IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Comprehensive Unified Framework for Vehicle's Security Systems

[1]Hussam Elbehiery, [2]Khaled Elbehiery

[1]Computer Science Department, October 6 University (O6U), Egypt
[2]Computer Information Systems Department, Park University, USA

Abstract: In this modern age there is a rapid increase in the number of vehicles and so is the number of car theft attempts as well. With the growing and strong stealing techniques, owners are in fear of having their vehicles being stolen from common parking lot or from outside their home, thus the protection of vehicles from theft becomes important and crucial due to insecure environment. Real time vehicle security system based on computer vision provides a solution to this problem, many of recent vehicle security systems performs image processing based and real time user authentication using face detection and facial recognition techniques and run on microprocessor control system fixed on board with the vehicle or online application on the cloud. The system also adds an extra layer of security thru a custom authenticating driver list of the vehicle before it could even power up which offers a safe environment [1]. This paper is covering the design of an integrated anti-theft control system for an automobile that primarily based on an advanced communication technology identified as LTE. Integrating with GPS and GSM, the vehicle location will be located and tracked as well. In the event of theft attempt or unauthorized person's trial to drive the vehicle, a text in format of Multimedia Messaging Service (MMS)/ Short Message Services (SMS) will be sent to the owner along with the location followed by a choice of actions such as tracking the vehicle, shutting it completely down, or locking all doors and calling the authorities [2]. This anti-theft control system could also be integrated the national Digitized ID card or UniCard as well.

***Index Terms* - IoT, Face Recognition, Vehicle Security Systems, National Identity ID, Digitized ID, Unified Card, Vehicle security, Anti-Counterfeiting, eID, Mobile ID, Authorization.**

I. INTRODUCTION

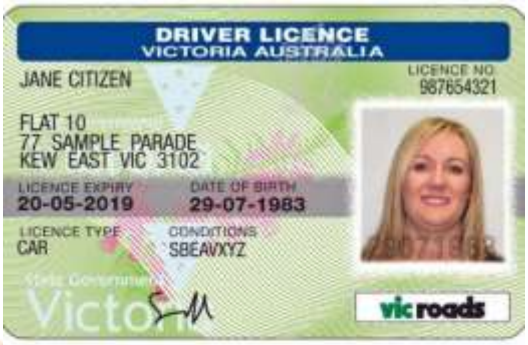
In recent years, the popularity of the automobile sector is increasing all over the world, unfortunately there is an exponential increase in vehicles crime. At the present time, most vehicles are controlled using mechanical keys, security cards, and password/pattern but with the development of IoT technologies and many embedded mechanisms, the vehicle security systems are continuously improving. These improvements are depending on the vehicle's owners and law enforcement requirements. Whereas, they are not only concerning with the theft of vehicle contents, but also the loss of vehicles and the personal security requirements of the vehicle's owner. Many well-known biometrics-based identification and verification techniques existed such as fingerprints, facial features, and iris have been integrated in various security applications. Face recognition is considered the growing common technological choice biometric technique for vehicle security and alarm, meanwhile, the face recognition process uses some complex calculations [4].

In addition, the proposed anti-theft system utilizes GPS, GSM or other radio or satellites navigation systems to locate the vehicle. The conventional products of anti-theft are typically categorized into three classes: vehicle tracking and recovery systems, the alarm system, and vehicle locking mechanical system. The proposed system targeting a better-guaranteed security solution with low cost, Google map and other similar services are also integrated [3]. This research paper introduces a fully reliable IoT system based on Digitized ID or Unicard as a guard against vehicle theft. The anti-theft system offers the availability to disable or bypass the authentication process under certain circumstances [5], and the owner is able to decide who could or could not operate the vehicle [6]. Section 2 of the research paper explain the driving license, biometrics, and Anti-Counterfeiting of drunk driving, while section 3 presents the connected cars via communication networks concepts. GPS and IoT tracking system are discussed in section 4 along with IoT fleet tracking and Cellular tracker as well. Section 5 and section 6 demonstrates detailed information about eSIM and the Governmental identity respectively. Finally, section 7 expands on the proposed vehicle security systems design.

II. Driving License and Biometrics

The Victorian Government has joined the Commonwealth Government's National Driver License Facial Recognition Solution. The National Driver License Facial Recognition Solution (NDLFRS) will protect Victorians from identity theft, prevent crime and improve road safety and UniCard or Digitized ID verification. It is part of the Government's National Identity Matching Services (NIMS). Once in use by the government, the NDLFRS will mean (See Fig. 1):

- Citizens will be better protected from identity theft and crime.
- Getting dangerous drivers off our roads.
- Increased capabilities to prevent, detect and investigate identity crime.
- Everyone can easily and securely verify their identity.
- Locating missing persons will be easier.



DRIVER LICENCE
VICTORIA AUSTRALIA

JANE CITIZEN

LICENCE NO
987654321

FLAT 10
77 SAMPLE PARADE
KEW EAST VIC 3102

LICENCE EXPIRY
20-05-2019

DATE OF BIRTH
29-07-1983

LICENCE TYPE
CAR

CONDITIONS
SBEAVXYZ

vicroads

Figure 1: Australia driver license Model

2.1 Personal Information protection

Citizens driver license data will be stored in the NIMS. In the unlikely event that the system is hacked, the Citizens Government will follow the cyber incident response steps. Notification will be of any serious data breach involving the personal information and recommend the steps which should be taken in response [8].

2.2 Driver-License Databases Authentication by FBI

United States immigration officers have used facial recognition technology to search drivers' licenses in states that issue licenses to undocumented immigrants. This is thought to be the first known case of FBI agents using facial recognition technology to scan drivers' licenses for surveillance purposes [9].

2.3 Anti-Counterfeiting of Drunk Driving

In recent years, the government increases the fine and the penalty for drunken drivers to curb the drunk driving. However, many drunken drivers rely on luck to drive a vehicle, with the result that there are many casualties in the traffic accidents. Obviously, the prevention of the drunk driving is important for traffic safety. Accordingly, many automotive manufactories have implemented the "Alcolock" successfully, such as the "Alcoguard" system of Volvo, and the "Alcokey" (breathalyzer car key) of Saab. Most of these products analyze the breath alcohol concentration of the driver to determine if the vehicle can be started. There are several related laws in the United State, Canada, and Australia. To be enforced on the recidivist of the drunk driving. Currently, the technologies of the anti-counterfeiting of drunk driving include the analysis of the driver's physiological signal, the behavioral analysis of the driver, the alcohol concentration analysis via alcohol detector, and the driver's face recognition system, also some important special information like the Digitized ID or Uni-card. However, the driver may suffer discomfort because he/she should wear the physiological sensors. For the behavioral analysis of the driver, the driving control signals of the vehicle are used to construct the control model of the driver. Moreover, the control signals and their corresponding recognition mechanisms are utilized to estimate the driver status.

