# Risk Assessment of Attack in Autonomous Vehicle based on a Decision Tree

Sara FTAIMI[1], Tomader MAZRI[2]
Laboratory of Advanced Systems Engineering, Ibn Tofail University, Kenitra, Morocco

***Abstract*—Risk management has become increasingly essential in all areas, and it represents a cornerstone of the Safety Management System. In principle, it brings together all the procedures to identify and evaluate risks to improve systems performance. With the development of the transportation system and the appearance of intelligent ones (ITS) that are changing citizens' mobility nowadays, the risks associated with them have also increased exponentially. In ITS, vehicles can reach 100% autonomy since they are equipped with sensors to move safely. The vehicle's architecture and embedded sensors enfold inherent vulnerabilities that attackers may exploit to craft malicious acts. In addition, vehicles communicate with each other and with the road infrastructure via vehicular adhoc network (VANET) and may use Internet connections, raising the risk that an attacker performs malicious actions and may take control of a vehicle to perform terrorist acts. This paper aims to draw attention to the risks associated with autonomous vehicles (AV) and the interest in evaluating flaws inherent in AV. For this purpose, our paper will extensively detail a new approach to assess the risk of attacks targeting autonomous vehicles. Our proposed approach will use a decision tree model to predict risk criticality based on the probability of attack success and its impact on the targeted system.**

***Keywords*—Vehicular adhoc network; intelligent transportation system; decision tree; risk assessment; impact; autonomous vehicle; attacks***

## I. Introduction

The emergence of the smart city concept has brought several sub-concepts to the forefront, like transportation which is very important in smart cities. Making transportation intelligent will facilitate the mobility of citizens, which is a major concern in smart cities. Every second, a citizen uses a mode of transportation to go to work or school or even to travel. Making these systems intelligent will make citizens satisfied and facilitate their travel by enriching users with advanced information on traffic, real-time operating information on local convenience, seats. Resulting in reduced travel time for citizens and improve their safety and comfort and make the experience enjoyable. Therefore, the benefit of ITS is not restricted to control and give information on traffic jams, but also to reduce the rate of accidents because, in several studies, the human factor is the cause of a very high percentage of accidents. In an intelligent transportation system(ITS), we will have autonomous vehicles. These vehicles are based on the information collected by the several sensors installed on-board the vehicles and on machine learning algorithms that analyze this information and make decisions (whether the vehicle should stop or continue its trajectory), besides the infrastructure such as roadside units and base stations, installed all along the road. The vehicle will communicate with each other via vehicle to vehicle communication, and the infrastructure will communicate with the vehicle by sharing with them information about the status of the road via infrastructure to vehicle communication. Nowadays, vehicles are equipped with several ports to connect phones or other devices, and those devices are connected to the Internet, which presents a door for an attacker to conduct their attack. The security of vehicular Adhoc networks (VANET) and the different port of the vehicles besides the sensors installed in the vehicle represent a major challenge for the ITS. The security in ITS is critical because if an attacker could control a vehicle, he could cause an accident or steal the vehicle to cause a terrorist attack, and this will cause dangerous damages such as the loss of life and the perturbation of the whole ITS. Several kinds of research in the field of intelligent transport focus on the security aspect. The importance of this paper resides in the fact that unfortunately in the literature there is no work related to the risk in relation to the field of transport and especially the attacks on autonomous vehicles. In This article, we will study the assessment of risk in the context of an autonomous vehicle. It is very important in an ITS to measure risk, prevent dangerous damages, and make our system more resistant to attacks. This study will focus on the attack on the autonomous vehicle since attacks in ITS cames from the vehicle itself or the network. Therefore to measure the risk of attack, we need to calculate the probability of attack success because an attack that has a probability of attack success equal to zero could not harm our system because it could not happen, while an attack with a high probability of success should be taken into consideration while measuring risk. So we propose to implement a decision tree that will predict the probability of success of an attack.

In this article, we will create a decision tree that will predict the class of probability of attack success. Then we will create a decision tree to predict the risk based on the probability of attack success and the impact of the attack. The paper's structure will be as follows: we will start by presenting risk management and our proposed scheme, which contains two subsections. In the first subsection, we conduct a study on identifying risk threaten an autonomous vehicle, i.e., interfaces that attackers can exploit to produce an attack besides the attack in each interface. In the second subsection, we will assess risk by measuring the probability of attack success using a decision tree, and we will also describe the impact of attacks on an autonomous vehicle (AV). Furthermore, finally, we will present the risk assessment by using a decision tree based on two criteria: the probability of attack success and the impact of attack and conclusion.

## II. Risk Management

In our daily lives, we are exposed to risks. The development of technologies made this risk bigger and bigger, especially in the intelligent transport system where we will have a 100% autonomous vehicle (with no driver intervention), which makes any safety violation very dangerous. Therefore, it is essential to start with risk management more than ever to avoid any danger such as death. In this section, we propose to study risk management in the context of the ITS by starting with the identification of all interfaces that can pose a loophole for an attacker to start his attack, and after that, we will analyze risk by using a machine learning algorithm that will predict the probabilities of success of an attack and measure the risk. The measure of risk will be very helpful in preventing attacks that can be very damaging for the citizen and the ITS.

### A. Proposed Scheme

We will be based on the risk management scheme to start our proposed algorithm to predict risk in an autonomous vehicle. Risk management identifies the possible risks in advance, analyzes them, and implements safety measures to decrease and reduce the risk. As shown in Fig. 1, risk management starts by identifying risk, assessing the risk, and controlling the risk [1].

*1) Risk identification:* Attacks on ITS can come from two systems, the vehicle itself and the network. In our study, we focused on attacks against autonomous vehicles(AV). Attacks that can threaten an AV can come from four interfaces described in Fig. 2. In this section, we will present the interfaces that have vulnerabilities and the attacks that have occurred by exploiting these interfaces. Table I summarizes the result found.

*a) Buses and ports*

*i) CAN:* The Controller area network (CAN) is an electronic communication bus defined by the ISO 11898 standards, well known for its low cost. It allows communication between the different systems or electronic control units (ECU) of the vehicle. However, the CAN protocol is exposed to several inherent vulnerabilities, such as broadcast transmission. The CAN protocol sends the packet to all the other nodes without exception to transmit the information to a specific node. Therefore, if there is a malicious node, it can easily spoof all transmitted frames from other nodes.

