I. J. Engineering and Manufacturing, **2022, 6, 32-39**
Published Online on December 8, 2022 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijem.2022.06.04

An Adaptive User Authentication Architecture for Drunk Driving and Vehicle Theft Mitigation

Edward O. Ofoegbu
Pan Atlantic University, Department of Computer Science, Lagos, Nigeria
Email: eofoegbu@gmail.com
ORCID iD: https://orcid.org/0000-0002-5666-5680

Received: 31 May, 2022; Revised: 26 June, 2022; Accepted: 29 July, 2022; Published: 08 December, 2022

Abstract: The high rate of vehicle theft and the loss of lives occasioned by drunk driving has caused irreparable losses to people and businesses, from a personal, commercial and reputation perspective. Existing systems deployed to mitigate against vehicle theft have all been breached by the ever-adaptive criminals. Drunk driving has been estimated to be a leading cause of deaths on highways and motorways, through preventable accidents. Technology has provided the tools that can aid in mitigating the vices aforementioned with the aim of provisioning lasting solutions. This paper proposes a new architecture for adaptive user authentication in order to mitigate drunk driving and vehicle theft. It considered user authentication in three (3) phases and proposed an authentication architecture for each identified phase, with a step by step description of the implementation method and tools for each phase. The architecture proposed in this study can aid in real time prevention of vehicular theft, unauthorized vehicular access and usage, while also utilizing the benefits of the latest technologies in machine vision and alcohol breadth analyzers to detect and prevent drunk driving, and the associated accidents it causes.

Index Terms: Security Architecture, User Authentication, Vehicle theft, Drunk Driving

1. Introduction

The menace of drunk driving in the society has been an ever-occurring issue of discourse amongst researchers, policy makers, think thanks and the general public. [1] Identified the need for stronger measures to mitigate the social and practical consequences of alcohol impaired driving, as existing traffic regulations penalizing driving under the influence (DUI) are insufficient. Drunk driving is estimated to kill at least 28 people every day in the United States, according to [2], with 10,142 deaths reported in 2019 alone due to unsafe alcohol induced driving. The same high trend of deaths due to drunk driving is also reported in Europe [1]. Majority of the victims are young people, with a high prevalence occurring during weeknights [3]. Blood alcohol concentrations (BAC) are the standard methods of measuring the quantity of alcohol in the bloodstream, with an accepted value of 0.08% in the US for people above 21 years of age, and a value of 0% in people under 21 years of age [4]. The general operation of any form of machinery while under the influence of alcohol is undesirable as accidents have also been observed with motorcyclists, bicycle riders, industrial machine operators etc [4]. This paper however focuses on cars, buses, trucks and all other vehicle types operating on four wheels. While a driver is under the influence of alcohol he is likely to experience impaired judgment, over relaxation, slowed eye movements, slow reaction speed, slow information processing, impaired vision, impaired reasoning and impaired perception. Majority of people generally employ the following techniques to prevent the occurrence of a drunk driver, such as the use of a designated driver to social events where alcohol will be consumed, holding one another accountable for themselves to ensure no one drinks too much, also the idea of planning and holding alcohol free events to prevent the possibility of drinking and the after effects of driving drunk. All these are good measures, but they still ensure that the decision-making process of whether to drink and drive is still subjective to each individual. People are emotional beings and tend to lose all rationality as emotions emerge, thus it is imperative that technology is adopted to ensure that no drunk driver is allowed to operate a vehicle. This study thus examines the issues relating to vehicle theft and drunk driving respectively, with the aim of proposing a system architecture utilizing the best available technologies so as to minimize human and financial loss. The proposed architecture will offer a hybridized solution to the two identified problems of vehicular theft due to ineffective user authentication, and drunk driving. The deliverable of this study would be a well developed architecture that can be implemented with the suggested techniques, in order to achieve the study aim.

2. Related Works

Vehicle user authentication is a method that uses various techniques to validate the users of a vehicle, this is useful for anti-theft systems and safety driving assist systems [5]. The entire idea is to equip the vehicle with a means of distinguishing between legitimate users and illegitimate users. [5] Developed an intelligent identity authentication for vehicle security systems with the sole aim of tackling the menace of unauthorized user access and vehicle theft. The study utilized the gait profile of users for identification and authentication. A wireless signal convolution kernel in an artificial neural network was used for user identification and authentication. User authentication is useful as it allows the vehicle a means to determine a valid driver from an invalid driver. As much as vehicle authentication technology is most applicable for theft detection systems [5], over speeding detection and avoidance systems [6], driving recidivism [7], secure vehicle to vehicle communication using VANET [8], it can also be applied in drunk detection and safe driving detection systems [9] amongst others.

