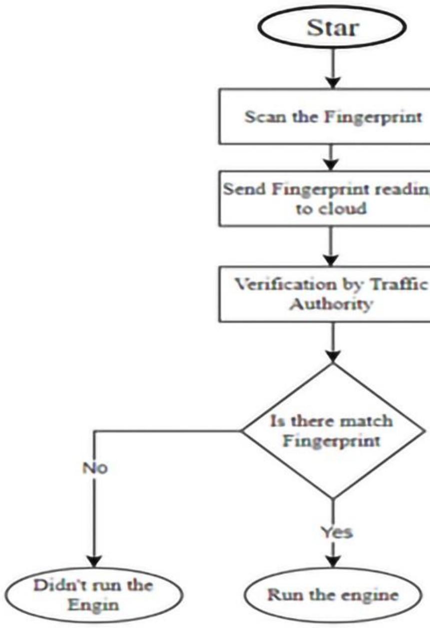

Fig. 2: Flow-chart of the system procedure

The proposed functional schematic diagram is presented in Fig. 3 and the prototype in Fig. 4 is primarily centered around the Microcontroller unit as it is considered the core component. This diagram also includes a power supply for circuit operation and incorporates a fingerprint scanner responsible for scanning, storing fingerprint data, and facilitating user interaction through the Internet.

In the proposed system, user information is systematically collected and securely stored in a database during the registration phase. During the verification phase, the process involves installing a fingerprint reader inside the vehicle to verify the user's identity before allowing the driver to operate the vehicle.

This system securely gathers and retains user information within a database managed by the r during the registration phase. In the verification phase, the steps involved the installation of a fingerprint reader device in the vehicle to validate the user's identity before permitting them to drive. As a result, the hassle of carrying personal information including a driver's license will be reduced significantly. The proposed solution offers better security, stability, and reliability in identifying the owner.

Developed with embedded system technology, the system is secure, reliable, and easy to operate. Nonetheless, the system's performance may be affected by dry, wet, or soiled fingers, which is a limitation of this approach. Coverage might also pose an issue for elderly individuals or those with skin conditions. This system can be utilized to ensure vehicle safety and, by providing access to only licensed drivers, contributes to reducing accidents. It essentially makes it impossible to drive without a valid license if this method is employed.

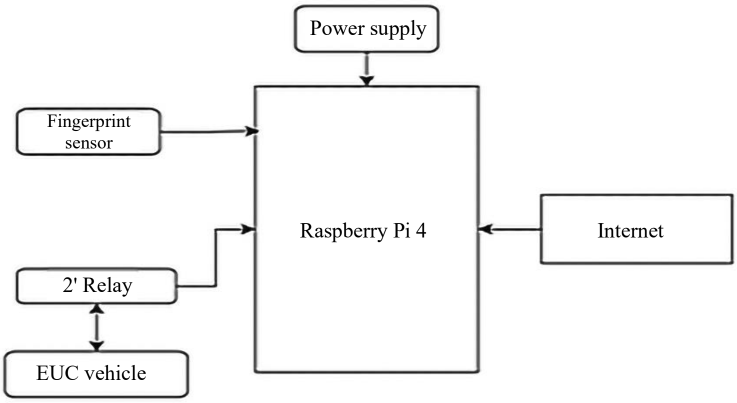

Fig. 3: Block diagram of the proposed system

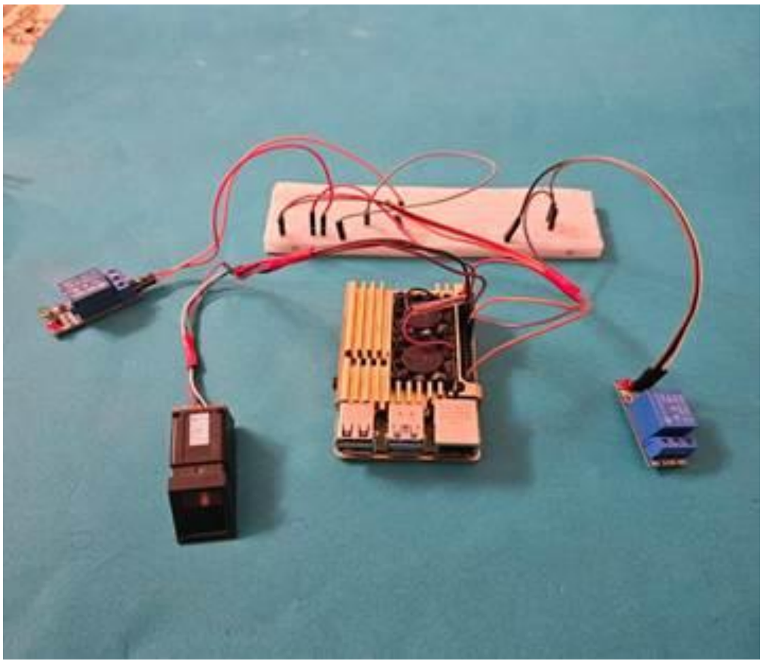

Fig. 4: Prototype of Proposed System.

