AI-Based Solutions for Enhancing Vehicle Security

By Dr. Olga Petrova

Professor of Applied Mathematics, National Research University Higher School of Economics (HSE), Russia

1. Introduction

Rapid advances in wireless communication, embedded systems, telecommunications, Internet of Things (IoT), and sensor technologies have resulted in a significant impact on our lives. These technologies have made our lives more convenient. New developments are occurring in the transportation world, particularly in the automotive sector. Advanced driver assistance systems have driven automobiles to evolve, as well as the next generation of autonomous cars. Unfortunately, with each advanced vehicle technology, criminal activity grows more frequent. Vehicle crime remains a significant issue confronting vehicle users, owners, insurers, and manufacturers. Vehicle crime includes offenses related to the theft of or from vehicles or vehicle components, such as daylight and nighttime burglary, car-hire offenses, car conversion, car theft, and car robbery, as well as vehicle component theft. There were car robberies and thefts of other cars or motorcycles in 2017/2018 in England and Wales alone. Indeed, during that same period, around cars and other automobiles were stolen worldwide. These observations have piqued the attention of vehicle users as well as the automotive industry, which is exploring new ways to boost vehicle security without raising costs and weight.

Given this background, this study is intended to identify the various approaches described in the literature that employ artificial intelligence (AI) to provide solutions for enhancing vehicle security. It will provide the most recent information pertaining to potential vehicle security concerns, existing challenges regarding vehicle security, and future research directions. The study is designed to achieve the following research objectives: • To discuss vehicle security in terms of its two types (i.e., passive vehicle security and active vehicle security). • To highlight potential vehicle security threats and their identification on a theoretical basis. • To outline areas of vehicle security that require further attention. • To provide a foundation from

which vehicle owners, vehicle users, insurance companies, and vehicle manufacturers can realize innovative methods for enhancing vehicle security.

1.1. Background and Significance

Vehicle security has become a significant challenge in the last century as there are innovative explorations in the automotive industry. Manual operation mechanisms and keys were employed in the early stages of the automotive industry to ensure security. In advanced stages, centralized and electrical locks were introduced, and in modern vehicles, the entire ignition process can be conducted wirelessly. New security measures are brought forth to minimize the aforementioned issues. Furthermore, the existing keyless entry systems have vulnerabilities that make it possible to perform multiple attacks such as relay and key fob re-functioning. However, this is a significant aspect as it underscores the importance of vehicle security. As a result, the effectiveness of security systems is retrievable from historical perspectives.

The evolution of vehicle theft has mirrored the prosperity of technology used to reduce automotive threats. In the past, thieves started vehicles by breaking the steering wheel lock and manually jump-starting the vehicle, a technique that progressed to hot-wiring as progress occurred in ignition locks. Such acts of vehicle theft are hardly seen today thanks to technology like remote-controlled alarms which are predominantly used today. With the possible uptakes of technology, such as optical systems, new risks in the black market are emerging. In addition, two Tesla bikes were stolen in Iceland by hacking into the vehicle's network and leveraging known vulnerabilities in a specific voltage-charging system. Such information emphasizes the necessity of introducing new security technology. Currently, there are over one billion vehicles around the globe, and 50 to 100 of these vehicles get stolen regularly. There were 767 incidents of vehicle hacking in 2018. The attackers can gain full control of the vehicle and steal it. Such events may lead to significant damage and loss in terms of vehicles and lives. This shows why vehicle security is important. Therefore, such threats require vehicle owners to be increasingly concerned about their security. Given the vulnerability of the early 21st-century automotive security systems, it is imperative that improved methods of mechanical and electronic security be introduced as quickly as feasible. With the current and future state of technology increasing the ability of cyber risks in vehicles,

it is essential to employ new methods of anti-theft systems. The development of AI and its wide range of applications is changing the world in a multitude of ways. The implementation of AI in vehicle security can equip it to handle the enhanced nature of e-threats. AI-based technology is a larger field for suitable car security systems, and it is pivotal that a comprehensive survey of this technology be conducted to assess such suitability for future research.

1.2. Research Objectives

The primary goals of the study for the research in the vehicle security area are to identify the AI-based solution that will be effective in surveilling the environment, the driver, and the car itself to enhance the overall security measures intended to be proposed in this study. A detailed research on the application of state-of-the-art techniques in the area of machine learning, decision trees, and deep learning will be articulated for the enhancement of the security surveillance system. 1. To analyze the different state-of-the-art technologies and recommend existing technology improvements for the development of the most efficient tools or methods for vehicle security, proposing the recommendation as an identification method and artificial intelligence (AI) solution that helps to enhance the vehicle features and functions, which include driver surveillance inside and outside, and enhancing and identifying the vehicle obstacles. 2. To investigate the innovative techniques and tools, such as possible areas of surveillance, implementing the management module, time response of the software, artificial intelligence (AI) techniques, building the required neural model, extracting and optimizing the deep learning model, and hardware for data collection. 3. To offer consultancy and collaborate with the industry in developing the solution and help in modifying or proposing potential software or applications of the proposed hardware improvements for the use of road traffic, which can increase overall road vehicle security. Any individual is free to contact during the research process; provide feedback or comments on the study. The main task or primary priority now is to work and search smartly to partially build and also test the existing advanced tools in developing the soon-to-be-developed work and current updated project.