Vehicle theft is a growing problem globally as it is estimated that 7.4billion Dollars was lost to motor vehicle theft in 2020, with over 810,400 cars stolen in the US alone [10], thus it is imperative that technological solutions are applied to curb the menace and reduce the emotional and financial loss companies and individuals have to bear. Diverse researchers have investigated the issue and proffered solutions suing different techniques. An anti-theft system based on image and location relay was investigated in [11], they estimated that a secret button can be used for driver authentication in conjunction with a connected GSM and GPS modem for onward relay of vehicle location, if a driver fails to authenticate within 5mins. [12] Proposed a multifactor authentication technique for smart vehicle authentication. The study proposed the initial use of a password and then in addition of biometric to identify and validate a user before the car ignition system can be activated, in the event that an unauthorized user is detected, the system deactivates the vehicle and sends an SMS containing the vehicle location coordinates, using an installed GSM and GPS module to security operatives as well as the owner. [13] Also utilized biometrics for user authentication in addition to GPS and GSM modules for facilitating real time reporting of the vehicle's location. Real time location reporting of stolen vehicles using Google earth was investigated in [14]. The study developed an API that could be interfaced with Google earth to provide real time tracking of vehicle location either by a legitimate user or when reported stolen. An android phone was proposed to be used to facilitate the tracking. Vehicles were considered as a source for cyber security threat in [15], where the authors considered advanced encryption requirements, intrusion detection and prevention systems, and secure cloud service providers as possible mitigation techniques for preventing illegal usage and access of vehicles. Thefts aren't limited to vehicles alone as [16] proposed a method for the immobilization of motorbike brakes in conjunction with near-field communication (NFC) technology in order to meet the increasing demand for security and convenience of motorbike drivers. However, this study only focuses on vehicles with an aim of proposing an adaptive architecture for handling unauthorized vehicle access and usage to prevent theft and drunk driving.

Ignition interlock devices (IID) or breath alcohol ignition interlock device (BAIID) as shown in Fig.1., is a Breathalyzer attached to a user's vehicle.

Fig. 1. Alcolock Breathalyzer

A user simply has to blow into a mouthpiece connected to the device in order to start or continue operating a vehicle. If the measured breath alcohol level is greater than the preset threshold as defined for each country, the device prevents the vehicle from being started. The IID is usually placed near the driver's seat and is connected to a vehicles ignition system. In a typical vehicle without an IID installed, there is a direct signal connection to the ignition system of the car, when the key is used to trigger an ignition. The IID acts a barrier, where it intercepts the signal and will only allow it to pass onwards to the ignition system, if and only when there is a valid sample measured from the intended driver. IID's do not on their own have an automatic engine shutoff feature, due to the numerous legal and safety challenges that could be posed by an abrupt engine shutdown.

Advances in technology now mean that self-parking cars are now a thing. Automated driving hardware equipped with sensors has ensured that self-driving cars and associated technologies are making a lot of headway. Majority of drivers are still humans for now and thus it is important that self-parking features serve to solve a current issue plaguing IID systems. The lack of abrupt engine shutdown as a default feature implies that if in the event a user utilizes someone else to breathe into the analyzer or a situation where the user wasn't drinking at the time he/she entered the vehicle, but

started drinking while driving, then there should be real time monitoring to ensure that if it is detected after the engine has started that the breath alcohol level is above the limit, the vehicle should be able to initiate self-parking. Thus, addressing legal and safety issues relating to regulations.

Biometric identification has been utilized as the best method for user identification most especially the use of fingerprint, however acting alone it would not provide a robust solution to detecting unauthorized users. Real time image recognition systems based on convolutional neural networks has been investigated in [17] where the MINST dataset images were recognized with 96% accuracy. [18] Developed a machine learning and deep learning-based framework for real time detection and recognition of human faces in closed circuit television images (CCTV). The framework used principal component analysis (PCA) and convolutional neural network for feature extraction. The developed system was able to identify faces with varying levels of light level, rotation and scaling at 90% accuracy and minimum computation time. Thus, image detection can be combined with biometric to serve the purpose of user authentication.