One of the benefits of the suggested system is the anti-counterfeiting of drunk driving, which prevents drivers from drunken driving and cheat of driver's alcohol detection. It depends on the driver's facial image match by a serial image processes. It is suitable to be applied under the internal environments of cabin. By analyzing the facial features of drivers, the time of driver's exchange is detected, and the driver's identity is identified. Then the Digitized ID or Uni-card step come it after the facial process to check if the identified drivers registered before as drunk or not. When the cheat act of driver's alcohol detection occurred, the system will generate warning signals through a buzzer to notice the driver to take alcohol detection. The system detected the time of driver's exchange effectively, and identified different driver's identity successfully [10].

III. Connected Cars via Communication Networks

"Connected car" has become one of the buzzwords of the last few years as the potential for combining the automotive and Information and Communications Technology (ICT) industries becomes clearer. It's important to understand what the car can be connected to, and how these different connections an create opportunities for services and applications. Connecting the car to the passenger creates an infotainment opportunity including multimedia, and when GPS data is added, enables mapping and direction applications. Connecting to the cloud opens up telematics applications, including the potential to change the way insurance services are delivered, or cars are maintained. Connecting to other cars if done with a technology that enables acknowledgement of the message) enables fuel-efficiency and safety applications. Connecting to transport and other infrastructure also provides for better traffic management. The term for all of these connections together is V2X – vehicle-to-everything. Major players from the automotive and technology industries have stepped up connected car research activities over the last five years. Between 2010 and 2015, over 2,500 inventions relating to V2X (vehicle-to-everything) technologies were filed, while a further 22,000 patents relating to self-driving cars were also submitted during the same period.

Currently, every major automobile manufacturer is actively testing integral technologies for future connected vehicles. New players such as Tesla, Google, Apple, and Faraday Future are also investing heavily in this area. In 2016, every new car has the potential to be a “connected car” as infotainment services and software updates are provided via the Internet, and increasing numbers of vehicles are being fitted with lane changing, assisted braking and cruise control systems. Tesla’s Autopilot feature, currently in beta mode, already provides a limited amount of hands-free driving and is being continuously refined with over-the-air updates .

Between 2015 and 2020 nearly 184 million new connected cars will be produced, according to analyst company Gartner . The industry consensus is that we still have some way to go before we see mass production or adoption of autonomous cars, but that the technological developments available today will move us closer to that objective. The self-driving market is expected to reach critical mass within 15 to 20 years. By the end of 2035, 76 million cars will be in circulation worldwide . Connected and self-driving vehicles will have a profound impact on many industries, particularly in automotive, telecoms, logistics and insurance. The more intelligent cars become, the greater the need there is for them to incorporate cellular connectivity as standard. A report from Allied Market Research suggests that the global connected car market may generate revenues of $141 bn in total by 2020 as shown in Fig. 2. This paper looks at some example connected car applications, and the networks that will enable them – now, in the next five years, and further into the future.

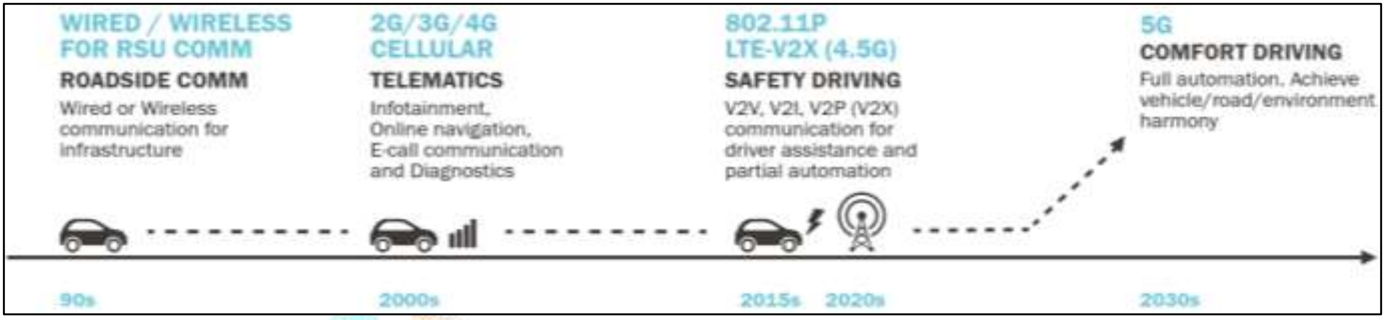
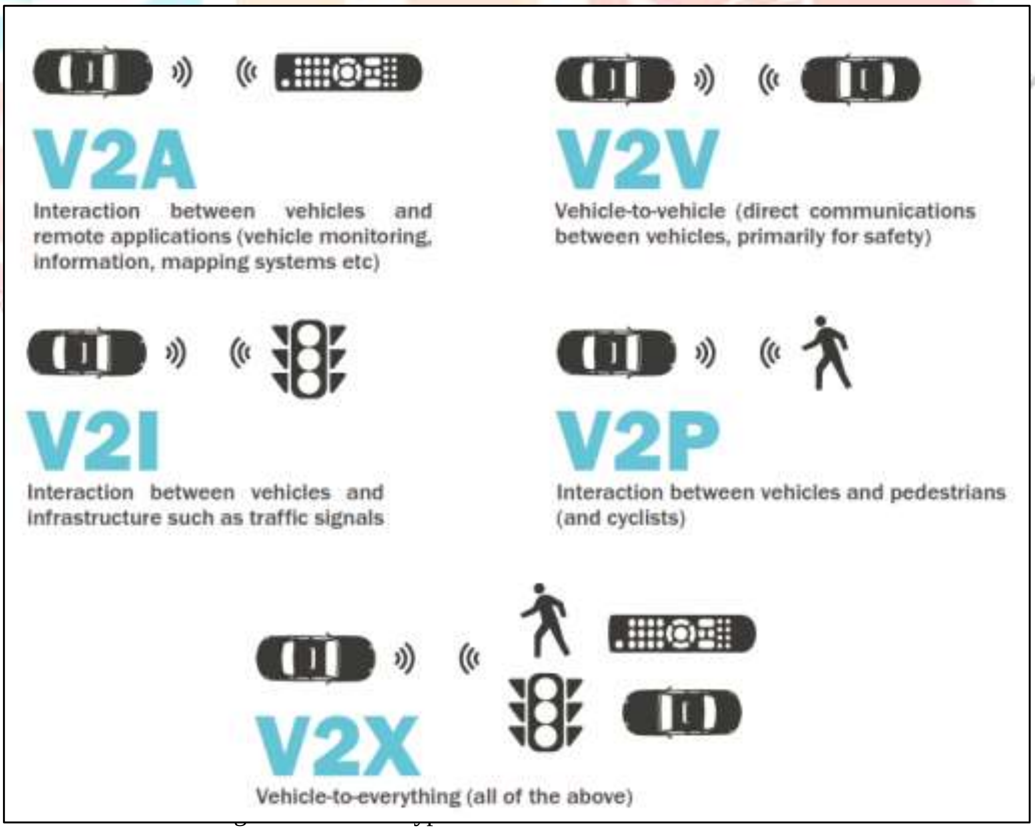