Moreover, since it does not support the identification mechanism [2], each node must decide for itself whether the packet should be rejected or supported. As a result, a receiving node cannot differentiate between valid and false frames. This feature helps a malicious node easily hide its identity and send false frames to other nodes connected to the CAN bus to control the vehicle. Among the problems encountered when using CAN is the ID-Based Priority Scheme. Each packet has a number that indicates the packet's priority when packets sent on the bus are continuously relevant and may delay the delivery of a less urgent packet, which makes the network vulnerable to DOS attacks. Providing the example of a malicious node that streams frames with the smallest identifier to have the highest priority, preventing legitimate nodes from sending their valid frames. Besides, the CAN frame is not encrypted. Therefore, an attacker can rely on the recorded history of the CAN frames to scan the CAN frames. Among the major problems that the CAN network faces is that the attackers can access the network via interfaces such as the OBD port and CD drive, USB port, and telematics systems. Therefore, various attacks can be implemented, including DoS attacks, frame sniffing, and frame injection. As mentioned before, the CAN frame presents several intrinsic vulnerabilities, which may necessitate a switch to a new version of CAN protocol which is the CAN-FD.

- CAN FD offers three main advantages over the traditional CAN.
- It offers a higher data rate of up to 8 Mbit/s.
- It allows data payloads of up to 64 bytes (as opposed to 8 bytes).
- It allows the authentication mechanism.

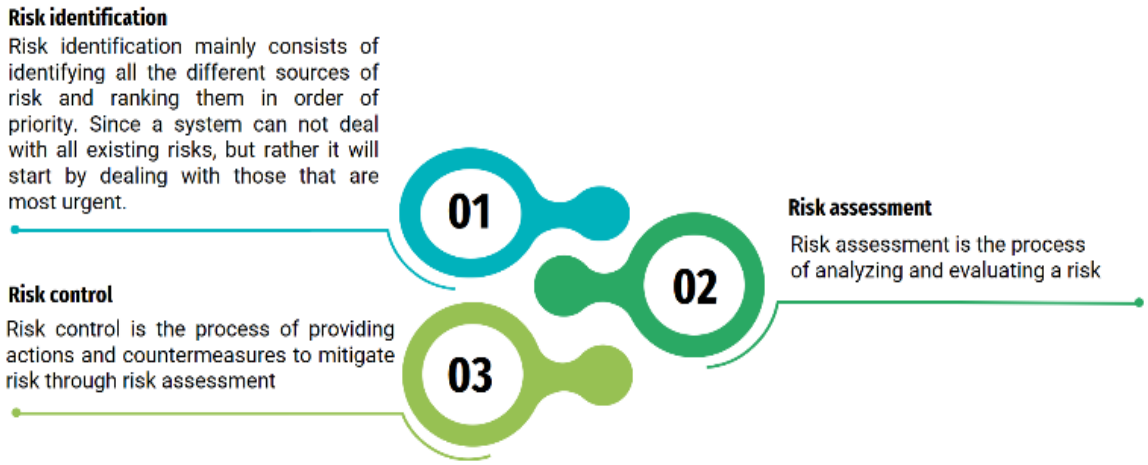


Fig. 1. Risk Management.

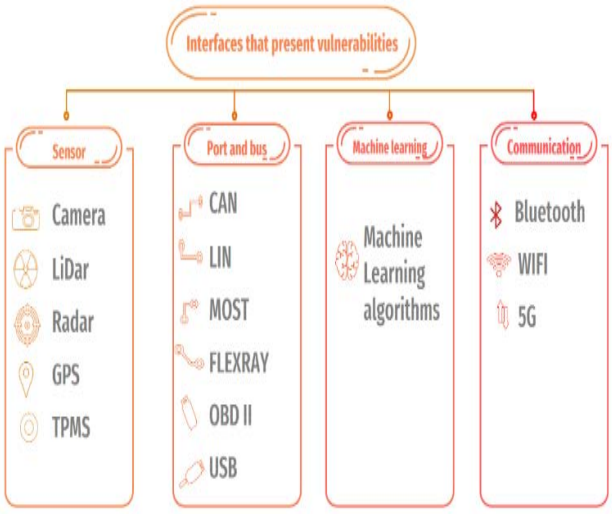


Fig. 2. Taxonomy of Attacks in Autonomous Vehicle.

*ii) OBD-II:* OBD-I was first introduced in 1987 to give a standardization of on-board diagnostics for vehicles, but the latter encountered many flaws and challenges, which led car manufacturers to migrate to a new version of OBD in 1996 called OBD II as well as all vehicles built after that date was equipped with an OBD II port. On-Board Diagnostics (OBD) is a vehicle self-diagnosis and reporting system that provides access to the status of various vehicle sub-systems, such as airbags, braking, speed control, and is used to monitor the condition of the vehicle's systems. OBD systems use a standardized digital communication port to transfer data in real-time. The OBD system uses the can bus to perform these data transfers. When the vehicle fails, the OBD system uses a standardized set of Diagnostic Trouble Codes (DTCs) to identify the malfunction and remedy the identified problem quickly. However, OBD II exposes the vehicle to several threats because today's vehicles are equipped with wireless communication tools (WIFI, Bluetooth 5G), so attackers can use these communication channels to send malicious programs to the CAN bus via the OBD port in order to control the vehicle. In addition, some scanners may also have a feature that allows them to extract and modify ECU codes. An attacker who uses this type of scanner can easily modify the ECU code for malicious purposes. An adversary can also use the OBD port to connect to the vehicle to listen to unencrypted packets and gather data for a replay attack [3], [4].

*iii) LIN:* The Local Interconnection Network (LIN) is a low-cost vehicle bus standard, the communication rate used by the LIN does not usually exceed 20kbps [5] therefore, it is only used for data that does not require high transmission rates such as control of lights, engines, air conditioning, steering wheels, seats and doors [5]. LIN is based on a master/slave architecture that consists of a single master node and many slave nodes connected using a single wire. While most research on embedded networks security is focused on CAN, the attacks on Local Area Network (LIN) is also as harmful as they can's attacks since a LIN master serves as a gateway to the CAN bus so the attacks can spread easily to other ECUs and other ECUs as well. The access to the LIN bus can be logical or physical. An attacker can access the LIN via the master node because the master node is always connected to the CAN bus [5]. Among the attacks that LIN buses are exposed we quote header collision, Spoofing, and response collision.