3. Method

3.1 System Architecture

The phases of user authentication can be classified into three phases

1. Phase 1: user authentication before the door is opened.
2. Phase 2: user authentication after door is opened but before engine can start.
3. Phase 3: user authentication in real time after vehicle has started and is in motion.

Phase 1 is already handled as all vehicles are provided with a key that ensures only people with access to the key can open the door. Therefore, the key system of a vehicle acts as a user authentication mechanism in the first phase. Biometric (fingerprint) was identified as an ideal method for authenticating a user when he enters the vehicle and thus preventing it from starting if the user isn't authenticated, this is thus applicable for the prevention of theft. The alcolock ignition interlock system was also identified for the detection of breath alcohol level and preventing the vehicle from starting if measured alcohol level is above the set threshold, this is thus applicable for the prevention of drunk drivers. Both can be applied for phase two user authentication. Image detection and recognition using convolutional neural networks, in addition with principal component analysis (PCA) was identified as an ideal solution for real time detection and recognition of faces from still images captured by a camera and can thus be applied for phase 3 of user authentication.

The adaptive user authentication architecture being proposed in this paper is represented in top-down view as depicted in figure 2

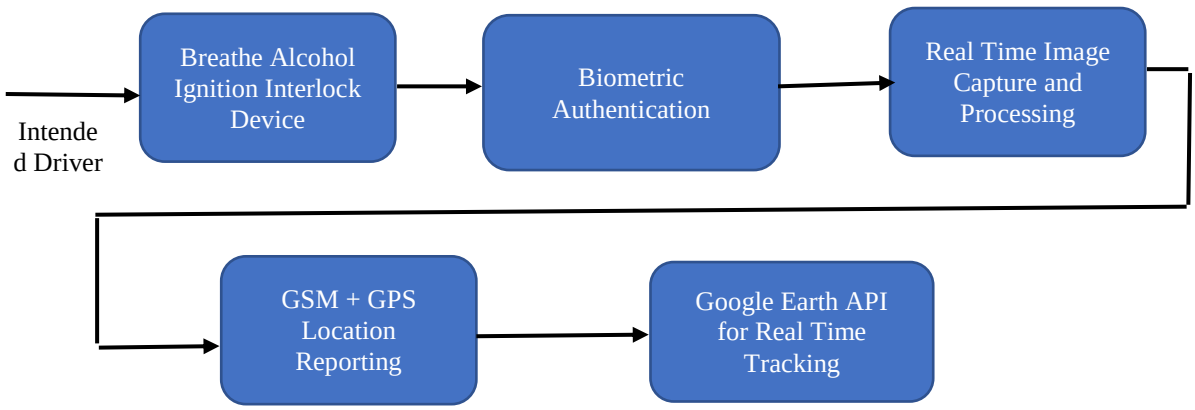

Fig. 2. System Architecture for Adaptive User Authentication

GSM + GPS location reporting, as well as Google Earth mapping offers real time feedback information to car owners and security operatives if applicable, when an unauthorized use has been deemed to have occurred. This has been well explored by other researchers as cited and thus can be used as is.

The flow chart depicted below in Figure 4, details the operation of phase 2 of user authentication. The system first expects a user to pass the breath test for alcohol. Thus a user must first provide a breath sample to the alcolock IID by breathing into it. The system will then compare the measured blood alcohol content (BAC) with the set threshold defined for the location the vehicle is registered under. If the BAC is higher than the threshold, the system will prompt the user to retry again till it is lower than the threshold. Once the BAC is lower than the threshold, the system will prompt the user to scan his/her fingerprint on the finger print sensor attached to the driver side as depicted in fig.3.