The system is programmed using Thonny IDE with Python. Fig. 5 illustrates the procedures for configuring the default window of the Thonny IDE. When running Raspberry Pi, programming requires the use of an integrated development environment like Thonny IDE instead of Arduino IDE. Once the Raspberry Pi is operational, locate Thonny IDE in the application menu or use the command `Thonny` in the terminal interface. Thonny IDE opens with a graphical interface ready for programming. Open a new file to start coding. To upload the code to Raspberry Pi, configure the parameters in Thonny IDE. Choose the type of Raspberry Pi you are using from the “Board” or “Target Device” menu. Ensure that Raspberry Pi is connected to your computer using a USB cable. Thonny IDE can automatically detect and install the necessary drivers for Raspberry Pi. Select the correct port, then begin writing and uploading the code to Raspberry Pi. Upload the code, check for errors, and run it on Raspberry Pi.

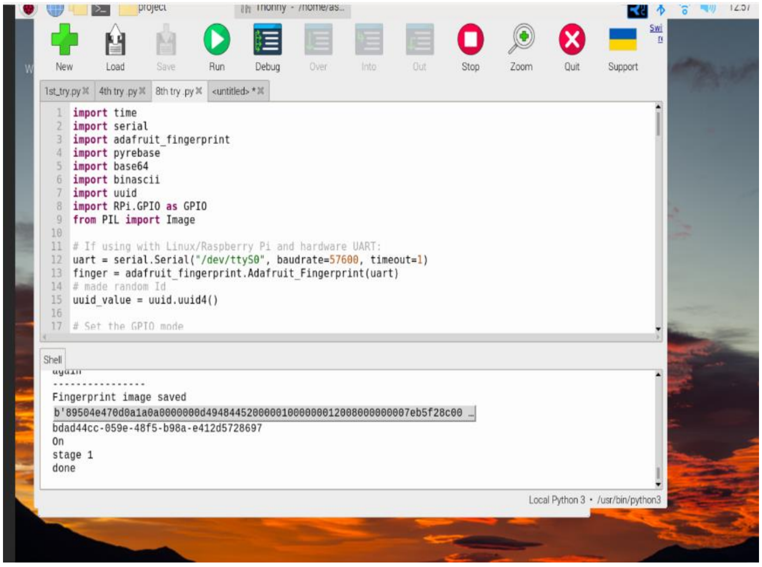

Fig. 5: Thonny IDE default window.

3.1.1. Elements of the proposed system

In this section, the software and hardware elements employed in deploying the proposed approach are explained. Following that, introducing the current system along with its intricate details.

3.1.1.1. Fingerprint Sensor

A fingerprint sensor is a tool designed to scan a person's fingerprint. This device works using a microchip that is sensitive to light, which produces a digital image of fingerprints during the scanning process. Then, the computer analyzes this image to remove the fingerprint pattern, with a similar matching pattern used to convert this data into a specific code (Sadikin, et al., 2019). Fig. 6 shows a trial of fingerprint scans, especially focusing on the functionality of an optical fingerprint scanner that uses the principle of total internal reflection (TIR). In this context, glass prism plays an important role in facilitating TIR. For TIR, the light is sent out from a light emission diode (LED) on one side of prism at a predetermined angle. The reflected light then passes through the opposite face of prism, which has a lens and an image sensor, acting effectively as a camera. In the absence of a finger on prism, the light is completely reflected from the surface, resulting in an empty image taken by the image sensor. The refractory waves interact differently with materials that are officers with separate refraction indices (RI). When a finger makes contact with the surface, only the hills get effective contact with the glass, while the air holes separate the valleys from the surface. Given that human skin and surrounding air are different RIs, causing the uneven effects on the unfortunate area.