TABLE I. INTERFACES AND ATTACK ON AUTONOMOUS VEHICLE

| Interfaces | | Attack |
|---|---|---|
| Port et bus | CAN | • Replay attack [6], [32], [33].<br>• DOS [6], [33]–[35].<br>• Eavesdropping attack [6], [33].<br>• Injection attack [6], [33]. |
| | OBD II | • Code Modification[4]<br>• Code Injection: [4]<br>• Packet Sniffing [4]<br>• Packet Fuzzing[4] |
| | LIN | • Header collision [5], [6]<br>• Spoofing [6], [8].<br>• Response collision [5], [6] |
| | MOST | • Forged messages [9].<br>• Jamming attacks[8], [9], [36] .<br>• Synchronization disruption attacks[6], [8]. |
| | Flexray | • Replay attacks[6], [37].<br>• Spoof attack [7] .<br>• Injection attacks [6], [7], [37].<br>• The Masquerading [6], [37].<br>• Eavesdropping attack [6], [7], [37]. |
| | USB | • Injection attacks[6]<br>• Spoof attacks[6] |
| Short-range Communication | WIFI | • Eavesdropping attack [6], [16].<br>• Dos [6], [17].<br>• Jamming attack [6], [15]. |
| | Bluetooth | • Eavesdropping attack [11],<br>• Sniffing [11],<br>• Stealing personal information[11],<br>• Buffer overflow attack.[11] |
| | RFID | • Eavesdropping [6], [18].<br>• Brute force [6], [18].<br>• Replay [6], [18].<br>• Man-in-the middle [6], [18].<br>• Synchronization attacks [6], [19]. |
| Sensor | Camera | • Blind camera[4], [20], [21] |
| | Radar | • Jamming [23], [38], [39].<br>• Ghost vehicular attack [22]–[24]. |
| | LiDar | • Jamming [4], [20], [21].<br>• Spoofing [4], [20], [21]. |
| | GPS | • Spoofing [4], [20], [22].<br>• Jamming [4], [20], [22]. |
| | TPMS | • TPMS based attack [4], [20], [21], [27]. |
| Machine learning | | • Adversarial attacks [29], [30]<br>• Black box attack [28]. |

In a spoofing attack, the master in a LIN network can force a slave to perform tasks including sleep and SYNC field definition. An attacker can exploit these two characteristics of the master to force slaves to fall asleep and cause the network to shut down. In addition, it can spoof messages and modify the SYNC field to distort the synchronization [6]. While The collision attack consists of sending a wrong message simultaneously as a correct message is sent. In the LIN protocol, an attacker exploits the LIN error handling mechanism, which consists of stopping transmission of a slave node when he detects that the value in the bus differs [6]. The Header collision attacks happen when an attacker sends a false header to crash against a legitimate header from the master node. When a response is sent from the new editor node, the attackers can carry out a response collision attack to insert their illegal message. In this way, attackers can distort the sequence of responses sent on the LIN bus and leave the vehicles' automated sliding doors open and lock the steering wheels while the vehicles are on the road[6].

*iv) Flexray:* Flexray was developed in 2007 by BMW. Flexray is an expensive and complex communication tool. It is used for critical data that requires more security; this is due to the time-division multiplexing of FlexRay, which facilitates the design of modular, distributed, and security-related systems. Flexray is known for its transmission speed which can reach 10Mbps for each channel, and FlexRay offers scalable fault tolerance by allowing one or two-channel communication. Nevertheless, one channel can also be connected when redundancy is not required. However, The bandwidth can be increased by using both channels to transfer non-redundant data. The absence of the confidentiality mechanism in the FlexRay protocol allows an attacker to read all data sent over the bus. In addition, FlexRay does not have an authentication mechanism so an attacker can create and inject data, e.g., an attacker can create and inject a request to switch on the stoplight [7]. Flexray protocol is also vulnerable to attacks that can target the static segment of the FlexRay communication, such as replay attacks, injection attacks, and the Masquerading [6].

*v) MOST:* MOST (Media Oriented System Transport) is a serial communication system used for audio, video, and control data transmission via fiber optic cables, and it is also used for GPS. MOST (Media Oriented System Transport) is a serial communication system used for audio, video, and control data transmission via fiber optic cables, and it is also used for GPS. This high-performance technology is based on synchronous data communication with a high data rate of up to 150 Mbps and the fact that MOST is not sensitive to electromagnetic interferences since it uses plastic optical fibers instead of traditional copper wire. MOST communication is susceptible to synchronization-disrupting attacks and jamming or denial-of-service attacks [8], [9]. An attacker can perform a jamming attack by prompting a malicious node to continuously send fake messages that continuously block legitimate messages. In addition, an attacker can cause a synchronization interruption by sending fake synchronization frames to disrupt the MOST synchronization [6], [8].

*vi) USB:* Nowadays, all vehicles have a USB port to connect phones, navigation systems, or any USB devices. However, this port exposes the vehicle to different threats since attackers can access the CAN buses via a USB port and inject malicious code or spoof network cards [6].

*b) Short-range communication*

*i) Bluetooth:* Bluetooth is a very well-known communication protocol and is widely used in today's vehicles. Once the phone is connected via Bluetooth to the vehicle, it allows fully wireless access calling functions from the phone via the vehicle's dashboard, control screen, steering wheel buttons, or voice commands, which is very convenient because the driver can keep both hands on the steering wheel. However, this protocol exposes the vehicle to several threats because of the vulnerabilities it faces. The lack of an authentication mechanism before pairing the devices makes it easier for hackers to access the vehicle. Therefore, an attacker can inject viruses or malicious programs to exploit important information (e.g., address book passwords) once the Bluetooth device is paired. In addition, the Bluetooth interface enhances the routes of the cyber-attack as follows: Eavesdropping attack, Sniffing, stealing personal information, Buffer overflow attack [10]–[12].

*ii) WIFI:* WIFI is a wireless network used to connect multiple devices. The term WIFI is an abbreviation of Wireless Fidelity. The IEEE 802.11 standards govern it. WIFI is similar to Bluetooth in the vehicle except that WIFI has lower latency and higher bandwidth and, of course, a high cost [13]. WIFI remains less used in the vehicle than Bluetooth due to the cost and interference with Bluetooth since the two technologies share an overlapping spectrum[14]. WIFI usage in the vehicle exposes the vehicle to serious threats, namely jamming attacks [15]. In addition, an attacker can also get access to an illegitimate WiFi access point and listen to the vehicle's activity [16]. WiFi protected access can also be threatened by a denial of service attack [17].

*iii) RFID:* RFID is a radio frequency-based technology to identify tagged objects that pass close to a detector. Thus, contrary to the barcode, we can follow the path of objects and store and retrieve their data. Nowadays, RFID technology is widely applied in several sectors (aeronautics, transport, food industry, health ...), and we can also find this technology in our daily lives, namely transport cards, anti-theft tags, contactless keys, highway badges. However, RFID technology is vulnerable to several threats, namely eavesdropping, brute force, replay, and man-in-the-middle attacks [18] and Synchronization attacks [19] that block the synchronization system.

