Journal of Multimedia Information System VOL. 9, NO. 1, March 2022 (pp. 33-42): ISSN 2383-7632 (Online)
https://doi.org/10.33851/JMIS.2022.9.1.33

The Intelligent Blockchain for the Protection of Smart Automobile Hacking

Seong-Kyu Kim[1], Eun-Sill Jang[2*]

Abstract

In this paper, we have recently created self-driving cars and self-parking systems in human-friendly cars that can provide high safety and high convenience functions by recognizing the internal and external situations of automobiles in real time by incorporating next-generation electronics, information communication, and function control technologies. And with the development of connected cars, the ITS (Intelligent Transportation Systems) market is expected to grow rapidly. Intelligent Transportation System (ITS) is an intelligent transportation system that incorporates technologies such as electronics, information, communication, and control into the transportation system, and aims to implement a next-generation transportation system suitable for the information society. By combining the technologies of connected cars and Internet of Things with software features and operating systems, future cars will serve as a service platform to connect the surrounding infrastructure on their own. This study creates a research methodology based on the Enhanced Security Model in Self-Driving Cars model. As for the types of attacks, Availability Attack, Man in the Middle Attack, Imperial Password Use, and Use Inclusive Access Control attack defense methodology are used. Along with the commercialization of 5G, various service models using advanced technologies such as autonomous vehicles, traffic information sharing systems using IoT, and AI-based mobility services are also appearing, and the growth of smart transportation is accelerating. Therefore, research was conducted to defend against hacking based on vulnerabilities of smart cars based on artificial intelligence blockchain.

Key Words: Smart Car, Big Data, Deep Learning, Cyber Security, Artificial Intelligence.

I. INTRODUCTION

The more advanced and advanced the technology for smart transportation, the more important the security-related importance is in this paper. As the transportation system is directly related to the safety of users, the associated security threats will intensify and become more complex, and the extent and impact of security accidents will be greater. Therefore, in order to safely utilize the technologies associated with smart transportation, users and stakeholders need to enhance security awareness and establish advanced security measures. This paper aims to improve the understanding of systematic and efficient classification of smart traffic and related guidelines. It also presents security requirements for security items in consideration of the threats and countermeasures of smart transportation. The components of the vehicle provide basic vehicle services by sending and receiving CAN (Car Area Network) messages over the internal network, and various services for safety and user convenience through vehicles, vehicles, infrastructure and networks. As the vehicle and the transportation system are networked, exposure to security threats to any of the vehicle's components and transportation services could escalate into an overall threat to the transportation service. As a result, it is important to identify possible security threats from smart transportation and to understand how to attack them [1,2]. The assets of smart transportation services affected by vulnerabilities and threats were divided into 'smart cars', 'communications' and 'external systems' as shown below. 'Smart car' means a smart car itself, including an internal communication system. External systems are classified as back-end servers, other 'smart cars' and 'mobile devices' connected to smart cars, but this paper deals with vulnerabilities and threats to back-end servers in a significant way. The purpose of the research is to use intelligent blockchain to defend against hacking in order to enhance the components of smart transportation, enhance security awareness, and internalize security.

In addition, problems caused by defects in artificial intelligence and automobiles can be classified into intentional

Manuscript received December 20, 2021; Reivised December 30, 2021; Accepted December 31, 2021. (ID No. JMIS-21M-12-053)
Corresponding Author (*): Eun-Sill Jang, +82-31-8075-1660, esjang@joongbu.ac.kr
[1]Department of Information Security, Joongbu University, Goyang, Korea, e-mail: skkim@joongbu.ac.kr
[1]Department of Public Policy and Information Technology, Seoul National University of Science and Technology, Seoul, Korea.
[2]Department of Student Growth and Liberal Arts, Joongbu University, Goyang, Korea, e-mail: esjang@joongbu.ac.kr

and unintentional types of AI(Artificial Intelligent) threats in self-driving cars. Intentional threats are attacks that intentionally exploit the vulnerabilities of AI and machine learning (ML) to cause damage. Intentional misuse of AI creates new types of vulnerabilities, poses potential risks, and requires changes in the current cybersecurity environment. If cyberattacks exploit security flaws and vulnerabilities in AI and ML systems that automate decision-making, AI and ML systems tend to engage in important decisions, which can seriously affect safety issues caused by cyberattacks. In addition, cybercriminals can automate attacks using AI to carry out large-scale attacks more quickly and precisely at low cost. On the other hand, unintended threats arise from inherent functional vulnerabilities related to reliability, robustness, and safety of current AI and ML methods. In other words, disadvantages of AI and ML, unpredictable malfunctions due to design errors or internal characteristics, and interruption create unintended threats.