WIRED / WIRELESS FOR RSU COMM
ROADSIDE COMM
Wired or Wireless communication for infrastructure
2G/3G/4G CELLULAR
TELEMATICS
Infotainment, Online navigation, E-call communication and Diagnostics
802.11P LTE-V2X (4.5G)
SAFETY DRIVING
V2V, V2I, V2P (V2X) communication for driver assistance and partial automation
5G
COMFORT DRIVING
Full automation. Achieve vehicle/road/environment harmony
90s
2000s
2015s
2020s
2030s

Figure 2: Connected car technology evolution

There are very many connected car applications, but it is helpful to look at some examples and assess the demands that will place on communications networks. An early use case is infotainment: connection directly to the car can overcome some limitations of using smartphones in vehicles, such as the shielding of the metal structure inhibiting network performance. An integrated LTE module with an active antenna can significantly improve the user experience. Looking beyond the provision of infotainment, there are other types of use cases requiring advanced mobile connections, illustrated in the Fig. 3. Different types of communications are needed between vehicles and other vehicles, transport infrastructure, cloud-based and other applications, and even pedestrians or cyclists [11]:


V2A
Interaction between vehicles and remote applications (vehicle monitoring, information, mapping systems etc)
V2V
Vehicle-to-vehicle (direct communications between vehicles, primarily for safety)
V2I
Interaction between vehicles and infrastructure such as traffic signals
V2P
Interaction between vehicles and pedestrians (and cyclists)
V2X
Vehicle-to-everything (all of the above)

3.1 Connected Services: Available LTE Wi-Fi Hotspot

The built-in LTE Wi-Fi Hotspot* (vehicle must be on or in the accessory position for Wi-Fi to function) turns your vehicle into a reliable mobile hub, with great signal quality and bandwidth. It provides a better in-vehicle experience than your smartphone and is powered by your vehicle, so you’re not reliant on a mobile device battery. The built-in LTE Wi-Fi Hotspot* provides a better in-vehicle experience than your smartphone. The stronger signal means you have a fast and reliable connection. It is powered by your vehicle, so you are not reliant on a mobile device battery, and you can access your hotspot up to 50 feet (vehicle must be on or in the accessory position for Wi-Fi to function) from your vehicle. The built-in LTE Wi-Fi Hotspot is easy to use because it’s automatically on after initial setup and ready to connect to your mobile devices. The vehicle ignition needs to be in the “Run” or “Accessory” position for the Wi-Fi Hotspot to be active. The coverage for the built-in Wi-Fi Hotspot* depends on the wireless carrier network coverage. When you are in areas where coverage fluctuates, performance may be impacted. In a 2G-coverage area, the Wi-Fi Hotspot will not work. In a 3G-coverage area, streaming data or video to your devices may result in the degradation of your service. View the coverage map. Also, the vehicle ignition needs to be in the "Run" or "Accessory" position for the Wi-Fi Hotspot to be active [12].

IV. GPS AND IOT TRACKING

Since the turn of the millennium, one of the technical megatrends observed on the market is the replacement of isolated control units by intelligent (inter)connected devices, named today as the Internet of Things (IoT). Fundamentally, the IoT is considered as a network of physical objects with embedded sensors and communication capabilities allowing remote control or monitoring via an internet-like structure. Among the myriad of IoT devices available on the market today, GPS trackers are offering a wide scope of applications and benefits. The use of GPS trackers may be a great help in various situations, as their satellite-controlled positioning function can help to find persons in need of protection such as children, patients suffering from alzheimer disease, elderly persons or even pets who ran away. Being able to locate and find our loved ones using easy-to-use tracker systems offer security and peace of mind. But GPS trackers can also be used to locate and protect various types of assets such as vehicles, cars, bicycles or any valuable (and moving) object. In a business environment, fleet management is one of the applications offering immediate benefits and quick ROI of using tracking devices.

4.1 Fleet Tracking

Many applications and services can be offered using a combination of GNSS ("Global Navigation Satellite System") and IoT technologies. In a GPS tracker, the positioning sensors can calculate at any time the exact position of a moving unit and send it to a central system. This is the case for fleet management solutions which can use trackers in various situations. Fleet managers can use products like the MiniFinder® Zepto which is the world's smallest GPS tracker for fast connection via the vehicle diagnostics socket, OBD port. Once connected to the on-board diagnostics socket, it allows the fleet manager to monitor the position of the vehicle in real-time. The device being "Plug & Play", it can be installed and ready to run in less than a minute.

Several types of alerts can be configured with a GPS tracker designed for fleet monitoring: speed alert (to find out when a vehicle exceeds the preset speed), anti-sabotage alert (to detect unauthorized access and use of a vehicle) and geo-fencing alert (to be notified when the vehicle is located outside of the authorized perimeter). Once their vehicles on the road, fleet managers often lack insights on the performance and utilization of their fleets. Using GPS tracking technology bring many benefits to fleet managers: more accurate billing, lower costs for fuel and maintenance, use of the vehicles (detection of private use for example)… Doubtlessly, logistics and transportation is one of the application fields which can get immediate benefit of using IoT associated to GNSS. With such a technology combination, companies have the opportunity to efficiently organize and manage their fleets of vehicles without heavy investments [16].

4.2 Cellular IoT GPS Tracker

Whether it is scooters or shipments, the ability to keep track of your IoT devices as they travel in real time is crucial. Without this, businesses can be left scrambling, unaware of when their asset will arrive at its destination. Most asset tracking projects rely on cellular connectivity due to its nation-wide coverage and pre-built infrastructure. After all, connecting to 3G/4G using our smartphones is easy as long as we have a SIM card. But there's more to building asset tracking than simply relying on strong cellular connectivity. You need to choose hardware that will provide value to your operations year in and year out. It is important that you invest in a SIM-powered GPS tracker that enables you to consistently keep a watchful eye over your fleet of IoT devices. However, finding the perfect match is more difficult than it sounds as there are multiple variables to consider before you can confidently make a final decision.

Depending on your business, an "asset" can be anything from people to produce. As a result, there are certain qualities that a cellular GPS tracker should have to fit the specific needs of your project. For instance, industrial IoT projects would likely require a ruggedized cellular IoT GPS tracker that can handle extreme temperatures, dust, humidity and vibrations. For those that may be placed deep underground, antenna length can drastically affect coverage strength and range. Within flatbeds, reefers and tankers, cellular IoT GPS trackers that are waterproof or water resistant could provide additional flexibility in the case of a leak or flood.

In addition, industrial cellular GPS trackers that are used in hard-to-reach places and harsh environments are ideally power-efficient with some even boasting recharging capabilities. This is because limiting the amount of time and energy spent swapping batteries or performing maintenance cuts costs and keeps upkeep low. Some GPS trackers on the market will last as long as 10 years on a full charge depending on usage, providing IoT project managers with tons of valuable uptime to gain insight from. However, for wearable devices and other commercial applications, having a ruggedized cellular GPS tracker is not only unnecessary but could also be worse due to additional weight and size.

In many projects that involve wearable devices and asset tracking, cellular IoT GPS trackers need to be as small as possible to save space, lower weight and optimize power. Plus, it can provide IoT project managers with more design flexibility an important part of wearables. While this may have applications for industrial IoT projects as well also known as IIoT — geo-fencing can allow users to set geographical boundaries that assets cannot travel past without sounding an alert. This has a variety of different applications, from monitoring an e-scooter to make sure it doesn't leave the city limits, to ensuring an elderly relative does not leave the safety of their caregiver [17].