*c) Sensor*

*i) Camera:* The camera is a very important sensor because it allows the vehicle to understand its surroundings. In order to maintain a 360-degree view of its surroundings, the

vehicle must be equipped with at least eight cameras installed at several angles. In addition, the camera allows the detection of obstacles and object recognition, but unfortunately, a fast laser burst of 650 nm is capable of completely blinding the camera without ever getting recovered from blindness [4], [20], [21].

*ii) Radar:* Radar is a system that allows the detection of objects. However, this system is also vulnerable to attacks such as jamming attack and ghost vehicular attack which aims to convert and store the signal using a DRFM (digital radio frequency memory) and use it to deceive the transmitting radar in order not to recognize it from other legal signals and considered as an obstacle [22]–[24].

*iii) Lidar:* Lidar, is an abbreviation of Light Detection and Ranging, is a method of remote sensing which uses light in the shape of a laser pulse to measure distances (varying distances) to the object. This system is used in autonomous vehicles to detect obstacles. However, liDar is also exposed to attacks such as jamming and spoofing [4], [20], [21]. For example, an attacker deceives the lidar by pretending the existence of an obstacle and forcing the vehicle to stop [25], [26].

*iv) GPS:* The GPS is a Satellite Geolocation System. It can determine the geographic coordinates of any point on the surface of the globe. The attacker can block a vehicle to receive the GPS signal by performing a jamming attack. In addition, GPS can be easily hacked by an attacker using a radio transmitter that broadcasts a false GPS signal and interferes with nearby GPS receivers in order to perform a spoofing attack and deceive the GPS device by forcing the driver to deem that the vehicle is in an area when it is not [4], [20], [22].

*v) TPMS:* Indirect TPMS is used to calculate the rotation speed of each wheel. If a wheel rotates faster, it means that its pressure is not correct. The TPMS must send this data to the vehicle control unit (ECU). An attacker can exploit this data and execute a TPMS based attack and modify this data and send erroneous data to the ECU [4], [20], [21], [27].

*d) Machine Learning*

in adverse attacks, the attack strategy may differ from one attacker to another. This strategy is based on the attacker's capability, the purpose of the attack, and the expertise of the attacker. The concept of a contradictory attack consists of adding noise to the model's input to lead them to produce an erroneous prediction. The author in [28] successfully disrupted a deep neural network model by forcing it to predict wrong classes without prior knowledge of the model or the data used in the learning phase. This type of attack is called a black box attack. Szegedy et al. [29] carried out contradictory example attacks against MNIST, QuocNet [30], AlexNet [31]. They performed perturbations on inputs so that the correct and modified inputs cannot be distinguished from each other. This perturbation led to misleading the model.

*2) Risk assessment:* In this step, we are interested in measuring risk. We define risk as a relation between two variables: the probability of attack success and the attack's impact on the system. In this section, we will conduct a study to calculate the probability of attack success based on a decision tree then we will conclude the value of the risk.

$$Risk = Probability \times Impact \quad (1)$$

*a) Impact of attacks*

In the intelligent transport system, we will divide the impact of attacks on the system into four distinct levels levels shown in Fig. 3. The first level is the most important one, the impact on human life when the attacker aims to cause accidents or to hit pedestrians; this attack has to be considered because human life counts the most. The second level involves material damage to the VANET network, which is also dangerous because if an attacker manages to break down a base station, this can cause traffic jams and even accidents. The third level includes material and ecological damage when an attacker crashes into a tree, for example. Finally, the last level is moral damage; we refer to the attack intended to capture the driver's information or hack into the network information. It is important to mention that we may have a mixture of these levels of damage; in fact, we may have both material and physical damage or physical and moral damage, depending on the case.

*b) Probability of attack success*

The attacker is an essential element in calculating the probability of success of the attack. We will focus on two criteria of the attacker, which are the attacker's capability and his knowledge. These two criteria are very important in the calculation of the probability of success of the attack. For example, suppose an attacker has very high expertise and capability besides having a very high knowledge of the system. He can easily carry out an attack that can be very dangerous, and the probability of the attack being successful will be very high.


Fig. 3. Impact Levels.

On the contrary, if the attacker's capacity is very low and knowledge of the system is also low, then the probability of a successful attack will be very low as he/she does not have the expertise to perform a successful attack. If the attacker has high knowledge but very low capability, the attacker can carry out an attack that is very easy to perform but cannot carry out a very complex and dangerous attack. Therefore, we can conclude that the type of attack is another essential criterion in calculating the probability of success. In order to calculate the probability of success, we will focus on the complexity of the attack because a very complex attack need a that the attacker has a very high knowledge of the system and also very high capacity and expertise on the contrary of an easy attack that does not need attacker to be expert. So to measure the complexity of the attack, we will focus on four criteria.

- The attacks' adaptability is the type of attack that even if the system detects them, they can adapt and find another flaw and access to the system. Therefore, those types of attack require a very high capability of attack and very high knowledge of the system because they are very complex, and the probability of attack success is very high if the attacker has the essential element needed.
- Imperceptibility of the attacks: The degree of imperceptibility has a significant impact in determining the complexity of the attack. Because the system becomes imperceptible to differentiate between malicious nodes and legitimate ones, intrusion detection will be very hard. In this case, the attacker can carry out attacks that will cause accidents or send erroneous messages that will be considered the right messages since the system considers him a legitimate node. He can also carry out any attack, namely, DNS.
- The specificity of the attacks: when the attack has a specific target, and the attack aims to put down a specific functionality of the vehicle or even to change the value of the targeted function. For example, changing the value of the TMPS sensor and providing the wrong value of the wheel pressure.
- Type of attacks: The type of attack means if the attack needs physical access or remote access. The attack with physical access is very damaging since they can access the vehicle ECU and control the vehicle. The physical access means that the attacker can access the car via a port such as OBDII or USB, see Section IIA(1). The attacker can also access the vehicle via remote by using wireless communication. In this case, an attacker can carry out attacks such as jamming or spoofing.
- The probability of attack success is a relation between the complexity of attacks that contain four criteria and the attacker containing two criteria.

$$Probability\ of\ attack\ success = R(complexity, capacity, knowledge) \quad (2)$$

A successful attack has a probability of 1, and a non-successful attack has a probability of 0. In our case, we define the probability of success into six classes, as shown in Fig. 4. An attack that is sure to happen has a probability of success between 90 and 100%, and those attacks are very complex to detect by the system and the capability and knowledge of the attacker are very high the attacker can perform easily an attack that could be specific and target an ECU. As a result, he can control the vehicle and cause dangerous damage. Another type of attack that also presents a very high risk for the system is the attack with a percentage of success between 89% and 70%. In this type of attack, the attacker has a high capability and medium knowledge, and the attacker can perform an attack with a medium level of complexity. The third class is the class that remains dangerous but less than the fourth class. The percentage of probability of success is between 69- 50%. In this type o attack, the capability of the attacker and the knowledge are medium, and the attacker can perform attacks that have a level of complexity low or medium. The second class contains the attacks that might succeed or not; the probability of attack success is between 49% and 30%. In this class, the attacker's capability is low, and the attacker's knowledge is very low, so the attackers cannot perform complex attacks but rather can perform an easy attack such as eavesdropping. The second class contains attacks with a low probability of success between 29% and 10%. The attacker in this class has a very low capability; he cannot perform a complex attack, and he will find difficulty conducting an easy attack. The last class is the attack with a very low probability of success between 9% and 0%. In this class, the attacker's capability is extremely low, and the attacker's knowledge they cannot perform any attack.