II. RELATED RESEARCH

This paper studies the concepts of artificial intelligence and the study of various problems and models of emotional learning on how drug artificial intelligence and strong intelligence affect us. It also uses these emotional artificial intelligence to present better models in the future and to create improvement tasks to improve current problems. And it deals with the most important issue of empathy among many artificial intelligence systems.

2.1. Self-Driving Cars

Self-driving cars are composed largely of sensors, processors, algorithms, and actuators. Self-driving is done via the actuator after collecting data about the environment around the vehicle via sensors, and then receiving the data collected by the processor and interpreting the results through predefined algorithms to make driving decisions [3-5]. The most important of these processes is a software algorithm that makes decisions about steering, speed and stopping based on large amounts of data collected through sensors. Google, which is considered to be the leading driver of unmanned vehicles, is constantly collecting information through the operation of unmanned vehicles because it also aims to create more complete algorithms. It is developing from sensor-based safety technology that utilizes radar, ultrasonic waves, and cameras to V2X (Vehicle to Everything) Integrating Infrastructure-linked Traffic Information [6].

In addition, cars that can be driven on their own without human drivers intervening in vehicle operation are defined as "autonomous vehicles", which are divided into partial and fully autonomous vehicles depending on the degree of driver intervention and the autonomous driving ability of the vehicle system.

In addition, autonomous vehicles are divided into three main components: sense, thinking, and control, and utilize a variety of component technologies, such as software, hardware, platforms, and networks. Detection is necessary for driving traffic facilities such as traffic signals, lanes, and surrounding vehicles, pedestrians, various obstacles around them, location and speed of vehicles, etc [7].

It is to collect various kinds of data. Detection-related technologies include sensors such as GPS, camera, LIDAR (Light Detection and Ranging), radar 11, etc., dedicated processors (GPU), detection and recognition software, high-precision maps, and vehicle communications (V2X12). In particular, with regard to detection, the advantages and disadvantages of various types of sensors should be well complemented and combined to improve reliability and safety. That is, the sensor fusion process allows reliable and accurate positioning by combining the advantages of all sensors.

2.2. Distinguish the Technology Level of Self-Driving Cars

The U.S. NHTSA first classified autonomous driving technology from level 0 to level 4 (total of five stages) in May 2013. Since then, in 2014, the Society of Automotive Engineers (SAE) has more specifically divided the level of autonomous driving technology from level 0 to level 5, and the contents have been used globally until now after several revisions [8-10]. The World Automotive Engineering Association published the level of autonomous driving technology first distributed in January 2019, using a new chart that is clearer and simpler [11-13].

2.2.1. Phase of Level 0

Level 0 is the driver's level of control and responsibility for everything they drive. The driver will drive at all times, the vehicle's system will only perform auxiliary functions such as emergency alert. The driver of driving control is human, and variable detection and driving responsibility during driving is also at the level of human responsibility.

As shown in (Fig. 1), the SAE provides many standards for the automotive industry. Standards are not binding because they are not laws. SAE J3016 provides a step classification of autonomous driving systems. The self-driving stage that is now on the lips of many people is defined in this SAE. The U.S. Department of Transportation (US DOT) and its subsidiary, the National Highway Safety Administration (NHTSA), cite SAE J3016 in official documents and external communication to explain the steps of autonomous driving systems. However, so far, U.S. laws and regulations do not view this stage as an object of legal satisfaction and certification, and view it as a distinction of the manufacturer's declarative nature.