2. Fundamentals of Vehicle Security

Vehicle security is a multi-disciplinary practice that has developed many techniques and methodologies over the years. In order to accurately assess vulnerabilities and opportunities for the expansion of this research area, it is necessary to have a comprehensive knowledge of frameworks and focal points. The modern approach to vehicle security combines human-centered design, engineering practices, and regulatory compliance to better understand the needs, vehicles, and the operational environments. Vehicles are known to have many complementary security measures over the years. These measures include mechanical and hardware-based solutions, like locks and bolts, to more recent technology-based measures, such as immobilizers, alarms, and central locking systems. These systems are displayed at many public events in an attempt to display a secure image, which can only be overcome by a professional. Previous literature has described how such systems can be bypassed, assuming that an attacker has physical access to a vehicle. Attackers have followed this, and there is a low-level market that involves selling devices to bypass or turn off security measures. Additionally, there are many discussions exploring the design and vulnerabilities of modern vehicles. These include enthusiast and security professional documentation, many of which explore potential applications of existing bypass tools. As a result, there is a growing body of knowledge and an expanding market with multiple sources for help and advice available. Knowledge serves as a necessary background to contextualize advanced security solutions. Fits of both decentralized and centralized vehicle security systems.

2.1. Traditional Security Measures

Car anti-theft systems have been developed from passive physical locks to active alarms and immobilizers to thwart theft. Firstly, a thief has to break a lock and then physically drive a vehicle away. Faced with a locked car, a thief will have to try to find a weakness in a car's security, and some may simply decide it is too much trouble and give up. After unlocking a car manually, the thief can hot-wire it to make their getaway. They disassemble a steering wheel column to replace the ignition mechanism by short-circuiting wires. Additionally, they bypass a car security system. It is illegal for car owners and lawful car drivers to perform the hot-wiring process and instead requires specialized equipment and technical skills. Alternatively, the lock can be manipulated with a slim jim or lock-pick. It is equally illegal to enter a locked car for the purpose of stealing, but a car key can be bought on the black market.

Vehicle design and service also change the way in which these locks and keys are upgraded or broken into.

Modern vehicles have many security features. For example, alarms produce intimidating light effects and loud sounds to attract attention and prompt a thief to leave a car or particular accessories behind. Similarly, immobilizers use various mechanical locks, measuring devices, or digital electronic locks or more complex key interfaces to lock movement. Steering wheel locks and tire claw locks prevent a thief from steering or rolling a vehicle once inside. Strong metals are used to build more secure security devices. While security technology has significantly evolved in recent years, the tools and methods used by burglars have been shown to develop as well. The few people who can perform these acts generally work in groups because the steps require different skills. The lock method takes a bit more time but, when carried out properly and quietly, leaves no damage behind. Alarms and immobilizers are mandatory in most countries, and their effectiveness at preventing car theft was confirmed by interviews with criminals. These traditional passive and active methods are capable of deterring theft. Still, it is much less effective against professional criminal groups with high technical security skills and operating in networks. Additionally, relying only on these methods is simply not precautionary enough.

2.2. Challenges in Conventional Systems

One of the major challenges of using conventional methods as security solutions for vehicles is that these solutions tend to become obsolete over time because they do not get updated. Therefore, they provide less security and are vulnerable to attacks. The use of advanced technology is growing with the increasing demand and dependence on vehicles, so there is a need for more innovative security and safety systems that are adaptable to the changing environment. Another limitation of conventional methods is their complex technologies, which exceed the knowledge of common people. The effective use of conventional methods may also rely on strict rules and compliance from users, which is a significant challenge. The need for the development of new and robust security and safety systems is also evident because these conventional technologies only provide opportunities for attackers to exploit weaknesses left by manufacturers. Mainstream companies are increasingly interested in converting vehicles into more advanced computers on wheels, largely for competitive

advantage. This has a number of associated problems. The boundaries between information security and the physical protection of vehicles are no longer clear, and the potential to make a car unusable through cyber attacks is an emerging risk that needs careful attention. Certain manufacturers' vehicles have already been unlocked and started remotely by attackers. Demand for stolen car parts seems to be increasing, making it difficult to stamp out crime using security technologies alone. Criminals are studying existing vehicle anti-theft techniques and systematically developing sophisticated methods to counter each challenge. Each new technical fix seems to attract a new theft technique. Criminals tend to work as members of organized gangs, often using carefully developed techniques and traveling across international borders. Systematic use of local criminal intelligence to identify developing techniques, changing targets, and mobility patterns provides a simple approach to follow. For each new theft technique and vulnerability, one can consider how AI could be used to create security. The emerging sophistication of vehicle crimes suggests that there is a latent demand in the black market for the skills of others in the development of technology-based security systems.