*c) Decision tree*

As described in the previous section, we define six classes of probability, and because the probability of attack success is a relation between three-component, we will not be able to calculate it using a mathematical function. Rather, we will use a machine learning algorithm to predict the probability based on the attack's complexity, capacity, and knowledge. Finally, the decision tree will build a tree that will use our logic described in (Section IIA(2)) to find the probability class.

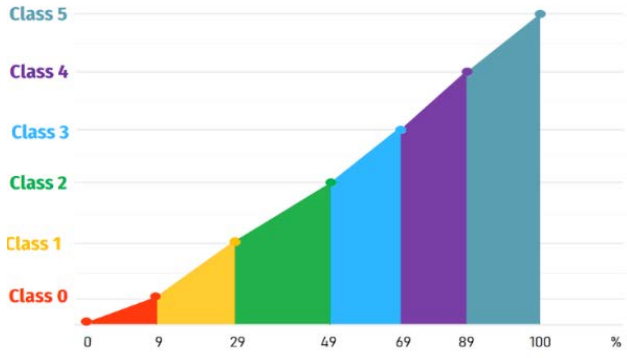


Fig. 4. Probability of Success.

The decision tree algorithm is a supervised algorithm that can be applied to regression and classification tasks [40], [41]. The decision tree is composed of three essential elements, which are:

- The root node: this is the node that represents the top of the tree.
- Intermediate nodes: these are the nodes that are placed between the root and the end nodes.
- Leave nodes: these are the final nodes of the tree, where predictions of a category or numerical value are made.

Decision trees use several algorithms to decide to split a node into two or more sub-nodes. The creation of sub-nodes increases the homogeneity of the resulting sub-nodes. Several decision tree algorithms are used to split the node. In our case study, we will use C4.5, a decision tree algorithm that supports several classes higher than two in its decision node calculation. In order to determine the placement of nodes in the trees, we will use the entropy and information gain principle [40], [41].

The entropy is the order of a data set, and we compute the entropy at each node of the tree then subtract the child's entropy from the parents' entropy. The outcome of this calculation is the information gain [40].

$$E(S) = \sum_{i=1}^{c} p_i \log_2 p_i \quad (3)$$

We choose the decision tree because it is easy to work with and also to interpret. The decision tree(DT) provides a graphical tree that will help understand the result. Besides, DT is tolerant of missing value and simple to implement. In our case study, the decision tree is the wright algorithm since, in each step, the algorithm must ask some questions (for instance, if the attacker has a high capability or not ), and based on the result of the question, a decision will be made to find the other feature that may give the right class of probability. The decision tree may present a problem of overfitting, which will be corrected using a post pruning technique. Pruning is a technique used for machine learning algorithms that reduces the size of the trees by deleting segments of the tree. The result is a significant reduction in the complexity of the final classifier and consequently enhanced predictive accuracy by reducing overfitting. Tree pruning can be done in two ways: pre-pruning or post-pruning. In our experiments, we will use post-pruning based on reduced error pruning. The algorithm is very simple and fast. It produces small, compact trees. It will sequentially transform each subtree into one single leaf. It assesses the pattern against a set of test data and then compares the error rate with the original tree. The sub-tree having the highest error reduction would be pruned. This process would be repeated until there is no more error reduction.

## III. Experiment Result

### A. Probability of Attack Success

Before starting the creation of the decision tree, we first prepare the database that will be the input of the machine learning algorithm. Machine learning algorithms are highly data-dependent. Therefore, data preparation is a very important step as it speeds up the learning of the algorithms and gives a correct result. Therefore, the first step in creating the decision tree was the data cleaning or removing any missing data, and then we transform the data using hot encoding as the algorithm does not support categorical data.

TABLE II. Accuracy Value

| | Before pruning | After pruning |
|---|---|---|
| Training accuracy | 90% | 90% |
| Testing accuracy | 75% | 87% |

The database we use in our algorithm is created randomly by giving each criterion, namely attacker capability, attacker knowledge, attack adaptability, attack specificity, attack type, and attack imperceptibility, one of the following values (very low, low, medium, high, or very high). After creating the database and preparing it, we split the data into test and training sets. Then we will create the decision tree and calculate the accuracy of the tests and training to identify whether there is an over-fitting. We start first by creating the decision tree and measuring the accuracy for the training and the test. As mentioned in Table II, the accuracy of the training is 90%, and the test accuracy is 75%, which means that there is an over-fitting. To resolve the overfitting problem, we recreate the decision tree. We use a post pruning technique described in (Section IIA(2)) to correct the overfitting, so as mentioned in Table II, after the post pruning, the accuracy of the training is 90%. The accuracy for the test is 87%, the overfitting is corrected, and the accuracy of the tests was increased by 12%, and the gap between training and testing was reduced to 3%, we can conclude that the algorithm learns well.

The decision tree is constructed through iteration from the root node to the leaves node using the training set. First, the data set is split into two sets: the training set, which the decision tree is using to learn, and the test set, which is used to evaluate predictions to the real values and measure the performance of the decision tree. Next, the tree is built by calculating entropy and the information gain. The node with the highest information gain is eventually placed as the root node in the decision tree. Then we will repeat this process when the subset is split.

Moreover, each time, we will recalculate the remaining values that are in that subset. If two nodes are compared together, and they have the same information again. Then a concept called the gain ratio will determine which of these will be used. The gain ratio is calculated based on the node that has the fewest unique values. This node will become preferred. It can be seen that this tree includes a total of 58 nodes, among which 30 are leaves nodes, including one leave node in class 0, 3 leaves nodes in class 3, five leaves nodes in class 2, 14 leaves node in class 3, 5 leaves nodes in class 4 and 2 leaves nodes in class 5 as shown in Fig. 5. Note that entropy is also calculated and given in each node to characterize the purity of the sub dataset in that node. For every node, there is information about the split/decision. For the top of the tree root node, the tree starts by assessing whether the attacker has

a high capability or low capability. The entropy criterion at this point is 2.347. An entropy of 0 represents purity. Therefore the value of the entropy criterion must be lower as we move down the branches. The number of samples at this node is 131.