Fig. 3. Finger Print Sensor

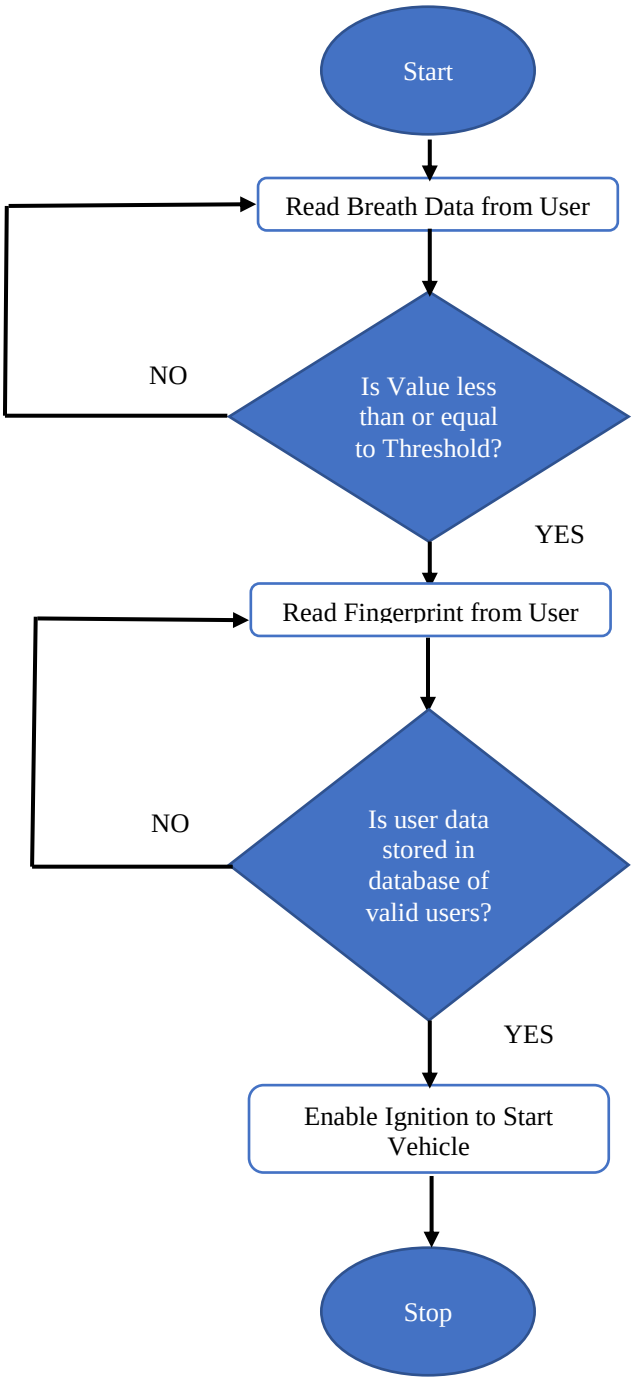

Fig. 4. Flow Chart for Phase 2

The scanned finger print is compared to a database of valid fingerprints with authorization to use the vehicle (family members, work colleagues etc.), if a match is found, the vehicle ignition will be allowed to start the car, else the system will continue to prompt the user to scan his/her fingerprint with a valid user print that can be allowed access to start the car.

Once the car has started and is in motion, the vehicle enters phase three of authentication as depicted in fig. 5.

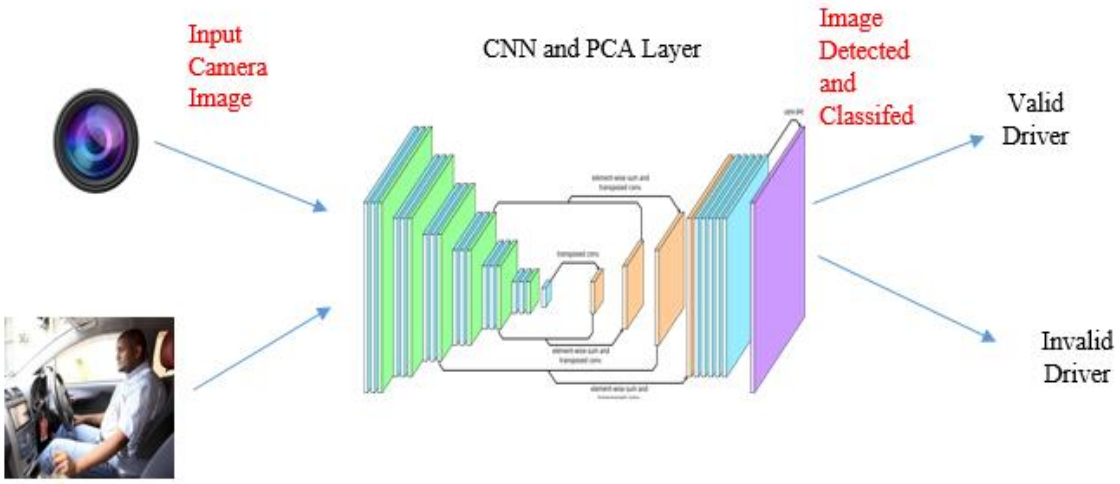

Fig. 5. Phase Three Authentication

Under phase 3, a camera takes a picture of the driver and using convolutional neural network (CNN) described as a process where a small matrix of numbers (called kernel or filters) is passed over an image in order to transform it based on the values of the filter as described in equation 1.