3. Machine Learning in Vehicle Security

The use of machine learning in vehicle security has been widely discussed. Machine learning is a modern and effective artificial intelligence method that can process large amounts of data to identify possible threats and make instantaneous or delayed mitigations. With the help of machine learning algorithms, the vehicle learning process is conducted. The architectural overview and classification of different vehicle learning mechanisms are also widely discussed. The predictive analytical features of machine learning are different from traditional auditing mechanisms, which are used to uncover security concerns.

The existing literature emphasizes the use of machine learning in vehicle security, especially in detecting and responding to feasible vulnerabilities by incorporating exterior data and establishing sign models. Moreover, the prevailing narrative is that machine learning can be used in intelligent platforms to help stop, prevent, or reduce the results of security attacks in UAVs. Real-time threat detection has been the most significant application of machine learning in UAVs. Another important consideration when developing vehicle protection systems is the adoption of predictive analytics. As a matter of fact, predictive analytics

determines what is likely to happen. Another element of an AI technique is the decision-making procedure, which is essentially reliant on a set of rules that are used to figure out what to do in a certain circumstance. Predictive analytics would operate as a preventive measure on a security breach. By employing approved algorithms, vehicle security workers may perform partial application detection. Over the past decade, there has been a notable increase in the activities of the UAV industry. The empirical findings exposed various types of countermeasures, with companies offering UAV countermeasures and their pervasive usages.

3.1. Overview of Machine Learning

Machine learning is a domain associated with the study of algorithms and models that systems use to perform tasks without explicit instructions. The use of machine learning to identify distinct cases of interest within security systems constitutes an active area of security research. Often, the algorithms are designed so that machines can perform their tasks and detect unusual entities, patterns, or behaviors automatically. "Machine learning" and "pattern recognition" are two areas being investigated to increase the accuracy of certain systems while trading off other goals such as speed, flexibility, and processing complexity. Machine learning provides different techniques and models that can be used by security researchers to accomplish classification-based and regression-based tasks. The primary focus of supervised learning is to learn information or structure from labeled data, which is abundant in security contexts, whereas techniques lacking labeled data are described by unsupervised learning.

For categorization of input data, using the pattern of output labels is referred to as classification, and making psychological predictions involving interdependence and variability among different variables is referred to as regression. By breaking the related dataset into two parts—learning and testing—and by using learned information or structure, it can achieve predictions of any novel data sample. This approach helps enhance the model's generalization aspect. Conversely, clustering assists individuals in verifying data's proposed hierarchical structures and is heavily reliant on unsupervised learning. A major criticism of machine learning concerns the quality of the training set. Early in the training or iterative process, an abundance of data is necessary for model learning. It is often the case that classifications degrade in accuracy when training data are poor or substandard, a factor that makes the quality of pattern recognition subject to overhead costs.

In many applications, machine learning comprises an iterative process that gradually refines a continuously improving model. Accordingly, when faults occur in the process of classifying data, conscious human intervention may be necessary for the system in question to be fixed and hence improved. However, in other scenarios, collecting more data allows systems to improve on their past actions by adapting to new circumstances. Within security, attaining and collecting pertinent building information enables machines to learn their capabilities. Models get better with more data at hand; in essence, models require more training information to make them more robust and versatile, that is, they should be able to learn from new datasets. They can be periodically trained offline with incrementally updated or fresh data to be operational.

3.2. Applications in Real-Time Threat Detection

In recent years, machine learning has been proposed for use in real-time data stream analysis for vehicle security. Such systems can continuously process large volumes of data generated from diverse sources including vehicle sensors, global positioning systems, and in-vehicle networks to swiftly identify deviations that signify a threat to vehicle security. The timely detection of threats is critical to ensure that users and network operators can respond to incidents in a proactive manner. Real-time security measurement and descriptive tools have the potential to provide visualizations and alerts in real-time to identify if and when unauthorized access and attacks are subsequently performed.

Recent research indicates that machine learning-based systems could be used to analyze the vehicle data streams for critical situations contributing to failure in one or more functions of the vehicle. Such proposals would be compatible with the system scheduling condition as the aim of the system is designed to create alerts and visualizations for security managers to take subsequent action. This demonstrates the interactive nature of the synergistic interaction between the vehicle and the security system. The provision of timely alerts to users is in stark contrast with the offline data algorithms as it enables the security user to take immediate preventive action against unauthorized controlled access and not just the following subsequent access. In-vehicle use cases could include analysis of global positioning systems, as security managers could set guidelines detailing when an authorized driver leaves the vehicle unattended if there are movement patterns immediately indicating an unauthorized

update of the vehicle's GPS or if there are no movements at all which could indicate vehicle theft.