Fig. 6: Fingerprint Sensor

3.1.1.2. Programming languages used

- **Python**

Fig. 7 illustrates a sample code of the programming language Python, which is widely recognized as a high-level programming language, positioned considerably distant from hardware. It can also be viewed as an invaluable tool frequently applied in hardware development. Micro-Python is tailored for utilization in Microcontrollers, which is a version of the Python language that is derived from the Python reference. This implementation has been successfully adapted to various target platforms, demonstrating scalability and adherence to open-source principles. Its popularity has surged in recent years within the developer community, as evidenced by the existence of more than 2,000 various forks on GitHub. These forks include various customized changes, expansions, and adjustments specifically designed for a wide range of experimental and development boards.

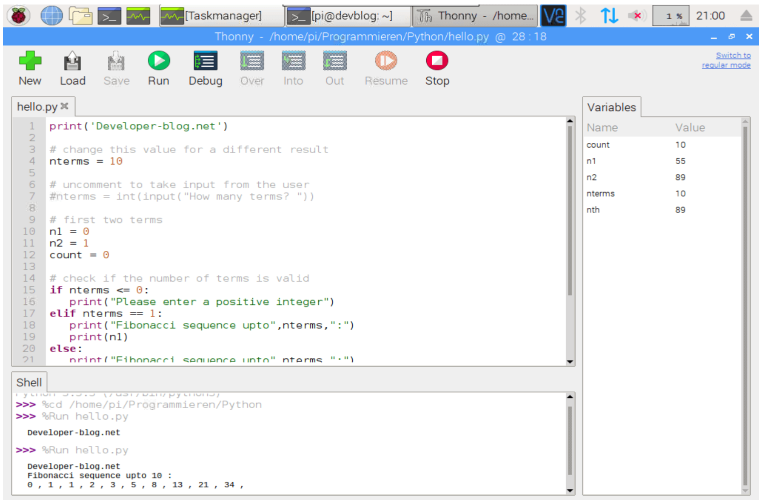

Fig. 7: Sample code of Python language

- **C#**

Numerous software applications are developed using the C# language on the .NET platform, encompassing web applications, desktop applications, games, mobile applications, office applications, and various other domains. Fig. 8 illustrates a part of the code used in this project, where the programming language C#, is widely recognized as a versatile and object-oriented language utilized in diverse software development domains.

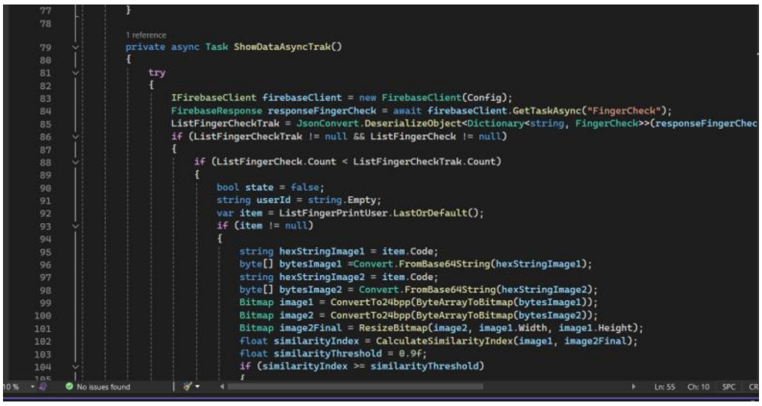

Fig. 8: Sample code of C# language

3.1.1.3. Relay

A relay is an electrically operated switch that consists of two main parts: a mechanical switch and an electromagnet (coil). Relays utilize electromagnetic principles to transfer a switch with low-power voltage, enabling the control of high-voltage electrical circuits. For example, a relay that operates on 5V and draws 50mA of current can actuate the armature relay, effectively conducting electricity at 220V with a current of 2A. We use a relay as one of the main parts of this project. Fig. 9 shows the layout of the relay.

Fig. 9: Relay module

3.1.1.4. Raspberry Pi 4

Fig. 10 shows the Raspberry Pi 4 (RPi4) Model B, which as a single-board computer was chosen as the primary device for this project due to its powerful processing power and versatile communication features. This allows you to access the Internet wirelessly via an Ethernet port or Wi-Fi. The ease of connecting to the Internet represents a distinct advantage of the RPi over the Arduino. In addition, Raspberry Pi 4 supports programming languages such as BASIC, Python, Java, C, C++, Ruby, and Perl. In contrast, Arduino is limited to C/C++ or an Arduino-specific language.