$$G[m,n] = (f,h)[m,n] = \sum_j \sum_k h[j,k] f[m-j, n-k] \tag{1}$$

Equation (1) depicts the kernel convolution applied in CNN for image detection on an image described using matrix notation as G[m,n], where n and m depicts the order of the matrix of pixels in the image. However, the application of multiple filters within a single layer of an image, so as to aid convolution over volume implies that, so long as the image and the filter to be applied has the same channel, then each filter can be convoluted on the same image separately, before being stacked one on top of the other to form the complete image as depicted in equation 2.

$$[n, n\ n_c] * [f, f, n_c] = [\left[\frac{n+2p-f}{s} + 1\right], \left[\frac{n+2p-f}{s} + 1\right], n_f] \tag{2}$$

Where, n is the image size, f is the filter size, n_c is the number of channels in the image, p is the used padding as depicted in equation 3, s is the used stride and n_f is the number of filters.

$$p = \frac{f-1}{2} \tag{3}$$

Where f is the filter. The image obtained from the camera can be convoluted using CNN together with principal component analysis (PCA), is able to compare the picture taken with existing pictures of legitimate users registered on its database. If a valid driver is detected the system will wait for a random time, before taking pictures again of the driver to still confirm his identity. If an invalid user is detected the system, will trigger a warning to the driver to park and discharge from the car within three (3) minutes, after which it will trigger an automatic engine shutoff and lock the car doors. Figure 6 details a flow chart of the phase three process.