The challenge of reducing the processing time of AI pipelines against different attacks within vehicle AI is significant. Most AI pipelines have limited real-time processing times which make it difficult to analyze all of the vehicle AI telemetry before sending the results back to the driver. However, considering the development of mature vehicle AI technologies, new real-time intelligent detection systems are feasible. These detection systems can analyze some data regarding the unauthorized or untrusted behavior of the drivers in the vehicle as well as physically block access or disable certain data feeds to other vehicle AI applications. The generic transport design outlined is functional for deployment in different vehicle types provided GPS and Internet connectivity are present, plus the vehicle has internal ECU logging. It is recognized that ethical approval and trial results will also vary between the deployments as while the primary vehicle operations may be the same, how security implementations are tested or tried and the security requirements will differ by application or by country where trials are being conducted. The challenge for scaling the concept is that merely considering GPS security, be it maritime, air, or land, there are many different vehicle types and additional safety, security, and international regulations that the generic design should consider. However, the value proposed in having a system that provides real-time summaries of the vehicle's tracking data for security use is transferable across different vehicle types.

4. Intrusion Prevention Techniques

Intrusion prevention is a significant security approach used to secure any vehicle against unauthorized access. In addition to reducing the possibility of being attacked, such techniques are also considered to offer a proactive security approach. An intrusion prevention system uses real-time feedback to detect suspicious activities and alerts the intrusion detection and protection systems in the context of zero-day vulnerability to discover identity thieves and verify their legality. Users can then stop and block any upcoming actions in preparation for the possible assault. Therefore, it is a proactive system because it suppresses potential misuse, allowing customers to secure and limit harmful activities.

Intrusion detection is performed using various sensors that monitor humans in the proximity of running vehicles. In addition to these, the systems are typically based on the analysis of signal data such as radar or lidar data. Similarly, acoustic or wavelet data can also be used. Most of the sensors developed so far can be categorized under the following groups: (i) through wall imaging, (ii) determination of human motion trajectory, (iii) shape information-based sensors, and (iv) presence or absence of any object-based sensors. In their basic form, these sensors are not used in isolation, but typically, the tracking of human motion trajectory requires not only information about the direction of the moving object, but also the relative orientation, the velocity, the location, and the distance of the object needs to be determined.

In addition to the sensory data, behavioral characteristics can also be utilized to identify some intruding individuals. The behavioral characteristics used to identify the intruder can, broadly, be divided into profiling, which explains the 'normal' set of behaviors a person might exhibit, and anomaly detection, which includes the identification of non-normal behavior and flagging of it. Profiles can be of various types, such as those which tell about 'what' actions can be performed, using what component, 'how' the task is performed, etc. Profiles can also be case- or context-sensitive, which would mean that different profiling rules need to be used for detection in different scenarios. Furthermore, systems need to be designed to be context-aware, so that different patterns of behavior can be modeled for different areas and normal patterns are only detected in the correct context. Behavior can be inferred from sensors distributed in the environment or from a history of activities. Inference from monitoring sensors is real-time or live behavior discovery, while inference from activities is a post-hoc discovery of behavior. Generally, combining multiple techniques through a layered security approach represents the most effective defense. AI can be used to enhance various concepts presented in this section.

4.1. Sensor-Based Systems

Sensor-based systems. In this aspect, various sensors are employed, which can detect unauthorized access into the vehicle and/or detect suspicious motion behavior around the vehicle. Later in this review, we provide an overview of a few of them and the known state of the art. With the advancements in alert systems, if an event is detected, an alert is sent to the

rightful vehicle owner as well as to the command and control center where the security personnel can intervene.

Motion detectors: These sensors detect potential criminals that touch the sensors or generate heat, and this information is analyzed to determine if access to the car is unauthorized. Cameras: When a camera placed inside the vehicle detects unauthorized personnel, once it is detected, a possibility to send an alert will be present. Furthermore, a camera placed in a vital location can detect if a vehicle was stolen. GPS-based systems: When a vehicle is stolen, one approach to automatically detect the theft is to fit a GPS module that uses cellular phone transmission to automatically detect the theft. All of the systems alert security personnel after the fact. There are GPS-based systems that are connected with mobile phones, where you can receive an alert on your mobile phone in the event of a theft. Finally, and unfortunately, none of the above solutions allow real-time detection in most scenarios. Issues in mathematical models have been innovated to use signal processing algorithms with increasing sophistication to achieve more accurate detection of access methods. While individual sensors generally cannot specify a particular security threat, the combination of many sensors, i.e., sensor fusion, adds up to a sensor network solution that should be able to provide most of the solutions sought when trying to meet the level of situational security. It has been discovered that there are limitations to this approach, particularly because sensor accuracy can never be 100% correct nor near 0% wrong. One class of problems is called false positives, where the alert system sends an alert every time the light beam increases.

4.2. Behavioral Analysis

A theft alarm is usually triggered when a thief has already accessed the vehicle, so it is too late to prevent the theft. The goal of behavioral analysis methods is to determine a typical behavior for each person and then use the developed methods to detect anomalies, which may indicate unauthorized access. Behavioral analysis, however, cannot be based only on the sum of point data but should also include knowledge of the individual user and their driving behavior. An approach to the continuous profiling of users combines user profiling with vehicle-context prediction in security-related applications.