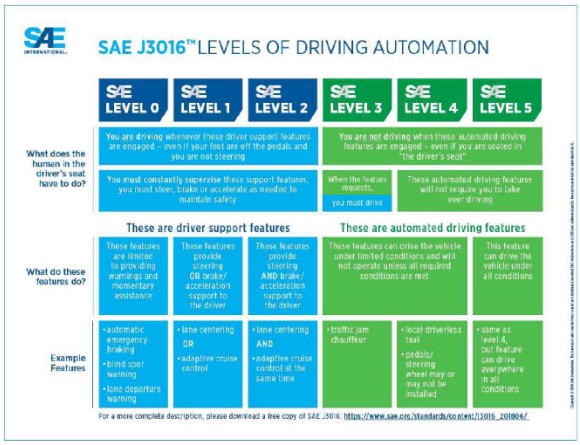

Fig. 1. Self-driving car phase. Sources: SAE, "SAE J3016 Levels of Driving Automation", sae.org (2019.1.7.).

2.2.2. Phase of Level 1

Level 1 assists the driver with adaptive cruise control, lane keeping, and level 1. Activate the system to assist the driver with vehicle speed, maintenance of the car's wheelbase and lane keeping. Driving control principals are in humans and systems, and the detection and driving responsibility of variables that occur while driving is at the level of human responsibility.

2.2.3. Phase of Level 2

Level 2 is a level of technology that enables partial autonomous driving. At this level, the driver should always be prepared and actively careful to intervene in the operation of the vehicle. Level 2 has two or more automation functions in operation at the same time under the control of the driver, and SAE J3016 states that lateral and longitudinal control is maintained in the use of certain functions.

2.2.4. Phase of Level 3

Level 3 is a level of technology that enables conditional automation. In this phase, if the autonomous driving system is unable to manage the vehicle's driving, the control of the vehicle shall be transferred to the driver and the driver shall always be prepared to intervene at any time in the event of a situation.

2.2.5. Phase of Level 4

Level 4 is a level of technology that corresponds to 'high self-driving'. At this stage, an autonomous driving system can control and monitor vehicle driving on its own under certain conditions. While driver intervention is not required during operation of the system, the use of an autonomous driving system without driver intervention is possible in a limited range of locations and environments.

2.2.6. Phase of Level 0

Level 5 is literally a level of technology that enables full self-driving. At this stage, the autonomous driving system controls the vehicle movement on its own in all situations, which does not require human driver intervention.

2.3. Automotive Blockchain

Blockchain can be used for any purpose in automobiles. In order to know this, we need to first look at the value of blockchain. Blockchain can be defined as 'P2P(Peer to Peer) information sharing platform'. While existing systems have information in one place, blockchain is a way to share this information with nodes [14-16]. This provides transparency. However, if information is shared with many people, inconsistencies can occur. This can be caused by a malicious node or system error. For example, the contents of the same information stored on node A and node B may differ. It is the "alignment algorithm" that emerged to solve these problems. Existing systems use consensus algorithms because there is no central administrator in the blockchain if they manage the storage of information centrally. Consensus algorithms are algorithms that contain solutions when information inconsistencies occur. In addition to these features, they are also used to define how blockchain operates. It can also be seen as an algorithm that guarantees the integrity of information. Most consensus algorithms have high integrity because they are determined by multiple nodes. In order to manipulate the information in the blockchain, internal and external malicious people must hack into a number of targets, not one, which is much more difficult than the existing method. These characteristics of blockchain provide three value values. The first value is 'sharing'. Since blockchain is a shared platform, it is natural to provide the value of sharing. The second value is 'trust.' The transparency and integrity of information leads to trust. The last one is 'Departure'. Blockchain does not have a central administrator and has the trust of information. There is no need to rely on third parties [17]. In particular, the de-center was further strengthened as the "Smart Contract" function was added to the blockchain. Smart Contract is a function that allows contracts to be made automatically when certain conditions are met. In other words, there is no need to leave the contract brokerage to a third institution.