The class prediction at this point is 3. This prediction will become significantly more accurate as we go down the tree. We will assess the first True of the decision tree, which means that the capability is very low, so the decision node will assess whether the attacker has knowledge about the system. At this node, The entropy criterion is equal to 1.226 as discussed earlier, the entropy criterion is decreasing, and the class prediction here is class 1. For the second true, we get to a leave node with an entropy equal to 0 and a prediction class equal to zero, which means that an attacker with a very low attack's capability and also a very low attacker's knowledge the attack probability will belong to class 0, which means that the attacker could not perform an attack on the system. If we evaluate the second false in the decision tree, the decision node here evaluates the specificity of the attack. The entropy is equal to 0, 455, and the prediction class equals one if the attack is specific. The decision tree arrives at a leave node with an entropy equal to 0 and a prediction class equal to 1. we can explain that by following the decision logic if the attacker's capability was very low. He has a high knowledge. Then the decision tree evaluates whether the attack is complex by first evaluating whether the attack is specific. If the attack is specific, then the probability of attack success will be class 1 because an attacker with high knowledge and very low capability could not perform a complex attack. If the attack was not specific, then the decision tree will look for the other criterion: adaptability and imperceptibility.

## B. Risk Assessment

To measure the risk, we first started by identifying risk interfaces in the autonomous vehicles, then we calculated the probability of attack success and evaluated the impact and severity of the attack; then, we can conclude the value of the risk. As mentioned in section (b), the risk is a relation between the attack's impact and the probability of success of the attack. There is a set of rules that can be executed to measure the risk. If the probability of attack success is (very high or high) means that the probability belongs to class five or the fourth class and the attack's impact is physical then, the risk will be very high, and we should stop the attack as soon as possible. Besides, if the impact is material, then the risk will be high. While if the impact is not so dangerous, which means that the impact is moral and the attacker is trying to steal information from the network, then the risk is medium, and we should consider this attack, but it is not urgent compared to the first one. If the probability of success is medium, that means that the probability of attacks belong to the third or the second class and the impact is physical or materiel or both then the risk will be medium because the attack may happen or not the priority of those attack is less than the first one but should be taken into consideration. While if the impact is moral, then the risk will be low because there are no damages, and we should increase the mechanism of confidentiality and authenticity to stop the attacker from listening to the network. If the probability of attacks belongs to class zero, then the risk will be low. We will use a decision tree that will predict the class of the risk. We could present these rules in a decision tree that will predict the value of the risk based on the value of the probability of attack success and the impact of the attack.

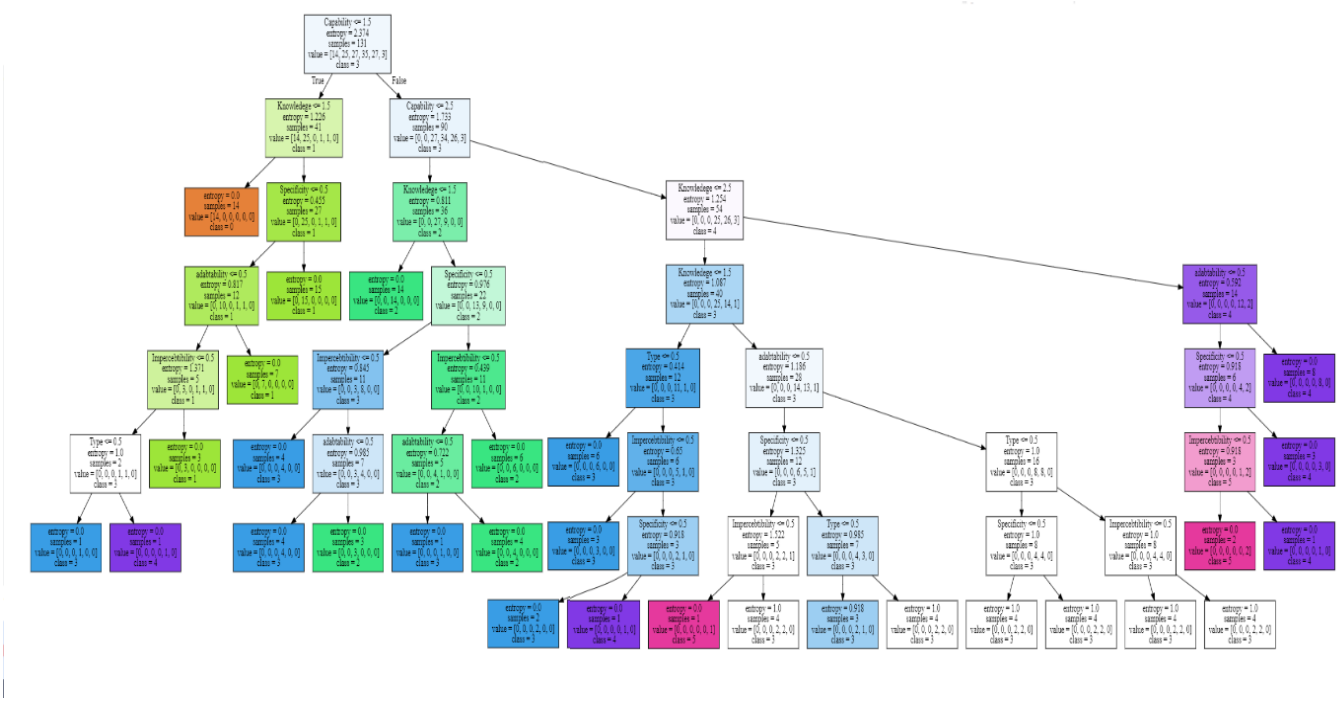

Fig. 5. Decision Tree of the Probability of Attack Success.