A completely different approach to the development of a secure tracking device is proposed. The suggestion is to use a prediction-driven unit that models different aspects of a tracked

person's behavior based on behavioral profiles. Anomalies in the observed behavior would result in updates to the current system's models in near real-time. Various profiling and predictive techniques could target both security and business intelligence. A potential weak point of the approach used is that evaluating driver behavior with all details is very time-consuming, so complex investigations may not be performed in the case of a short theft attempt. Additionally, the continuous prediction of all possible driver behaviors may lead to a practical problem of data storage for very long periods. In determining the behavioral profiles described, the necessary data will probably violate the privacy of road users, as the method takes advantage of practically all their behaviors. Moreover, such an approach implies that human behavior could be predicted in the long term, which leads to many privacy and ethics problems. The potential for surveillance generated by machine learning and artificial intelligence technologies can also be used to project future actions. It is believed that from an ethical point of view, no kind of learning based on the probable opinions of individuals should be performed. The analysis of behavior is not considered as a prediction of the future course of action, but rather a window into the present state of mind.

5. Theft Prevention Strategies

The research in security features for vehicles avoiding theft has come up with some very interesting outcomes. Geo-fencing prevents the vehicle from being started if it is not in a particular geo-location. Carjacking can be avoided using an RPM sensor that switches off the car engine if there are fluctuations. There is an Intelligent Tracking System, popular among most car rental companies, which now has more features for stolen vehicle recovery and increased operational safety for the users. IoT wearable devices are useful for authenticating car occupants to avoid theft by sending all the occupant-facing cameras to the owner in case of theft. Biometric authentication also prevents vehicle theft by recognizing only a predefined person to unlock and drive the vehicle. Many theft prevention features can be achieved using an Advanced Driver Assistance System.

Advanced AI-based solutions can make it much more difficult for a thief to steal the vehicle. Geo-fencing solutions will prevent the vehicle from starting if it is not parked in a predefined area. In this scenario, an RFID sensor mounted on the vehicle will communicate with the GPS, and when all three criteria are matched, the vehicle will turn on. In case of moving the

geofence, the vehicle will switch off. A very interesting solution for OEMs is an Advanced Tracking System that provides exact positions regularly and lets customers know about the vehicle's transition into a new position to avoid theft and recover the vehicle instantly. A holistic prevention strategy against theft is a combination of both mechanical means of theft reduction and mechanisms of theft recovery, immobilizing the vehicle for use by any other occupant other than the owner, as well as taking countermeasures against hacking attacks. The implementation of these features will make vehicles difficult to steal.

5.1. Geo-Fencing and Tracking Systems

Geo-fencing systems are GPS-based technologies that create digital geo-fences to trigger alerts when a vehicle enters or exits a designated area of operation, such as a construction site, a city, or a constituency. The alerts are generated using real-time geographic location capabilities and directed to individual smart devices. Geo-fencing capabilities can be initiated by integrating onboard diagnostics data points with GPS data or radio-frequency identification technology. The proposed model will assist in curbing vehicle theft by alerting vehicle owners to possible vehicle movements as soon as they occur, anywhere in the world. While other tracking systems provide similar mechanisms for peace of mind to vehicle owners with enhanced satellite coverage, this model enhances the vehicle owners' level of interaction as it connects the functionality of the vehicle immobilization feature with their smartphones. This gives vehicle owners more control from the user end, mobile application engagement, and actionable functionalities when an alert is sounded. Tracking systems enable the police to detect a stolen vehicle in order to conduct a convoy and pull over sooner. It should be noted that the system operates based on data provided by mapping services; a remote area in the rural bush or central business district may complicate the alerts for the right authorities to respond quickly. Geo-fencing and tracking systems play a significant role in recovery. There is potential for decisions to be overturned regarding disqualifications of those feigning ignorance on double registration, thereby increasing the conviction rates for vehicle theft in the courtroom. The assumption can be made that vehicle owners will opt to switch off the security feature should it warn a competing party of an impending business opportunity the moment the vehicle has been tampered with. Data privacy and protection laws must be obeyed, and police loitering must be regulated to prevent misuse of the tracking system. The

vehicle owner will also have to be held responsible for making the choice to install and activate the devices.

5.2. Biometric Authentication

Biometric authentication has attracted significant attention given its prominence in security-based solutions. It employs the science of recognizing individuals based on unique biological traits possessed by humans. This method provides an increased level of identification accuracy that ensures a high level of system security and, ultimately, user identity. Often expressed in commercial products like USB-based biometric fingerprint recognition, laptops, and smartphone devices, the application of biometric authentication is outgrowing urban and rural areas. Generally, biometric authentication has found applications not only for restriction purposes but also for user acceptance. New and old vehicles have incorporated biometrics in their security systems. Biometric authentication is required to unlock the vehicle and start the engine, thereby preventing unauthorized use.

The vital importance of biometrics in preventing unauthorized access cannot be underestimated. Its inadequacies in other areas have been criticized, as previously highlighted through subjective and objective tests that, in turn, provide the proportion of user-PIN authentications. Despite this criticism, biometric authentication continues to gain acceptance. This is because of the system's user convenience, as the user is free from the burden of carrying physical keys, as in keyless entry systems and for physical entry as in fingerprint-based systems. In the few examples presented above, the technology uses alternatives—either fingerprint identification or finger vessel patterns to manage operations like unlocking the car and turning the ignition on. Despite the growing appetite in automotive mechanisms, the absence of a standardized format and the growing concern over storage safety and privacy may deter future growth. These experiences serve as a guide to similar systems because the failure of one system due to inaccurate acceptances or rejections reflects the fact that biometric systems require solid and reliable solutions.