As such, automobiles are changing in line with the era of the Fourth Industrial Revolution. This seems to see the transition of mobile phones in the past. The call was the main purpose of the existing mobile phone. However, as it evolved into a smartphone, various applications were installed. As a result, it was transformed into a portable computer. The same goes for cars. Various information and communication technologies (ICT) are being installed in automobiles [18]. As a result, automobiles are expected to evolve into smart cars, and they are expected to transform from transportation to software platforms. For this reason,

it is not strange at all for new promising technologies such as blockchain to be added to cars. As automobiles are connected to surrounding objects due to IoT (Internet of Thing), they can be fused with blockchain. This means that cars can act as participants (nodes) in blockchain.

2.4. Automotive Artificial Intelligent

Before discussing artificial intelligence technology directly in self-driving cars, it is necessary to first address the function of applying artificial intelligence. Earlier, when explaining major areas using GPGPU (General-Purpose computing on Graphics Processing Units), 3D image recognition for vehicle control was mentioned in the autonomous vehicle sector, and a more detailed study shows that pedestrian collision warning devices detect and avoid pedestrians appearing during vehicle operation [19]. The lane departure warning device is a function of detecting and warning lane departure while the vehicle is in operation. The forward collision alarm is a function of detecting and warning a vehicle or obstacle that appears in front of the vehicle while the vehicle is in operation. In addition, the speed limit warning is a function of reading and warning speed limit signs while driving, and traffic signal detection is equipped with a function of reading and displaying various traffic lights and signs [20]. Although a general image processing algorithm may be used to implement the above functions, artificial intelligence has recently been introduced as a way to increase accuracy regardless of context. In other words, instead of creating algorithms first and processing them by adding data, it is a method of creating algorithms by inserting data. This can solve the problem by adding additional data without modifying the algorithm according to the situation every time [21].

III. ENHANCED SECURITY MODEL IN SELF- DRIVING CARS

The components of the vehicle provide basic vehicle services by sending and receiving CAN (Car Area Network) messages over the internal network, and various services for safety and user convenience through vehicles, vehicles, infrastructure and networks. As the vehicle and the transportation system are networked, exposure to security threats to any of the vehicle's components and transportation services could escalate into an overall threat to the transportation service. Therefore, it is important to identify possible security threats from smart transportation and to understand how to attack them. The assets of smart transportation services affected by vulnerabilities and threats were divided into 'smart cars', 'communications' and 'external systems' as shown below. 'Smart car' means a smart car itself, including an internal communication system. External systems are classified as back-end servers, other 'smart cars' and 'mobile devices' connected to smart cars, but in this paper, we conduct model studies on vulnerabilities and threats to back-end servers.

The specific methodology builds a method for systematic security verification of AI models and data. Automobile data plays an important role in building and verifying AI systems in machine learning model learning, so systematic data validation is needed to prevent unexpected confusion and damage through data manipulation by attackers in autonomous vehicle situations. Accordingly, it is required to establish a data governance system in accordance with the specificity of data used for autonomous driving worldwide. In addition, AI models can change over time, so data management should be systematically performed throughout the AI model life cycle. However, in practice, systematic verification of AI models is a challenging task, considering data dependencies and model complexity, and systematically evaluating and testing the security and robustness of AI models by performing extensive systematic verification to ensure data quality and reliability.

3.1. Availability Attack

Availability attacks can also cause an attacker to interfere with communication signals or generate false data in the internal network of vehicle basic and secondary control, resulting in malfunction and malfunction. Signal entertainment, such as GPS (Global Positioning System) and DMB (Digital Multimedia BroadCasting) in vehicle infotainment and signal interference in communication channels with roadside base stations, may cause disruptions to vehicle location and traffic information delivery services. In addition, the influx of false data disguised as multiple terminals can cause traffic congestion due to incorrect collection of traffic information. In addition, various functions for user convenience and safety can be disrupted in the event of signal jamming, interference, etc. on mobile networks (Fig. 2).