V. ESIM TECHNOLOGY

The ordinary SIM card has survived for quite a while, but it now finally looks like it is on its way out, instead, the eSIM, a much smarter technology, is here to save the day. Before we dive into what an eSIM is, it might be helpful to understand what a SIM is. As known SIM, which stands for "Subscriber Identity Module" basically contains the information that authenticates your identity to a carrier. In other words, the SIM card is what tells a carrier that you are you — and without it, carriers would not know that you're subscribed to their network, and thus would not let you use their cell towers. But learning about a standard SIM card is not why you're here. New phones like the Pixel 4, iPhone 11 Pro, and Motorola Razr boast of eSIM support, so it is a good idea to know exactly what that means. Here's everything you need to know about the new eSIM (See Fig. 4).

Figure 4: New eSIM Technology

An eSIM is exactly what it sounds like: An electronic, or embedded, SIM. Instead of a physical card, SIM technology is built right into your phone. It's a small chip that's used to authenticate your identity with your carrier. Of course, you probably have some questions about that. When traveling with a traditional SIM card, you may have to swap to another carrier's SIM card to keep your coverage. If you want to change carriers at home, you'll also have to physically replace your SIM card. With that in mind, does a built-in SIM mean you have to switch phones? Thankfully, no. In fact, one of the advantages of eSIM technology is that it makes it much easier to switch carriers. Instead of having to order a new SIM and wait around for it to arrive, you can switch to a new carrier straight from your phone. If you're a dual-SIM user, eSIM technology supports multiple accounts — and switching between them is super easy. With an eSIM, your phone has a few new settings devoted to your SIM card that allow you to switch between lines and carriers and manage accounts.

The Google Pixel 2 was among the first phones to support eSIM technology, and an app for managing your eSIM is available from the Google Play Store. Then, the iPhone XS came out, and it offered both a physical SIM card and an eSIM as a secondary, though the eSIM was only enabled later down the line through an iOS software update. Unfortunately, the Chinese version of that iPhone did away with the eSIM altogether instead offering a dual-SIM slot (a practice continued with the iPhone 11). That could suggest that Chinese carriers are less interested in adopting the new tech, which is bad news for those who were looking forward to using an eSIM to travel to China. The eSIM is helpful for another reason: It helps make devices smaller. Now, that may not matter all that much for phones (although a little extra room for battery capacity is always nice), but it could be extremely helpful for wearables. The Apple Watch Series 5 and Series 4 already have eSIMs, and that helps Apple keep the overall size down, which is vital for something you wear on your wrist [15].

VI. Governmental Identity

Trusted identity is a vital component of a well-functioning society. That is why improving security, slashing ID fraud and identity theft and creating an infrastructure of trust for new online access are high on every government's agenda, with a call for greater security features and the necessary legislation to implement them. Many advanced countries are now demonstrating that, beyond the security benefits for both states and individuals, national ID cards with their derived digital IDs can provide citizens and businesses with real services and benefits, without infringing upon new rules on data protection and civil liberties (See Fig. 5).

Figure 5: Secure national ID cards

Many countries are now upgrading their national documents and rolling out government-issued IDs in the form of a credit card which is called **Uni-Card**. These new ID documents are including high-security printing features to deter fraud [13].

6.1 Digital Identity Revolution

6.1.1 Fundamentals of digital identity

Digital identity can apply to things as well as to people. This is important to keep in mind in our world of connected devices and things. Just as businesses and systems need to know who they're interacting with, a thing (such as a connected car) needs to be able to recognize another thing (such as another car, a charging station, a drive-through payment terminal, a tollbooth, etc.) to enable secure new mobility functions and experiences.

Authentication is simply the trusted recognition of the user's digital identity: Who is this? Is it really who he claims to be?

Authorization goes one step further: Based on their authenticated digital identity, what should this person be allowed to do? What applications and data should he be able to access based on factors such as his business role or relationship, customer subscriptions, account status, current scenario and so on?

Single sign-on simplifies the customer journey by allowing customers to log in once for access to all of your applications that they've signed up for, rather than having to log in application-by-application. Frictionless login across applications isn't just convenient; it's also fast becoming an industry standard. Meeting this expectation is increasingly important for maintaining a brand's credibility and trustworthiness.

Federation extends single sign-on beyond your organization to encompass your ecosystem partners as well. In addition to making life easier for customers, federation positions your company as a trusted identity provider and go-to access point for a broad range of content and services.

Simple multifactor authentication is, as its name suggests, the use of multiple factors to authenticate who someone or something is. Multifactor authentication typically uses a combination of identity types such as something they know (e.g., a password), something they have (e.g., a key fob or an iPhone app) and something they are (e.g., biometrics, such as a thumbprint or retina pattern).

Privacy is critical. Personal digital data is precious — customers have to be able to trust you with theirs. As the number of connected devices and things grows, companies must be able to secure the user experience wherever and however services are used, tailor it to the customer's data-sharing preferences and ensure that their data is never used in a way they haven't approved.

Security becomes more challenging all the time — and more important. As consumers become more mobile and do more online in more ways, businesses need to ensure continuous protection not just at login, but throughout each digital session. This includes responding to threats in context by asking for additional identity verification when something unusual takes place, like a resource request from an unfamiliar location or device.

6.1.2 From eID to Mobile ID

The delivery of successful and secure digital identity is fundamental to the modernization of states and the dematerialization of public services. It is also critical to support the digital transformation of their economies and the development of trusted public and private digital services. Governments are ideally placed to deliver this foundation for our digital future. Whether they are seeking to protect citizens online, boost economic growth, achieve greater efficiency or reduce the spiraling cost of public services, what is certain is that any national digital identity platform must be based on a backbone of Trust. One of Thales' greatest assets is the ability to extend smartcard-based national eID and digital identity schemes to mobile.

6.1.3 Mobility and Convenience

Accessibility is key to the success and adoption of digital services. Given the sheer volume of devices worldwide, smartphones offer a compelling proposition for governments seeking to provide citizens with secure and convenient access to online public services. The latest report from Juniper Research even forecasts over 3 billion citizens around the world will be equipped with a government-initiated mobile ID app by 2024 Users want a secure digital identity and frictionless mobile experience when transacting online. They are ready for mobile identity and want to replace passwords with simple mobile-based PINs and/or biometric authentication to take full advantage of the wealth of fast and convenient digital services available.

6.1.4 Mobile ID Schemes

Governments around the world are capitalizing on the mobile revolution. Many national mobile ID initiatives are underway, notably including Estonia, Norway, Belgium, Qatar, Oman, The Netherlands, Iceland, Finland, Moldova, etc... Many of these initiatives are either government-driven or government-supported to serve the entire economy by providing a single trusted digital identity to protect both public and private online services. Government-backed digital ID schemes can quickly achieve critical mass by focusing initially on public services and then expanding out to serve the broader economy. Once a scheme has a critical mass of active users, it becomes an extremely attractive proposition for the private sector, which can leverage the national digital ID scheme to secure their online channel or securely integrate new customers [14].