6. Case Studies and Implementations

The AI and ML technologies are widely developing into various industry sectors. In this paper, we have studied AI and ML-based approaches for enhancing the level of security for

high-value goods. These AI and ML techniques help to improve the security level of cars and reduce the risk of theft or breaches of cars armored with high-value missiles and ammunition. A simple inertia navigation system is developed to detect the relationship between the navigation system and the automobile body. The innovation improves the flexibility of a driver to maintain the reliability of the information obtained by the system. The system calculates all possible positions within 20 km using the time information obtained from the satellite communication system.

For each position of the automobile, data processing is done for locating the target. The automobile is modified to drive by wire mode for better sensor output. To detect curved road edges, GPS, gyros, lasers, and a single camera are used in conjunction as sensors. Identifying the sensor and determining the results are the key focus of the study. Alternatives for AI solutions are explored and evaluated in the context of prior art. Reserved data solutions for position estimation eliminate a priori data and assumptions. Other alternative methods like the neural-environment model, velocity-position Kalman filter as a sensor fusion method, neural networks in curve detection, artificial neural networks in position estimation from images, and Kalman filter as a sensor fusion method are used.

Case studies provide practical insight and measure the effectiveness of solutions in operation. In practice, there are indeed many solutions aimed at defying car theft and other related issues; from advanced vehicle tracking systems to high-performance video surveillance for parking lots and garages, as well as a variety of sensor-based systems incorporated into cars. Customization of such systems began to receive interest, and the integration of these solutions is also of interest. Car-anomaly detection using online learning is related to AI—to allow it to retrain or change its behavior as new data become available. Different features in short-term deviation cases are analyzed, concluding more than 90% accuracy in detection. An AI-based approach is used for feature selection in statistical methods such as AdaBoost, random forests, decision trees, and Naïve Bayes to create a methodology named ADAS (Anomaly Disturbance Analysis System). ADAS has a detection rate of all anomalies of 94% and a computational cost that is acceptable with a delay of 30 ms. To obtain the most out of auto data, AI has also been proposed with fuzzy c-means and feedforward artificial neural networks. The results were 88.31% preventive accuracy in detection.

6.1. Real-World Applications

One of the best ways to understand the impact of AI and machine learning in vehicle security solutions is to review real-world applications of these technologies. Based on experiences with end users, we can see that companies are indeed investing in highly advanced solutions for cellular and radio communication security. In the trailer tracking sector, companies use machine learning algorithms to protect highly valuable goods in storage and in transit. In the fleet management sector, companies enhance AI-based solutions with edge computing monitors; the operating condition sensors and EOBR functions within these products add even more vehicle security capabilities. A driver's associations versus a driver's habits feature has been included within products.

Automakers are adding AI machine learning technology that monitors a driver's use of devices, onboard systems, and the vehicle, hence a personalized vehicle. For example, a concern with the driver journey and the owner's personal preferences development shows the direction where the AI capabilities are being provided to end users. Evolving requirements for vehicle-based protection show new types of towing from the front in the U.S. and in Europe, and consumer acceptance of these new standards. Thus, cars can be found today with the camera linked to machine learning that look for familiar or unusual data, and react in various ways like sounding the horn, accelerating, sending an audio signal of distress, or granting the car permission to park itself while calling a rescue service number. Vehicle personalization is today becoming comprehensive, meeting the multiple factors that individuals face daily. Unlimited possibilities for AI and/or machine learning outcome technologies can make operations futile. Therefore, the technologies shared in this series, with values and measuring improvements, for a greater return on investment approach, are one way to approach the future. We must also remember that no system is 100% effective and operations and human controls, developed in association with AI and machine learning systems to identify and understand threat level or detection in real-time progression, weaken transportation-related security over time, are essential. In threats, progression and detection have to be fluid, constantly evolving in today's complex attacks on vehicles, companies with dedicated security groups and trained cross-education for adaptability, methods, and analysis within their company, in order to ensure the security of technology with a vision into the future.

6.2. Success Stories and Challenges

Multiple success stories illustrate the effectiveness of leveraging intelligent digital and AI tools that translate camera footage into a data stream and yield security benefits. Commonly highlighted wins include a return on investment stemming from reduced internal and external theft, shrink, and losses. One case involved a leading global vehicle rental company that experienced a drop in theft rates after adding cameras and AI-based theft detection software to its trailers. Receivers of these trailers often dismantle and salvage them because the average resale value for a salvaged trailer is typically $50 above scrap rates in the U.S. With these sizable gains, a weakness of AI-based video analytics technology is the willingness of stakeholders, including aftermarket venues, to embrace them and their potential legal limitations.