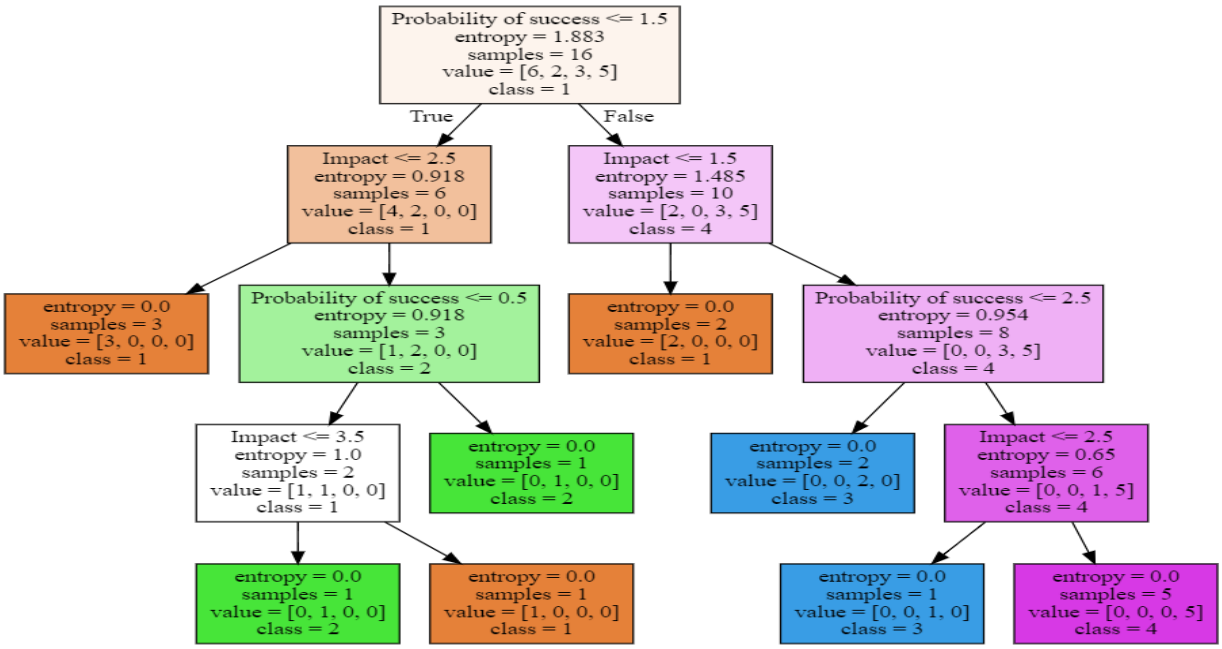


Fig. 6. Decision Tree of Risk Assessment.

It can be seen that in Fig. 6, the tree includes a total of 15 nodes, among which 6 are leaves nodes, including three leave nodes in class 1, 2 leave nodes in class 2, two leaves nodes in class three, and two leave nodes in class four. Note that entropy is also calculated and given in each node to characterize the purity of the sub dataset in that node. The accuracy of the decision tree is 100%, and the max depth of the tree is 4. The tree's leave has an entropy of zero, which means that all leaves are pure, and the tree follows the logic described in the previous paragraph. The tree started with the probability of attack success as a root of the tree because it has the highest entropy, and the entropy criterion decrease while going down the tree.

## IV. Conclusion

It is very important to list risks associated with autonomous vehicles to develop defensive mechanisms to enhance security in smart transportation.

The study and the evaluation of risk constitute an essential step in decision-making to opt for a mitigation technique more tailored to the transportation context.

The approach that we have explained in this paper suggests a new technique to evaluate the risks that may be enfolded in an autonomous vehicle based on two criteria: the attack success rate and its impact on the targeted system. To measure attack success probability, we have studied two main variables: the attacker's capabilities and the type of attack they perform. We have used a decision tree algorithm to forecast the risks class. We have derived a graphical tree that we have presented in this paper to help in understanding the proposed results. We will conduct a study on other machine learning classifiers in future work, and we will compare their performance in risk evaluation with the obtained results.

## References

[1] H. Fang and M. Duan, 'Safety System Engineering for Offshore Oil', in Offshore Operation Facilities, Elsevier, 2014, pp. e183–e347.

[2] O. Avatefipour and H. Malik, 'State-of-the-Art Survey on In-Vehicle Network Communication (CAN-Bus) Security and Vulnerabilities', ArXiv180201725 Cs, Feb. 2018, Accessed: Apr. 15, 2021. [Online]. Available: http://arxiv.org/abs/1802.01725.

[3] A. D. Kumar and K. N. R. Chebrolu, 'A Brief Survey on Autonomous Vehicle Possible Attacks,Exploits and Vulnerabilities', p. 6.

[4] V. L. L. Thing and J. Wu, 'Autonomous Vehicle Security: A Taxonomy of Attacks and Defences', in 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, Dec. 2016, pp. 164–170, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52.

[5] J. Takahashi et al., 'Automotive Attacks and Countermeasures on LIN-Bus', J. Inf. Process., vol. 25, no. 0, pp. 220–228, 2017, doi: 10.2197/ipsjjip.25.220.

[6] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, 'Cybersecurity challenges in vehicular communications', Veh. Commun., vol. 23, p. 100214, Jun. 2020, doi: 10.1016/j.vehcom.2019.100214.

[7] D. K. Nilsson, U. E. Larson, F. Picasso, and E. Jonsson, 'A First Simulation of Attacks in the Automotive Network Communications Protocol FlexRay', in Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS'08, vol. 53, E. Corchado, R. Zunino, P. Gastaldo, and Á. Herrero, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 84–91.

[8] M. A. Chowdhury, A. Apon, and K. Dey, Eds., Data analytics for intelligent transportation systems. Amsterdam: Elsevier, 2017.

[9] M. Wolf, A. Weimerskirch, and C. Paar, 'Secure In-Vehicle Communication', in Embedded Security in Cars, K. Lemke, C. Paar, and M. Wolf, Eds. Berlin/Heidelberg: Springer-Verlag, 2006, pp. 95–109.

[10] A. Yadav, G. Bose, R. Bhange, K. Kapoor, N. Ch. S. N. Iyengar, and R. D. Caytiles, 'Security, Vulnerability and Protection of Vehicular On-board Diagnostics', Int. J. Secur. Its Appl., vol. 10, no. 4, pp. 405–422, Apr. 2016, doi: 10.14257/ijsia.2016.10.4.36.

[11] H. Onishi, K. Wu, K. Yoshida, and T. Kato, ‘Approaches for Vehicle Cyber-Security in the US’, Int. J. Automot. Eng., vol. 8, no. 1, pp. 1–6, 2017, doi: 10.20485/jsaeijae.8.1_1.

[12] S. Checkoway et al., ‘Comprehensive Experimental Analyses of Automotive Attack Surfaces’, p. 17.

[13] R. Friedman, A. Kogan, and Y. Krivolapov, ‘On Power and Throughput Tradeoffs of WiFi and Bluetooth in Smartphones’, IEEE Trans. Mob. Comput., vol. 12, no. 7, pp. 1363–1376, Jul. 2013, doi: 10.1109/TMC.2012.117.