The Raspberry Pi4 Model B is an upgrade of the Raspberry Pi 3 Model B+. With a Broadcom BCM2711 quad-core 64-bit CPU clocked at 1.5 GHz and a Cortex-A72 processor, it outperforms the Pi 3's 1.4 GHz processor, making the Pi 4 GPU outstandingly powerful and powerful for better performance, the Pi 3 400 Runs comfortable at 500 MHz compared to MHz, improving imaging performance

Raspberry Pi4 Model B increased CPU and GPU skills are important factors, especially for optical recognition processes using PI cameras. This camera requires high processing speed to capture and process images effectively. As a result, Raspberry Pi4 is well suited for our system, as it provides better performance in video recording and live streaming compared to Raspberry Pi3 Model B.

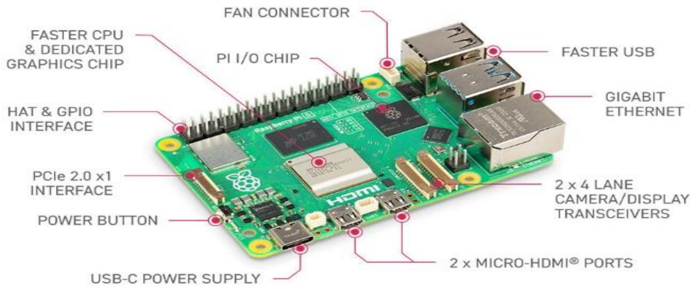

Fig.10: Raspberry Pi 4

4. RESULTS AND DISCUSSION

When the vehicle is turned on and power reaches the key system module, the fingerprint sensor activates via Raspberry Pi and captures the user's fingerprint. The captured data is then converted to base64 code to secure and hide it, and then sent to Firebase for storage and processing, as shown in Fig. 11. Using the Raspberry Pi as a central controller allows for easy management, ensuring the vehicle runs smoothly and safely.

After the fingerprint is captured, the data is sent to the Firebase database for storage. Strong encryption and security measures are implemented to protect the confidentiality and integrity of transmitted data. A C# system running as a backend on a server connected to Firebase matches fingerprint data with stored data of previously registered people. The hosted C# system analyses the incoming data and matches it with records previously stored in the database, as shown in Fig. 12. Advanced processing and matching techniques in C# ensure accurate data verification, enhancing the reliability of the monitoring and control system.

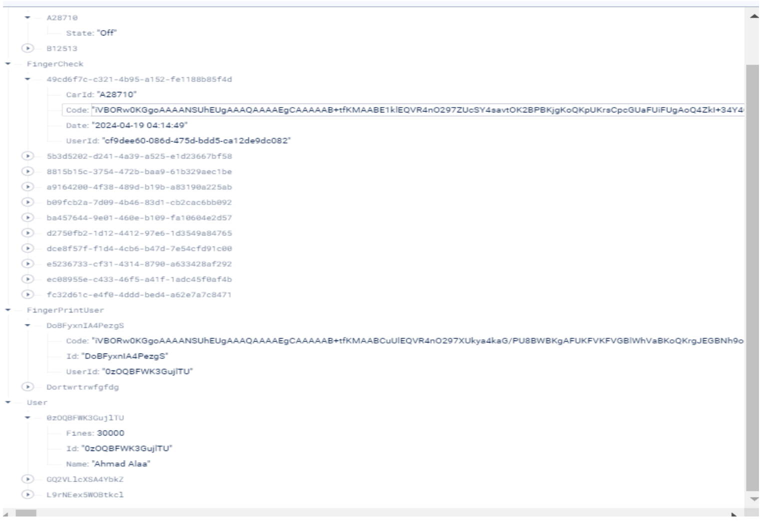

Fig.11: Database in Firebase Cloud

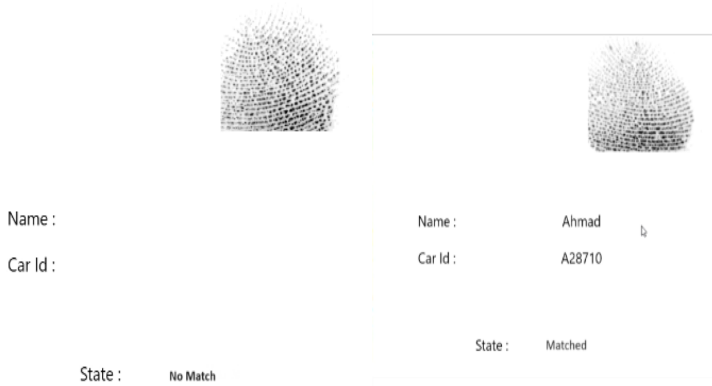

Fig. 12: Fingerprint checking in the background

Table 1 summarizes the performance of the fingerprint verification system, including the status of each attempt, the backend used, and the time taken for each verification process.