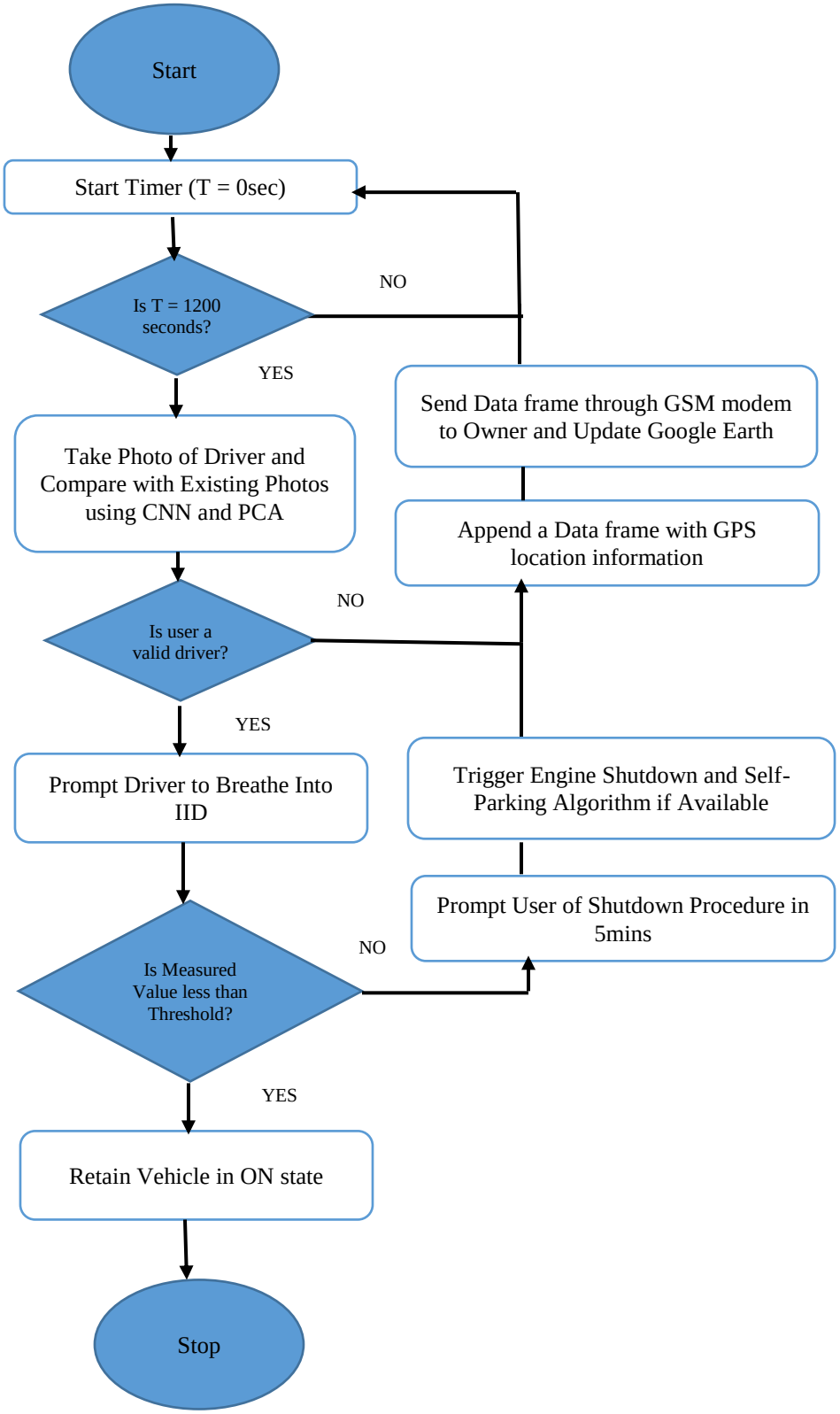

Fig. 6. Flow Chart for Phase Three

4. Discussion

The architecture proposed in this study ensures robustness in its approach to a hybridized solution for user authentication and drunk driving mitigation. The flow charts in Fig.4. and Fig.6. depicts the operation of the system for real time user authentication and drunk driving authentication. The system tried to ensure that in the first instance on a legal occupant of the vehicle can start the engine. It accomplishes this using the biometric fingerprint feature, this is classified in this study as phase 2. The biometric authentication of the intended user is carried out in tandem with a

validation of the breadth status of the user, through the breadth analyzer device. Phase two ensures that a legal user is allowed access to the vehicle system, but it doesn't stop at that, it also ensures that, if the user is valid, is the user's alcohol limit also below the set threshold for that location, for which is car is registered under. Only upon which these two checks are completed can a user start a vehicle. Phase 2, together with Phase 1 offers a very robust solution to user authentication and drunk driving mitigation. However, this study also tried to consider situations, where an illegitimate user, gets a legitimate user to bypass the phase 1 and phase 2 authentication processes under duress or on any other condition. It implies the car can be started by someone legitimate and the driving can be accomplished by someone illegitimate. This is where the phase 3 comes in. it checks the driver in real time and compares the image of the person throughout a given journey with who was initially authenticated. The system also prompts the user to intermittently breadth into the analyzer, to prevent a user from driving while drinking. Fig.6. depicts the entire process just explained. A combination of the three phases has considered all possible scenarios and is capable of providing a robust solution to the identified problem.

5. Conclusion

Effective authentication of users can reduce issues relating to theft and drunk driving. The existing architectures currently deployed have not been able to address the numerous challenges posed and researchers have looked more into effective reporting when a vehicle is stolen, not much effort was put into mitigation of theft and drunk driving. The authentication architecture proposed in this paper combines the authentication of users for both user validity and blood alcohol content level. This relatively offers to solve two problems with one solution. Already existing systems and methods were proposed for adoption in the implementation of the architecture, where CNN and PCA have long proven to be the best method for image detection and recognition, while the alcolock system has been long proven to deter drunk drivers. Thus, their utilization together under one architecture ensures that no unauthorized drunk driver can get behind the wheels of a vehicle and the real time check will help mitigate drinking while driving, as the system expects to continuously check the identity and blood alcohol content of a driver after every 20minutes of driving. This will go a long way in solving the issues raised when implemented.

Acknowledgment

This research has been supported by the school of science and technology (SST), Pan Atlantic University, Lagos, Nigeria.