Success. Prior to adopting any video security technology, this top 50 vehicle rental company approximated that more than 6% of trailers were being stolen with only a 0.4% recovery rate. In a recent phase of a multiphase initiative that involves 3,000 reefer and standard trailers, participants in the secure transport of pharmaceutical, electronics, and automotive equipment were experiencing a 10% loss rate due to salvage thefts. To address this weakness, the rental company pursued a technology-driven approach, beginning in 2018. Innovators, including C-level leaders with a stake in developing competitive advantages to impact the bottom line, derived actionable business strategies after participating in interviews with 23 companies and two focus groups consisting of 10 companies. Managers represented a broad range of U.S.-based OEMs, 3PLs, less-than-truckload carriers, IP lawyers, and investigators specializing in cargo theft. Management positions ranged from supply chain managers, security analysts, and senior investigators to senior vice presidents, vice presidents, and marketing, compliance, human resources, procurement, finance, and C-level executives.

7. Future Directions and Emerging Technologies

7.1 Future Directions in Vehicle Security

Advances in AI are expected to bring the vehicular security infrastructure to the next level. It is possible that personal AI will become a completely integrated part of a future vehicle. These AIs could be entrusted with a host of responsibilities for the safety and security of the vehicle

and its occupants. As AIs grow in size and capability, they could be entrusted with physical vehicle security roles such as patrolling a parked car on behalf of its owner. Many AIs will also have the capability to download and learn from their surroundings using advanced architectures. The integration of different AI learning techniques or model types will likely become standard practice. Many decision-making models will integrate aspects of dynamic function approximation, and thus will represent a class of hybrid expert systems with both learned and deterministic processes. Future security systems are likely to be part of a more general trend towards collaborative technology working in harmony. Communication is expected to be an integral part of future secure vehicles, allowing for long-range coordinated defenses.

One of the most anticipated advances in AI is, of course, its ability to learn from its environment. Those machine learning models that learn and adapt their behavior form the third AI trend. These systems are especially interesting as future selves, as one could, for example, enable a security system to have different behaviors for a car while it is parked in a well-lit area and another when the vehicle is parked on the street. The launch of advanced systems is not far away. Security models for autonomous systems might be the biggest growing trend in AI, and with the demand for autonomous systems growing, so does the need for models which can secure and protect these systems. Another focus for future research is to integrate advanced sensors with AI models. The aggregate capabilities of advanced sensors with machine learning in basic intrusion detection are expected. Specialized data analytics will exponentially increase the quality of the security information available and allow for next-generation security models, and could even allow the development of predictive security models. Another focus is to try to find out what future threats will emerge. Some areas of focus should be uniformly developed for defensive research, like improving vehicular security response and resilience systems, studying their function, orienting efforts toward intelligence-led methods, assessing and responding to general threat trends, and accelerating security, patrol, and response systems. These research thrusts can indicate the largely anticipated need to guarantee that vehicular defense keeps pace with technological advancement.

7.1. Advancements in AI for Vehicle Security

Advancements in AI are expected to shape the future of vehicle security. Research and development in the field of artificial intelligence are geared towards improving existing security measures. Research breakthroughs in the areas of deep learning and neural networks are potential options. Deep learning models boast their ability to establish a multilayered representation of data. Neural network models are known for their high level of accuracy in recognizing patterns among dynamic input signals. Artificial neural networks are considered a prominent example of computational systems that can distill useful insights from large amounts of data. Predictive analytics based on AI models are shown to be more accurate for threat detection and reduction.

AI models can predict behavior or physical operations of systems using operational data. AI is increasingly able to process a large proportion of IoT data, obviating the duplication of work that results from multiple tasks undertaken by both AI and IoT systems. The moves to connect AI and IoT systems support the use of AI in various security functions. Existing literature discusses the potential of AI and machine learning models in increasing the potential for better vehicle security. AI-based solutions, however, pose some data privacy and transparency issues. A solution concerning the transparency of the model design and algorithm employed in the learning process is still nascent. Data management is another issue that needs to be considered. All the data reported in the model must come from a verified source to ensure the inputs are consistent and complete; otherwise, the security system's accuracy and precision may be affected. AI and statistical approaches are promising in enhancing the security of vehicles. These enhancements are all potential changes for vehicle security.

7.2. Predictions and Trends in the Field

Even more interconnected vehicle systems. The next few years will still witness an increase in the volume and variety of vehicle-integrated systems and devices. Additionally, we will see more complex interconnected systems within the car as well as with the outside world. The security architecture of vehicles and their components will need to be modified so that they do not allow a chip inside the tire to control the brakes. A big change in user behavior. Today's cars offer a high level of comfort and convenience. Nevertheless, new vehicle users are demanding new security functions because they have learned from their smartphones and other platforms that these can be provided and, even better, be part of the physical security

platform. These trends will undoubtedly lead to new developments in introducing vehicle security as user behavior and expectations exclusively drive the market. It is expected that users will rely more on "autonomous solutions" than on "CAS solutions." Technological changes will require updates in regulatory requirements and trends. As artificial intelligence grows in importance, new user behavior is emerging as traditional "driver-centric" cars do not yet predict the evolution of autonomous or fully autonomous driving behaviors.