6.2 New Mobility and Digital Identity: The vehicle for success

In the physical world, each person is unique, with their own set of relationships, personal preferences, financial profile, physical characteristics, past behaviors, future plans and so on, the attributes that make up their identity. Being able to recognize each customer's unique identity makes it possible for companies to do business with them to know what kind of services to provide and recommend, charge and track payments accurately, measure and enhance satisfaction, and provide the kind of continuity that delivers optimal value for customers and providers alike. Digital identity is the extension of this concept into the digital realm and it's central to modern connected life. The ability to recognize and manage individual customer identities effectively is the foundation of:

- Trust, as companies safeguard each customer's personal information and use it with consent for their benefit.
- Consistency, by harmonizing identities and connecting user identity record across organizations and industries.
- Experience, making it possible for companies to know their customers, personalize services, simplify online interactions and increase satisfaction.
- Privacy, allowing customer transparency and choice on what where, and how their personal data is used.
- Security, helping companies protect against identity fraud, hacks and breaches.
- Innovation, as companies use identity across industries to capitalize on synergies and deliver new and dynamic connected experiences powered by context.

Most fundamentally, digital identity makes it possible to take a customer-centric approach to business. By building trusted relationships and delivering more personalized and consistent experiences, companies can improve customer retention, strengthen their brand, increase their share of wallet and achieve competitive differentiation. So, digital identity is the ultimate "vehicle for success" that must underpin the new mobility. To have a clearer understanding of that role, it's helpful to review a few of its core concepts. There are many ways the tools we use to provide and protect a secure digital identity can add value to the present-day development trends in connected and autonomous cars. For example:

- **Personalization and services: Feature on demand**

  For the most part, today's cars are personalized during the purchasing process not afterwards. If buyers subsequently wish they'd opted for more horsepower, matrix-LED lights or additional connectivity or GPS features, their only option is to try their luck with expensive after-sales projects. With digital identity, both owned and shared connected cars can allow flexible personalization of their software-enabled features on either a per-ride or ongoing basis. The identity of the user is linked with the identity of the car to sync the user's preferences with the car's configuration and trigger the corresponding monetization processes.
- **Identity for privacy and compliance**

  Some connected car capabilities raise delicate issues for user privacy. As part of predictive maintenance, a car's ECUs may push alarm messages to the carmaker's back end to signal a problem with the engine, gearbox or brakes. This message can include driven speeds, gear and RPM history, and geographical locations. And there's the catch: A driver or user may appreciate the alert there's something wrong with the car and where to find the next garage, but may not necessarily want to share information about how the car is being used. The carmaker needs a way to let users and drivers choose which data to share a preference that can be linked to their digital identity.

- **Connected car security and safety**

A modern car's functions and features are controlled by upwards of 100 complex ECUs whose interaction is critical for the safety of the passenger and of the car. Equipping each ECU with its own unique and secured digital identity makes it possible for these control units to identify themselves to each other when sending messages, helping prevent hackers from injecting malicious messages to cause malfunctions. These examples show how much even today's connected cars depend on secure identification of different parts of the cars to each other, as well as of the entire car to its driver or owner, to ensure both a good user experience and the protection of the data being generated during each ride. Designing digital identity and its corresponding tools into the vehicle from the very beginning provides a vital backbone for security, privacy and monetization.

6.3 IAM and CIAM

Initially, digital identity was used primarily as a way for businesses to control access to their systems by their own employees. Based on your digital identity, verified through your username and password, you would be granted to the appropriate applications and data for your role. By the same token, you would also be prevented from accessing applications and data that you shouldn't, aiding customer privacy and security. Digital identity also makes it possible to track your behavior over time, helping companies meet requirements for auditing, regulatory compliance, internal security and the like. Within the tech industry, technologies to manage digital identity fall into the Identity and Access Management (IAM) category.

Digital identity has now expanded to encompass personalization and quality of experience as well. As any successful business knows, the better you know your customer, the better service you can provide, helping you drive loyalty, growth and revenue. The personal information customers share with you to establish an identity with your organization, complemented with personal data from additional sources, helps you understand their individual needs more fully. This in turn helps you cross-sell, upsell and deliver more personalized experiences. Of course, security and control remain paramount as well. Reflecting the customer-centric orientation of this way of thinking about digital identity, this technology category is called Customer Identity and Access Management (CIAM).

VII. Vehicle Security Systems

The Vision Sciences Society (VSS) which is a nonprofit membership organization of scientists who are interested in the functional aspects of vision. VSS hold an annual forum scientists from the broad range of disciplines that contribute to vision science [7]. Nowadays, the automobile sector is one of the hottest applications, where vehicles can be intelligent by using IoT technology. But unfortunately, these vehicles suffer from many crimes. Hence it has become a big challenge for the IoT to avoid such these crimes from professional thieves. This paper presents a proposal for the development of a vehicle guard and alarm system using biometric authentication based on IoT technology. Whereas, for vehicle security issues; the proposed system VSS - IoT gives only full access for authorized vehicle's driver based on the interface of Communication unit inside the vehicle with the internet which is linked by the Pi camera, PIR sensor, and smart-phone.

Access rejection to the vehicle security system from the unauthorized person is a problem, but unfortunately, the actual problem is how to identify him/her face. Most robbed vehicles systems will help to get recovered, but the crime has already happened. Therefore, a good vehicle systems should be developed to offer a security based on new technologies like the Internet of Things (IoT). The vehicle system must employ user authentication for access control using biometric authentication based on IoT in a real-time. Moreover, the system should monitor the vehicle for any suspicious activity inside it. The surveillance system must keep the vehicle secured by notifying the authorized driver via his/her Mobile Application/Email in case of any unauthorized person, or any intrusion try to access the vehicle security system. The introduced system will add an alternative method for authentication instead of biometric which depends on the saved images even if in the communication module inside the vehicle or using IoT services by using the national digitized ID card or which is called UniCard. Also, the system should provide some extra features like vehicle location, within the same hardware without increasing complexity and cost.

The IoT performs intelligent functions, which lead to avoid vehicle theft. Many authors have been working on vehicle security systems to provide the best mechanisms not only concerning with the theft of vehicle contents but also the loss of vehicles, and the personal security requirements of the vehicle's owner. According to their works; they have developed a vehicle security systems based on "Biometric Authentication" type such as eye, finger, face recognition, etc. This section describes some relevant collaborations which are proposed in recent years. The recent systems used biometric authentication to access the vehicle. They showed that the system was simple and provided better results in various light conditions.

The objective here is offering advanced security system for any vehicle which is based on wireless communication and Bluetooth module. GSM module should be used for sending and receiving messages. The vehicle's owner can control the engine/ignition and turn it off at any time. Authors also suppose the system can use a password through the keypad (supposedly with ≤ 3 chances), that beside the using of national digitized ID card or which is called UniCard which controls the safety of vehicle locker door and wearing of a seat belt. Also, The controller is connected to a Bluetooth module.