References

[1] F. Alonso, J. C. Pastor, L. Montoro and C. Esteban, "Driving under the influence of alcohol: frequency, reasons, perceived risk and punishment," Substance Abuse Treatment, Prevention, and Policy, pp. 1-9, 2015.
[2] NHTSA, "Drunk Driving," United States Department of Transportation, https://www.nhtsa.gov/risky-driving/drunk-driving, retrieved 1/11/2022, n.d..
[3] H. Summala and T. Mikkola, "Fatal accidents among car and truck drivers: Effect of fatigue, age, and alcohol consumption.," Ergonomics, p. 36:315–26., 1994.
[4] K. Smith, "Drinking and Driving," PSYCOM, https://www.psycom.net/drinking-and-driving; Retrieved 1/11/2022, n.d..
[5] J. Zhang, Z. Wang and Q. yan, "Intelligent user identity authentication in vehicle security system based on wireless signals," Complex and Intelligent Systems, 2021.
[6] B. Isong, O. Khutsoane and N. Dladlu, "Real-time Monitoring and Detection of Drinkdriving and Vehicle Over-speeding," I.J. Image, Graphics and Signal Processing, 11, pp. 1-9, 2017.
[7] R.-C. Jou and Y.-H. Lu, "Factors Affecting Recidivism of Drunk Driving for Car and Motorbike Users," Hindawi, Mathematical Problems in Engineering, pp. 1-16, 2021.
[8] H. Xu, M. Zeng, W. Hu and J. Wang, "Authentication-Based Vehicle-to-Vehicle Secure Communication for VANETs," Hindawi, Mobile Information Systems, 2019.
[9] Nissan Motor Corp, "Drunk-driving Prevention Concept Car," Nissan Motor Corp, https://www.nissan-global.com/EN/TECHNOLOGY/OVERVIEW/dpcc.html, Retrieved 1/13/2022, 2022.
[10] Insurance Information Institute, "Facts + Statistics: Auto theft," https://www.iii.org/fact-statistic/facts-statistics-auto-theft Retrieved 3/31/3022, n.d..
[11] S. F. Kolawole and A. Zakari, "Design of Anti-Vehicle Theft System using GSM and GPS with Image Acquisition," Asian Journal of Engineering and Technology (ISSN: 2321 – 2462), pp. 82-92, 2017.
[12] S. O. Aliyu, U. Abdullahi, M. Pomam, S. O. Akanmu, M. Hafiz and A. Sanusi, "Smart Protection of Vehicle using Multifactor Authentication (MFA) Technique," in 3rd International Engineering Conference (IEC 2019) , Minna, Nigeria, 2019.
[13] B. Nagendra, B. Bhargavi, K. Ramyashree, K. Sukanya and K. Nagashree, "Anti-Theft Protection of Vehicles by using Fingerprint," International Journal of Engineering Research & Technology (IJERT), 2018.
[14] K. Rohitaksha, C. G. Madhu, B. G. Nalini and C. V. Nirupama, "Android Application for Vehicle Theft Prevention and Tracking System," International Journal of Computer Science and Information Technologies, pp. 3754-3758, 2014.
[15] C. Hodge, K. Hauck and S. Gupta, "Vehicle Cybersecurity Threats and Mitigation Approaches," National Renewable Energy Laboratory, 2019.

[16] T. Jin, "Evaluation of the Effectiveness of NFC-based Anti-Theft Security System for Motorbike," International Journal of Security and Its Applications, pp. 13-20, 2016.
[17] R. Chauhan, K. K. Ghanshala and R. C. Joshi, "Convolutional Neural Network (CNN) for Image Detection and Recognition," in First International Conference on Secure Cyber Computing and Communication (ICSCCC), 2018.
[18] R. Ullah, H. Hayat, A. A. Siddiqui, U. A. Siddiqui, J. Khan, F. Ullah, S. Hassan, L. Hasan, W. Albattah, M. Islam and G. M. Karami, "A Real-Time Framework for Human Face Detection and Recognition in CCTV Images," Mathemetical Problems in Engineering , p. https://doi.org/10.1155/2022/3276704, 2022.

Author' s Profile

Dr Ofoegbu Edward is a senior lecturer with Pan-Atlantic University, Lagos, Nigeria. He has a PHD in Electronics and Computer Engineering (Control Engineering). He has over twelve (12) years' experience in university teaching at undergraduate and postgraduate level. His research interest extends from Artificial intelligence, Machine learning, Automated control, autonomous systems, robotics and Smart sensor deployments. He is a well published researcher with numerous publications locally and internationally.

How to cite this paper: Edward O. Ofoegbu, "An Adaptive User Authentication Architecture for Drunk Driving and Vehicle Theft Mitigation", International Journal of Engineering and Manufacturing (IJEM), Vol.12, No.6, pp. 32-39, 2022. DOI:10.5815/ijem.2022.06.04