The results from Table 1 indicate that out of 20 attempts, the system successfully verified fingerprints 13 times and experienced 7 failures. The average time taken for each verification was approximately 6 seconds.

Fig.13 presents a graphical representation of these results, highlighting the distribution of successful and failed attempts along with the time taken for each verification process. This visual representation aids in understanding the performance trends and effectiveness of the system more clearly.

Fingerprint verification and consistent uptime. An average verification time of 6 seconds indicates reliable performance in wall systems. Despite high success rates, the existence of failed attempts highlights the need for further improvements. Investigating the causes of these failures, including backend system or data processing problems, is important to improve overall accuracy.

Data stored in Firebase is processed using advanced quantitative techniques and machine learning techniques to ensure data integrity and compliance. When the fingerprint data matches the stored records, the lock system is activated, allowing secure access. The system disables access in case of any discrepancies or unauthorized attempts, thereby strengthening security measures.

Table 1: Performance Results of the Fingerprint Verification System

Attempt	Backend answer	Status of test	Time taken in sec (online)
1	ON	Successful	6.53
2	ON	Successful	6.46
3	ON	Failed	6.23
4	ON	Failed	6.55
5	ON	Failed	6.34
6	OFF	Failed	6.18
7	ON	Successful	6.33
8	OFF	Successful	6.22
9	ON	Successful	6.18
10	OFF	Failed	6.21
11	OFF	Successful	6.74
12	ON	Successful	7.07
13	OFF	Successful	6.14
14	HIGH FINSE	Successful	6.35
15	ON	Successful	6.26
16	OFF	Failed	6.17
17	ON	Failed	6.71
18	OFF	Successful	6.71
19	HIGH FINSE	Successful	7.36
20	ON	Successful	6.68