7.1 Proposed Vehicle Security System

The main goal of the proposed system is to detect and recognize the faces of professional thieves. Moreover, the proposed system provides a low cost, increase the simplicity and user-friendly is the most important to implement an embedded real-time vehicle security system which using the national digitized ID card or which is called UniCard. Therefore, the system must get the identity of owner vehicle's driver first, then provide him an authorization to access his/her vehicle system. The proposed system has a combination of biometric techniques, embedded devices and IoT technologies to design effective surveillance and alert vehicle security system. Fig. 6 shows the basic flowchart of the entire vehicle security system. It illustrates the series of events starting from intrusion event up to the point when it sends out an alert.

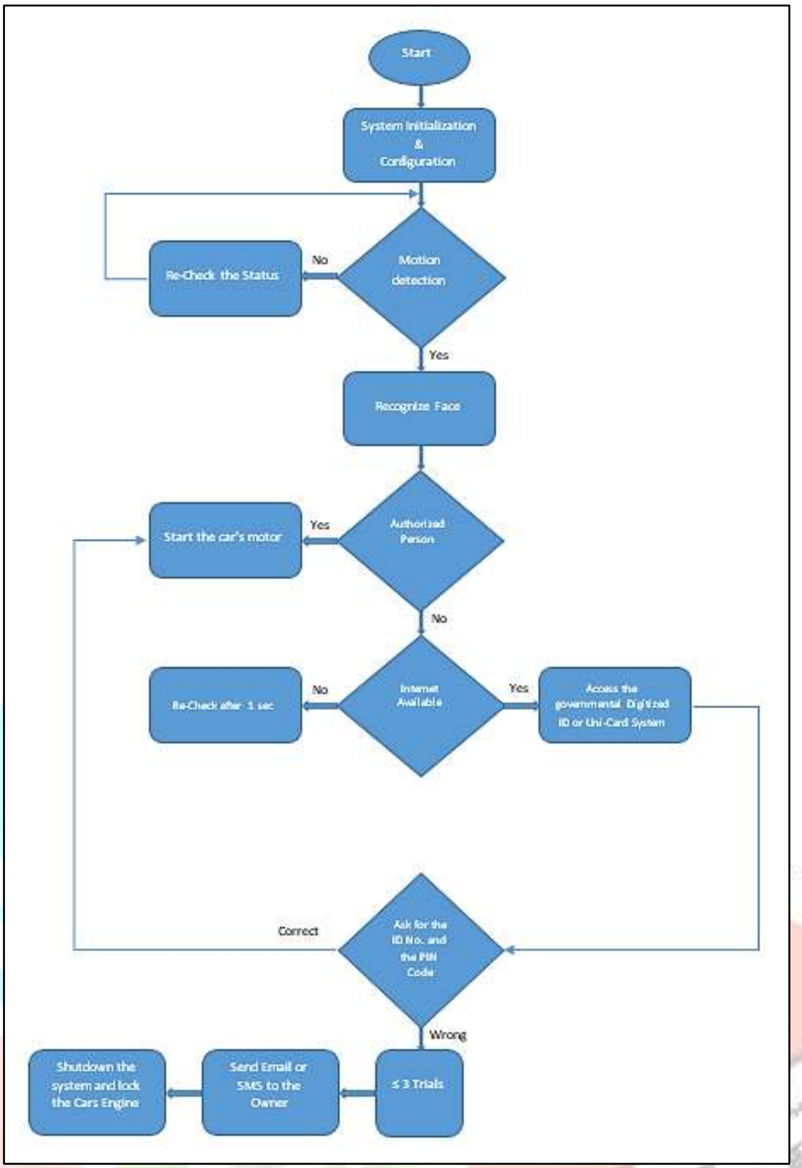

Start
System Initialization & Configuration
Motion detection
No
Re-Check the Status
Yes
Recognize Face
Authorized Person
Yes
Start the car's motor
No
Internet Available
No
Re-Check after 1 sec
Yes
Access the governmental Digitized ID or Uni-Card System
Correct
Ask for the ID No. and the PIN Code
Wrong
≤ 3 Trials
Send Email or SMS to the Owner
Shutdown the system and lock the Cars Engine

Figure 6: Basic Flowchart of entire Vehicle Security System

Fig. 7 shows the suggested Embedded system architecture of Vehicle Security System served by IoT.

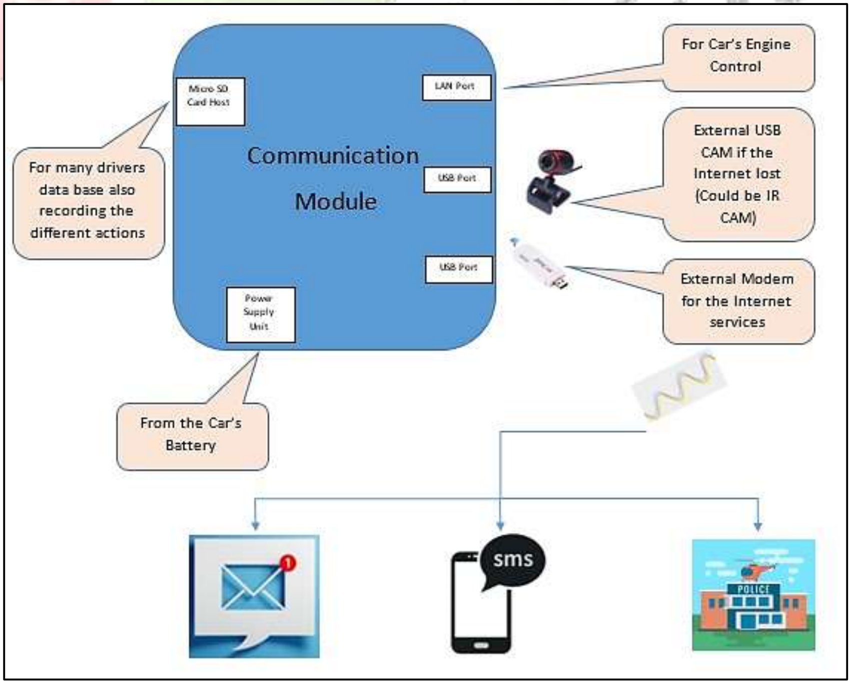

Communication Module
Micro SD Card Host
LAN Port
USB Port
USB Port
Power Supply Unit
For many drivers data base also recording the different actions
For Car's Engine Control
External USB CAM if the Internet lost (Could be IR CAM)
External Modem for the Internet services
From the Car's Battery
sms
POLICE

Figure 7: Embedded system architecture of Vehicle Security System

The proposed system' network also connects to other networks via Wi-Fi. Also, this system executes the following tasks:

- **Importing libraries and packages**: These libraries are predefined and help to make the interface modules work properly.
- **USB Camera setting and configuration** : After these configuration settings of USB Camera, the system was rebooted. This was done to ensure that the camera was allocated enough space in memory.
- **Generating and sending Messages or Emails** : It is necessary to generate and send Message or Email to the predefined subscriber after configuring the system. Multipurpose Internet Mail Extension (MIME) package used to generate the attachment mail. MIME supports characters and non-text attachments like (audio, video and application programs), etc [4].