[14] A. Mourad, S. Muhammad, M. O. Al Kalaa, H. H. Refai, and P. A. Hoeher, ‘On the performance of WLAN and Bluetooth for in-car infotainment systems’, Veh. Commun., vol. 10, pp. 1–12, Oct. 2017, doi: 10.1016/j.vehcom.2017.08.001.

[15] T. D. Vo-Huu, T. D. Vo-Huu, and G. Noubir, 'Interleaving Jamming in WiFi Networks', in Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, Darmstadt Germany, Jul. 2016, pp. 31–42, doi: 10.1145/2939918.2939935.

[16] O. Nakhila, E. Dondyk, M. F. Amjad, and C. Zou, 'User-side WiFi Evil Twin Attack detection using SSL/TCP protocols', in 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, Jan. 2015, pp. 239–244, doi: 10.1109/CCNC.2015.7157983.

[17] M. Vanhoef and F. Piessens, 'Denial of Service Attacks Against the 4-Way WiFi Handshake', in Computer Science & Information Technology (CS & IT), Nov. 2017, pp. 85–94, doi: 10.5121/csit.2017.71508.

[18] J.-S. Cho, Y.-S. Jeong, and S. O. Park, ‘Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol’, Comput. Math. Appl., vol. 69, no. 1, pp. 58–65, Jan. 2015, doi: 10.1016/j.camwa.2012.02.025.

[19] C. Zhang, W. Zhang, and H. Mu, ‘A Mutual Authentication Security RFID Protocol Based on Time Stamp’, in 2015 First International Conference on Computational Intelligence Theory, Systems and Applications (CCITSA), Ilan, Taiwan, Dec. 2015, pp. 166–170, doi: 10.1109/CCITSA.2015.52.

[20] S. Parkinson, P. Ward, K. Wilson, and J. Miller, ‘Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges’, IEEE Trans. Intell. Transp. Syst., vol. 18, no. 11, pp. 2898–2915, Nov. 2017, doi: 10.1109/TITS.2017.2665968.

[21] J. Petit and S. E. Shladover, ‘Potential Cyberattacks on Automated Vehicles’, IEEE Trans. Intell. Transp. Syst., pp. 1–11, 2014, doi: 10.1109/TITS.2014.2342271.

[22] C. Yan, ‘Can You Trust Autonomous Vehicles : Contactless Attacks against Sensors of Self-driving Vehicle’, 2016.

[23] M. Pham and K. Xiong, ‘A Survey on Security Attacks and Defense Techniques for Connected and Autonomous Vehicles’, ArXiv200708041 Cs, Jul. 2020, Accessed: Apr. 15, 2021. [Online]. Available: http://arxiv.org/abs/2007.08041.

[24] S. J. Roome, ‘Digital radio frequency memory’, Electron. Commun. Eng. J., vol. 2, no. 4, p. 147, 1990, doi: 10.1049/ecej:19900035.

[25] B. G. B. Stottelaar, Practical cyber-attacks on autonomous vehicles. 2015.

[26] M. Harris, ‘Researcher Hacks Self-driving Car Sensors’, 2015.

[27] I. Rouf et al., ‘Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study’, p. 17.

[28] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami, ‘Practical Black-Box Attacks against Machine Learning’, ArXiv160202697 Cs, Mar. 2017, Accessed: Apr. 15, 2021. [Online]. Available: http://arxiv.org/abs/1602.02697.

[29] C. Szegedy et al., ‘Intriguing properties of neural networks’, ArXiv13126199 Cs, Feb. 2014, Accessed: Apr. 16, 2021. [Online]. Available: http://arxiv.org/abs/1312.6199.

[30] Q. V. Le et al., ‘Building high-level features using large scale unsupervised learning’, ArXiv11126209 Cs, Jul. 2012, Accessed: Apr. 15, 2021. [Online]. Available: http://arxiv.org/abs/1112.6209.

[31] A. Krizhevsky, I. Sutskever, and G. E. Hinton, ‘ImageNet classification with deep convolutional neural networks, Commun. ACM, vol. 60, no. 6, pp. 84–90, May 2017, doi: 10.1145/3065386.

[32] T. Hoppe and J. Dittman, ‘Sniffing/replay attacks on can buses: A simulated attack on the electric window lift classified using an adapted cert taxonomy’, Workshop Embed. Syst. Secure., pp. 66–72, 2007.

[33] J. Liu, S. Zhang, W. Sun, and Y. Shi, 'In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions, IEEE Netw., vol. 31, no. 5, pp. 50–58, 2017, doi: 10.1109/MNET.2017.1600257.

[34] P. Carsten, T. R. Andel, M. Yampolskiy, and J. T. McDonald, ‘In-Vehicle Networks: Attacks, Vulnerabilities, and Proposed Solutions’, in Proceedings of the 10th Annual Cyber and Information Security Research Conference, Oak Ridge TN USA, Apr. 2015, pp. 1–8, doi: 10.1145/2746266.2746267.

[35] K. Koscher et al., ‘Experimental Security Analysis of a Modern Automobile’, in 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2010, pp. 447–462, doi: 10.1109/SP.2010.34.

[36] N. Kalid, A. A. Zaidan, B. B. Zaidan, O. H. Salman, M. Hashim, and H. Muzammil, 'Based Real-Time Remote Health Monitoring Systems: A Review on Patients Prioritization and Related "Big Data" Using Body Sensors information and Communication Technology', J. Med. Syst., vol. 42, no. 2, p. 30, Feb. 2018, doi: 10.1007/s10916-017-0883-4.

[37] R. Zhao, G. H. Qin, H. P. Chen, J. Qin, and J. Yan, ‘Security-Aware Scheduling for FlexRay-Based Real-Time Automotive Systems’, Math. Probl. Eng., vol. 2019, p. 4130756, Jun. 2019, doi: 10.1155/2019/4130756.

[38] R. M. Whitson and M. J. Lewis, ‘(75) Inventors: Walter E. Buehler, Issaquah, WA (US)’;, p. 16.

[39] R. N. Lothes, M. B. Szymanski, and R. G. Wiley, Radar vulnerability to jamming. Boston: Artech House, 1990.

[40] S. Singh and P. Gupta, ‘Comparative Study ID3, Cart and C4.5 Decision Tree Algorithm: A Survey’, Int. J. Adv. Inf. Sci. Technol., p. 7, 2014.

[41] A. Priyam, R. Gupta, A. Rathee, and S. Srivastava, ‘Comparative Analysis of Decision Tree Classification Algorithms’, Int. J. Curr. Eng. Technol., p. 4, 2013.