Hybrid systems trend. Once identified, hybrid systems that combine AI-based solutions and current classical solutions are not moving towards the abandonment of the "dumb" chip. There is potential for growth in a research area for use in Asia. This region is characterized by rapidly growing technological prosperity as well as a variety of secure mobility solutions developed for personal vehicles in areas of autonomous trucking. In the coming years, the adverse effects of emerging technology are expected to have a greater impact on the development of vehicle security systems. As a result, cybercriminals are expected to develop new attack types, and users are expected to have security issues with AVs and IVs. Research aspects related to safety are also emerging as a research product to identify such potential weaknesses and vulnerabilities quickly and perform corrective actions and secure system designs. Recent trends also suggest that the use of AI in vehicles can trigger several advanced side attacks. Researchers should pay more attention to further developing AI adversarial attacks in the context of safety and security considerations when designing IV solutions. Legislation and regulation, primarily concerned with safety, will also require consideration of trust and assurance. This will certainly give OEMs impetus to increasingly consider the need to provide users with proof that their vehicles are secure. This must be documented in a casual setting.

8. Conclusion

This paper presents an extensive review of various AI-based solutions that seek to enhance the effectiveness of tailored vehicle security systems. In doing so, pertinent insights have been gathered to underscore that many vehicle crimes, including car theft and hijacking, are growing at alarming rates. After conducting a comprehensive analysis of this growing problem, it is clear that there is an urgent need to incorporate the recent advances in real-time image processing and machine learning to not only predict but also to combat the increasing

crime rates of vehicle-related offenses. The findings of the current study suggest that over the last two decades, researchers have primarily explored two innovative technologies to prevent vehicle crime: 1) RFIDs or wireless sensor technology for recognition, control, and surveillance of vehicles; and 2) AI-based systems for targeted security solutions that prevent unauthorized entry into the vehicle. Thus, the study may serve as a springboard for future research in identifying the potential of integrating advanced, intelligent solutions for comprehensive research. In conclusion, early warning of potential criminal activity in vehicles is an area in which current technology has struggled due to the numerous challenges, complexities, and errors in traditional firewalls, face recognition, and cryptography. A comprehensive review of the various AI-based solutions has been presented throughout the various sections of this paper. The extensive review has mapped over two decades of technological development in different domains that are foreseen as challenging dimensions in preventing traditional solutions from intruders. We have reviewed two main areas of research from the last two decades, explored as promising directions with certain related publications that could be reinforced with the results of this research as a part of future work.

Reference:

1. Tamanampudi, Venkata Mohit. "Automating CI/CD Pipelines with Machine Learning Algorithms: Optimizing Build and Deployment Processes in DevOps Ecosystems." *Distributed Learning and Broad Applications in Scientific Research* 5 (2019): 810-849.

2. Pal, Dheeraj Kumar Dukhiram, et al. "AI-Assisted Project Management: Enhancing Decision-Making and Forecasting." Journal of Artificial Intelligence Research 3.2 (2023): 146-171.

3. Kodete, Chandra Shikhi, et al. "Determining the efficacy of machine learning strategies in quelling cyber security threats: Evidence from selected literatures." Asian Journal of Research in Computer Science 17.8 (2024): 24-33.

4. Singh, Jaswinder. "The Rise of Synthetic Data: Enhancing AI and Machine Learning Model Training to Address Data Scarcity and Mitigate Privacy Risks." Journal of Artificial Intelligence Research and Applications 1.2 (2021): 292-332.

5. Alluri, Venkat Rama Raju, et al. "Serverless Computing for DevOps: Practical Use Cases and Performance Analysis." Distributed Learning and Broad Applications in Scientific Research 4 (2018): 158-180.

6. Machireddy, Jeshwanth Reddy. "Revolutionizing Claims Processing in the Healthcare Industry: The Expanding Role of Automation and AI." Hong Kong Journal of AI and Medicine 2.1 (2022): 10-36.

7. Tamanampudi, Venkata Mohit. "Autonomous AI Agents for Continuous Deployment Pipelines: Using Machine Learning for Automated Code Testing and Release Management in DevOps." Australian Journal of Machine Learning Research & Applications 3.1 (2023): 557-600.

8. J. Singh, "How RAG Models are Revolutionizing Question-Answering Systems: Advancing Healthcare, Legal, and Customer Support Domains", Distrib Learn Broad Appl Sci Res, vol. 5, pp. 850–866, Jul. 2019

9. S. Kumari, "AI-Enhanced Mobile Platform Optimization: Leveraging Machine Learning for Predictive Maintenance, Performance Tuning, and Security Hardening ", Cybersecurity & Net. Def. Research, vol. 4, no. 1, pp. 29–49, Aug. 2024

10. Tamanampudi, Venkata Mohit. "Leveraging Machine Learning for Dynamic Resource Allocation in DevOps: A Scalable Approach to Managing Microservices Architectures." Journal of Science & Technology 1.1 (2020): 709-748.