VIII. Conclusion

This paper introduces an intelligent vehicle security system powered by IoT capabilities using a secure, efficient, low-cost, and low power processing microchips and connected to the Internet all the time. The new system uses camera for facial recognition that captures digital image by extracting the best features offering improving to the security of the automobile sector. It is integrated with Global System for Mobile (GSM) and Global Positioning System(GPS) for real time monitoring and also to send text messages and the vehicle location on Google map or similar services. With the adoption of standards and community awareness, this technology will become more and more acceptable. Integrating the Digitized ID or the UniCard governmental system offers additional layers of security and more authentication and authorization features to come. The system can be used to reduce the growing vehicle theft and allows the owner to identify the intruder through the face recognition system, correlating with law enforcement and authorities' databases ensure safety of vehicle and the driver. The vehicle owner has full control to stop the vehicle at any location and controlling the engine remotely. The vehicle status at all time is reported directly to law enforcement. Multiple communication methods are utilized such as LTE, GSP, GPS or even WiFi, the system operates properly in all-weather condition.

IX. Acknowledgments

The authors would like to thank ***October 6 University (O6U)***, ***Egypt*** and ***Park University***, ***USA*** for their support to introduce this research paper in a suitable view and as a useful material for researchers. The authors also would like to thank their colleagues who provided insight and expertise that greatly assisted the research.

References

[1] C. Nandakumar, G. Muralidaran and N. Tharani, "Real Time Vehicle Security System through Face Recognition," International Review of Applied Engineering Research, ISSN 2248-9967, Volume 4, Number 4, pp. 371-378, © Research India Publications, 2014, India. [Online] Available:
http://www.ripublication.com/iraer.htm

[2] Sundari, Y. B. T., Laxminarayana, G., and Laxmi, G. Vijaya, "Anti Theft Mechanism Through Face recognition Using FPGA," International Journal of Advancements in Research and Technology, ISSN 2278-7763, vol.1, no. 6, p.46-49, November 2012, India. [Online] Available:
https://ui.adsabs.harvard.edu/abs/2012IJART...1f..46S/abstract

[3] Dina A. Bahr, and Osama A. Awad, "LTE based Vehicle Tracking and Anti-Theft System using Raspberry Pi Microcontroller," Iraqi Journal of Information and Communications Technology(IJICT), Vol. 2, Issue 1, March 2019, Iraq. [Online] Available:
https://ijict.edu.iq

[4] Ahmed A. Elngar* and Mohammed Kayed, "Vehicle Security Systems using Face Recognition based on Internet of Things," published by De Gruyter, Open Comput. Sci. 2020; 10:17–29, Open Computer Science, 20 Mar 2020, Volume 10: Issue 1. https://doi.org/10.1515/comp-2020-0003. [Online] Available:
https://www.degruyter.com/view/journals/comp/10/1/article-p17.xml

[5] Sundari, Y. B. T., Laxminarayana, G., and Laxmi, G. Vijaya, "Anti Theft Mechanism Through Face recognition Using FPGA," International Journal of Advancements in Research & Technology, Volume 1, Issue6, November-2012-ISSN 2278-7763, USA. [Online] Available:
https://ui.adsabs.harvard.edu/abs/2012IJART...1f..46S/abstract

[6] C. Nandakumar, G. Muralidaran and N. Tharani, "Real Time Vehicle Security System through Face Recognition," International Review of Applied Engineering Research, ISSN 2248-9967 Volume 4, Number 4 (2014), pp. 371-378, © Research India Publications. [Online] Available:
http://www.ripublication.com/iraer.htm

[7] Vision Sciences Society, "Online Virtual VSS 2020," June 19-24, 2020, USA. [Online] Available:
https://www.visionsciences.org/

[8] Find, connect, shape your Victorian Government, "The National Driver License Facial Recognition Solution." [Online] Available:
https://www.vic.gov.au/national-driver-licence-facial-recognition-solution

[9] BBC News, "ICE and FBI used facial recognition to search driver-license databases," US & Canada, 8 July 2019. [Online] Available:
https://www.bbc.com/news/world-us-canada-48907026

[10] Yu-Sung Chen, Chia-Tseng Chen, Jia-Xiu Liu and Chung-Chih Tsai, "Anti-Counterfeiting System of Drunk Driving Using Driver's Facial image Identification ," Automotive Research & Testing Center (ARTC), Copyright © 2011 SAE International, April 2011, DOI: 10.4271/2011-01-0210, R & D Division, Taiwan. [Online] Available:
https://www.researchgate.net/publication/290093069_Anti-Counterfeiting_System_of_Drunk_Driving_Using_Driver's_Facial_image_Identification

[11] Cross-Industry Whitepaper Series: Empowering Our Connected World, "Communications Networks For Connected Cars," Copyright © 2016 Huawei Technologies Co., Ltd. Available: HUAWEI-WHITEPAPER-CONNECTION-CARS-Final.pdf

[12] OnStar, "Connected Services: Available 4G LTE Wi-Fi® Hotspot," [Online] Available:
https://www.onstar.com/us/en/support/4glte/

[13] THALES, “Identity Documents & Solutions,” 2019 Thales Group. [Online] Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity

[14] THALES, “Identity Documents & Solutions,” 2019 Thales Group. [Online] Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/digital-identity-services/mobile-id

[15] Mark Jansen and Simon Chandler, “What is an eSIM? Here’s everything you need to know,” Digital Trends, May 30, 2020. [Online] Available: https://www.digitaltrends.com/company-contacts/?itm_medium=footer

[16] Marc Kavinsky, “Tracking Based on GPS and the “Internet of Things,” IoT.Business.News, April 16, 2020, Copyright © 2011-2020 IoT Business News - edited by VisiQuest, France. [Online] Available: https://iotbusinessnews.com/2020/04/16/54510-tracking-based-on-gps-and-the-internet-of-things/

[17] Cody Lirette, “How to Choose the Right Cellular GPS Tracker for your IoT Project,”, © 2015-2020 SORACOM, INC., August 27, 2019. [Online] Available: https://www.soracom.io/blog/how-to-choose-the-right-cellular-gps-tracker-for-your-iot-project/

[18] Hussam Elbehiery, Khaled Elbehiery, " Unicard; National Identity Evolution " The International Journal of Engineering and Science (IJES), Volume 9, Issue 01, Series II, Pages PP 84-102, ISSN (e): 2319-1813 ISSN (p): 23-19-1805, January 2020. (DOI:10.9790/1813-09010284101) [Online] Available: http://www.theijes.com/Vol9-Issue1.html

[19] Hussam Elbehiery, Khaled Elbehiery, "National Identity Evolution" IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 10, pp.1-12, India, ISSN: 2348 – 7968, October 2019. [Online] Available: http://ijiset.com/vol6/v6s10/IJISET_V6_I10_01.pdf

[20] U.S. Department of Health & Human Services. “What is the difference between isolation and quarantine? ,” HHS.gov, USA, December 2019. [Online] Available: https://www.hhs.gov/answers/public-health-and-safety/what-is-the-difference-between-isolation-and-quarantine/index.html