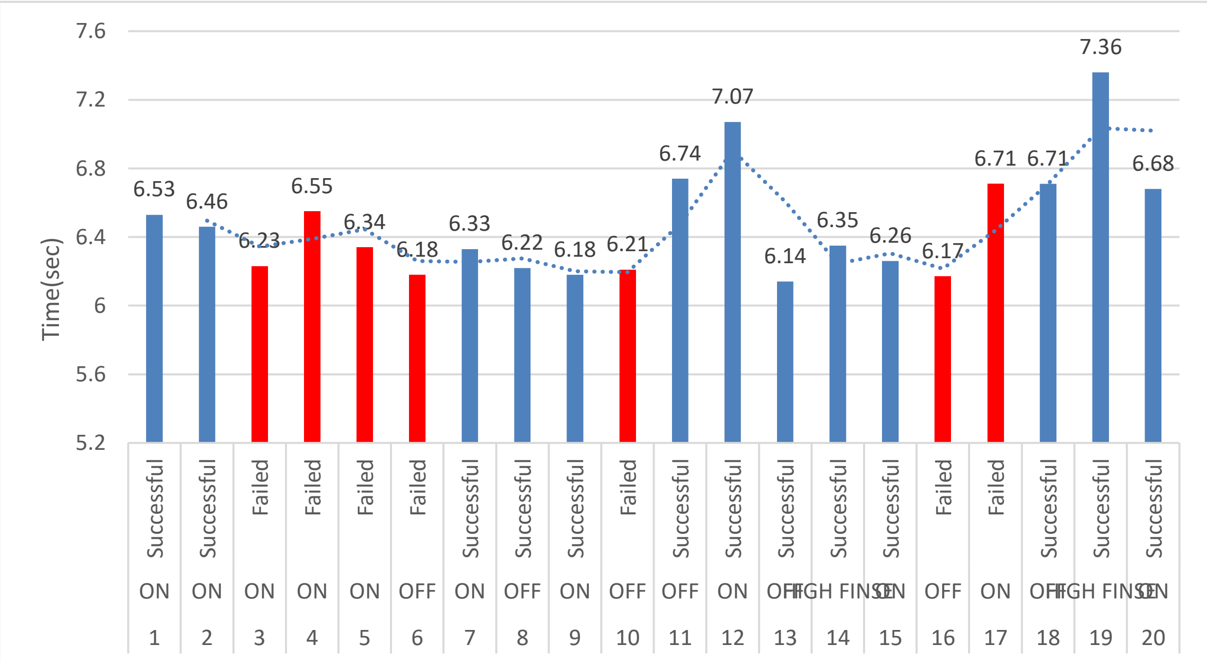

Fig. 13: depicts the system in Firebase with C#

5. CONCLUSION

A driving license tracking system that uses fingerprint technology has been developed to prevent people without valid licenses from driving, increasing safety on the road. The program aims to introduce the use of fingerprinting as a means of verifying the identity of individuals and preventing unauthorized persons from operating vehicles. The combination of cloud technology and IoT has improved system efficiency, ensured proper data storage, provided fingerprint authentication for increased accuracy and security, reduced risk of fraud and unauthorized access has reduced access by causing and reducing unauthorized traffic accidents, improved overall road safety, and improved safety for communities. The system showed a success rate of 65% from all attempts, with an average time of 6 seconds per certification process. While the success rate of the program is acceptable enough at this point, the presence of 35% of failed attempts highlights areas for improvement. In conclusion, the system shows promising performance in terms of speed and success rate but needs further research and development for future work to increase both accuracies to address failed validation attempts

6. REFERENCES

Akanbi, C.O., Ogundoyin, I.K., Akintola, J.O. and Ameenah, K., 2020. A prototype model of an iot-based door system using double-access fingerprint technique. Nigerian Journal of Technological Development, 17(2).

Ali, A.M., Awad, H.M. and Abdalgader, I.K., 2021, February. Authenticated Access Control for Vehicle Ignition System by Driver's License and Fingerprint Technology. In 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE) (pp. 1-6). IEEE.

Athab, A.F., Daghal, A.S. and Abas, S.A., 2020, November. Vehicle speed reduction based on authorized speed limits. In IOP Conference Series: Materials Science and Engineering (Vol. 928, No. 2, p. 022111). IOP Publishing.

Boulagouas, W., García-Herrero, S., Chaib, R., Febres, J.D., Mariscal, M.Á. and Djebabra, M., 2020. An investigation into unsafe behaviors and traffic accidents involving unlicensed drivers: a perspective for alignment measurement. International Journal of Environmental Research and Public Health, 17(18), p.6743.

Daghal, A.S., Athab, A.F. and Hatem, G.M., 2022, March. Social Media Apps Controls Communication Devices Based on IoT. In 2022 Muthanna International Conference on Engineering Science and Technology (MICEST) (pp. 101-105). IEEE.

Gaspar, G., Fabo, P., Kuba, M., Flochova, J., Dudak, J. and Florkova, Z., 2020, December. Development of IoT applications based on the MicroPython platform for Industry 4.0 implementation. In 2020 19th International conference on mechatronics-mechatronika (ME) (pp. 1-7). IEEE.

Hegde, N., Rashmi, R.S., Azeez, A., Mohamed, J.P. and Surendiran, J., 2022, July. IoT Based Biometric Supported Vehicle User Identification System. In 2022 IEEE International Conference on Data Science and Information System (ICDSIS) (pp. 1-6). IEEE.

Hemalatha, S., 2020, February. A systematic review on Fingerprint based Biometric Authentication System. In 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE) (pp. 1-4). IEEE.

Rahim, M.A., Rahman, M.A., Rahman, M.M., Asyhari, A.T., Bhuiyan, M.Z.A. and Ramasamy, D., 2021. Evolution of IoT-enabled connectivity and applications in automotive industry: A review. Vehicular Communications, 27, p.100285.

Rahmat, R.F., Loi, M.P., Faza, S., Arisandi, D. and Budiarto, R., 2019, June. Facial recognition for car security system using Fisherface method. In Journal of Physics: conference series (Vol. 1235, No. 1, p. 012119). IOP Publishing.

Rassokhin, D., 2020. The C++ programming language in cheminformatics and computational chemistry. Journal of Cheminformatics, 12(1), p.10.

Sadikin, N., Sari, M. and Sanjaya, B., 2019, November. Smarthome using android smartphone, arduino uno microcontroller and relay module. In Journal of Physics: Conference Series (Vol. 1361, No. 1, p. 012035). IOP Publishing.

Sawant, N., Sutar, S., Ghumare, G. and Itole, M.D., 2021. Fingerprint Based Car Ignition System Using Arduino and RFID. International Journal, 6(5).

Selvi, C.T., Amruthamathi, A., Surabhi, P.S., Motheswar, N.M. and Pavithra, D., 2021, March. Smart Authentication of Documents Using RFID and Fingerprint Modules. In 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 1462-1465). IEEE.