[21] American Medical Association (AMA), “Ethical Use of Quarantine & Isolation,” January 2020. [Online] Available: https://www.ama-assn.org/delivering-care/ethics/ethical-use-quarantine-isolation

[22] GeeksforGeeks, “Computer Network | AAA (Authentication, Authorization and Accounting).” [Online] Available: https://www.geeksforgeeks.org/computer-network-aaa-authentication-authorization-and-accounting/

[23] Serena Reece, “What is AAA security? An introduction to authentication, authorization and accounting,” Codebots Blog, Nov 27th, 2018. [Online] Available: https://codebots.com/application-security/aaa-security-an-introduction-to-authentication-authorisation-accounting

[24] UN Legal Identity Agenda, “Impact of COVID-19,” United Nations, Department of Economic and Social Affairs, Statistics Division, 1June 2020. [Online] Available: https://unstats.un.org/legal-identity-agenda/covid-19

[25] Luana Pascu, “Argentina enables remote digital ID processing for mobile during COVID-19 crisis,” Biometrics Research Group, Inc., Biometric Update.com, Apr 24, 2020. [Online] Available: https://www.biometricupdate.com/202004/argentina-enables-remote-digital-id-processing-for-mobile-during-covid-19-crisis

[26] Mahesh R. P., and Imdad R., "IoT Based Embedded System for Vehicle Security And Driver Surveillance", Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018), IEEE Explore Compliant Part Number: CFP18BAC-ART; ISBN:978-1-5386-1974-2.

[27] Vivek K. S., Soumitra M., and Harshit M.," Car Security using Internet of Things", 1st IEEE International Conference on Power Electronics Intelligent Control and Energy Systems (ICPEICES2016), 978-1-4673-8587-9/16/31.00 ©2016 IEEE.

[28] Tabassum J. Kh., M.R.Bhadange, Pooja S. P., Vinaya S., "Smart Vehicle Monitoring System Using Raspberry Pi", Spvryan’s International Journal of Engineering Sciences and Technology (SEST) , 3 (2), PP. 1 of 7,2016.

[29] Liu Z. , Zhang A. and Li S. , "Vehicle anti-theft tracking system based on Internet of things", Vehicular Electronics and Safety (“ICVES”), "IEEE International Conference” on, Dongguan, 2013, pp. 48-52., doi: 10.1109/ICVES.2013.6619601.

[30] ArunSasi and Lakshmi R. N., "Vehicle Anti-Theft System Based On An Embedded Platform", in IJRET: International Journal of Research in Engineering and Technology, 2 (9), 2013.

[31] Tahesin A., Prajakta Ch., Vidhi P., Megha G., Debajyoti M., "An Attempt to Develop an IoT based Vehicle Security System" ,2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), 0-7695-6618-9/18/31.00, 2018 IEEE, DOI 10.1109/iSES.2018.00050.

[32] Jian X. and Haidong F., "A Low-cost Extendable Framework for Embedded Smart Car Security System", Proceedings of the 2009 IEEE International Conference on Networking, Sensing and Control, Okayama, Japan, March 26-29, 2009.

[33] Shruthi K., Ramaprasad P., Ray R. ,Naik M. A. and Pansari S., "Design of anti-theft vehicle tracking system with a smartphone application" 2015 “International Conference on Information Processing” (ICIP), Pune, 2015, pp. 755-760. DOI:10.1109/INFOP.2015.7489483.

[34] Narayan T. D. and Ravishankar S., "Face Detection and Recognition using Viola-Jones algorithm and fusion of LDA and ANN", IOSR Journal of Computer Engineering (IOSR-JCE), 18(6), PP 01-06, 2016.

[35] Kumar K. S., Shitala P., Vijay B. S., Tripathi R. C., "REAL TIME FACE RECOGNITION USING ADABOOST IMPROVED FAST PCA ALGORITHM", International Journal of Artificial Intelligence and Applications (IJAIA), 2(3), July 2011.

[36] Shaik M. A. et al. "An Inexpensive Security Authentication System Based on a Novel Face-Recognition Structure", International Journal of Engineering Trends and Technology (IJETT), 4(9), 2013.

[37] Mohammad D., Amin A. and Olivier D., "Face Detection using Viola and Jones Method and Neural Networks", International Conference on Information and Communication Technology Research (ICTRC2015), pp. 40-43, 978-1-4799-8966-9/15/31.00, IEEE 2015.

[38] Ahmed A. E., "IoT-based Eflcient Tamper Detection Mechanism for Healthcare Application", International Journal of Network Security, 20(3), PP.489-495, May 2018 (DOI: 10.6633/IJNS.201805.20(3).11).

[39] Siddarth R., Dattatreya P. and Sadique N., "Face recognition using PCA and LDA: Analysis and comparison", IEEE International Conference on Advances in Recent Technology in communication and Computing, pp. 6-16,2013.

[40] Varsha G. and Dipesh Sh., "A study of various Face Detection Methods", International Journal of Advanced Research in computer and communication Engineering, 3(5), May 2014.

[41] Bavya R. and Mohanamurali R., "Next generation auto theft prevention and tracking system for land vehicles", "Information Communication and Embedded Systems"(ICICES), International Conference on, Chennai, 2014, pp. 1-5, doi: 10.1109/ICICES.2014.7033987.

[42] Zhixiong L. and Guiming H., "A Vehicle Anti-theft and Alarm System Based on Computer Vision", IEEE International Conference on Vehicular Electronics and Safety, 2005. DOI: 10.1109/ICVES.2005.1563666.

[43] Sarvesh V. A., Chetana R., "Face Recognition System for Unlocking Automobiles Using GSM and Embedded Technology", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, (An ISO 3297: 2007 Certified Organization), 5(7), July 2016.

[44] Christina Ma., Fernandez D., Kristina J. E. G., Aubrey R. M. L., Ron J. J. R., Argel A. B. and Elmer P. D., "Simultaneous Face Detection and Recognition using Viola-Jones Algorithm and Artificial Neural Networks for Identity Verification", pp. 672-676, 2014 IEEE Region 10 Symposium, 2014.

[45] Turk M. A. and Pentland A. P., "Eigenfaces for Recognition", Journal of Cognitive Neuroscience, 3(1), PP. 71-86, 1991.

[46] The ORL face database: http://www.cl.cam.ac.uk/Research/DTG/attarchive/facedatabase.html.

[47] Ebrahimpour R., Nazari M., Azizi M. and Amiri A., "Single Training Sample Face Recognition Using Fusion of Classifiers", International Journal of Hybrid Information Technology, 4(1), January, 2011.

[48] Novosel R. ,Meden B. , Emersic Z. , Struc V. and Peer P., "Face recognition with Raspberry Pi for IoT Environments", International Electro technical and Computer Science Conference ERK 2017, At: Portorož, Slovenia, September 2017.

[49] Saurabh P.Bahurupi, D.S.Chaudhari "Principal Component Analysis for Face Recognition" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[50] Nicolas Morizet, Frédéric Amiel, Insaf Dris Hamed, Thomas Ea, "A Comparative Implementation of PCA Face Recognition", 14th IEEE International Conference Electronics, Circuits and Systems", pp.865868, ICECS 2007.