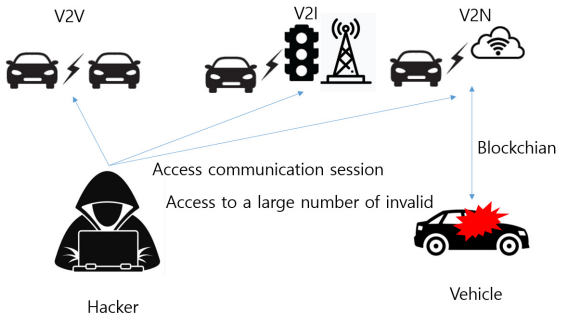

Fig. 2. Availability attack. Hackers show how to hack through various channels through V2V (Vehicle to Vehicle), V2I (Vehicle-to-Infrastructure), and V2N (Vehicle to Network).

Damage to internal systems (CAN Floating) The nature of the wireless protocols used by smart cars (vulnerabilities) or jamming of the smart car gateways, or the vulnerability of smart car gateways to shut down gateway behavior or to service high-value ECU (Engine Control Unit) systems. It also impairs updates due to DoS (Denial-of-Service) attacks, performing denial-of-service attacks on back-end servers, such as OEM (Original Equipment Manufacturer) servers, to disable updates of safety-related vehicles. In addition, short-range communications or sensor-aware interference can cause an attacker to malfunction a short-range communication module mounted on a smart car, causing unauthorized access to the smart car system through vulnerabilities in a sensor mounted on a smart car, and preventing data detection by spoofing. Blockchain also prevents availability damage when services that support the interaction between back-end servers and smart cars become inoperable due to environmental issues such as power, and when a cloud service provider using a mobile network stores data, it can show an unintended stop due to attacks or accidents.

3.2. Data Attack

Data attacks are the basis for attacks such as vehicle malfunction and control exploitation, if communications messages or 3rd party products can be detected and analyzed on the vehicle's internal network and maliciously modulated messages can be sent. V2X message analysis, such as communication between vehicles, vehicles, vehicles and infrastructure, and back-and-server communication, also includes analysis of credentials and personal information of the vehicle.

Threats such as remote control service authority acquisition, denial of message transmission and reception, and false data transmission can occur. The falsification or modulation of external communication messages can cause traffic congestion and accidents by allowing the operation of vehicle driving information, billing data, etc. Data modulation typically involves lightweight protocols, near-field communications and data confidentiality, malicious falsification, and security policy degradation in the process of transitioning to high-functioning protocols or long-distance communications (such as Ethernet). Malicious attackers change safety control or HW device's unique value to 'overwrite' attacks, causing fatal risks to the driver's life and health, overwriting vehicle retention data and code through communication channels, unauthorized change to system diagnostic data, charging voltage modulation, etc. In order to delete the data, a malicious attacker could change the unique value of a HW device to a 'overwrite' attack, resulting in a loss of functionality or fatal harm to the driver's safety by exceeding the vehicle's safety limit, unauthorized deletion of the system event log, Smart Traffic Security

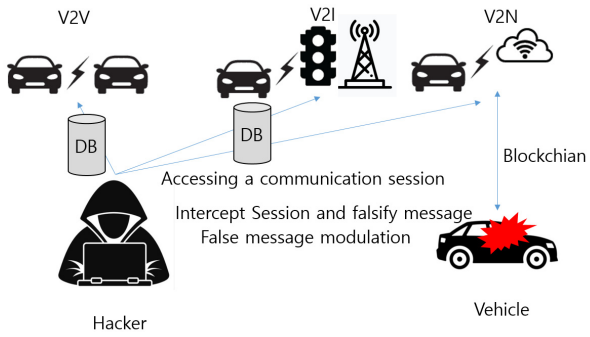

Fig. 3. Data attack. Through V2V, V2I, V2N, etc., the hacker shows how to hack through various channels with session values in the middle of the database server.

Guide and DRM (Digital Rights Management) conflict. And to prevent these illegal elements through blockchain, vehicle retention data and code can be inserted through the communication stream using modulated software binary files and generating illegal data code using communication channels (Fig. 3).

3.3. Man in the Middle Attack

The Man in the Middle Attack uses wireless communication to open and close the doors of the vehicle at close range, air conditioning, remote start-up, etc. When a user uses a smart car, an attacker can detect and replicate wireless communication signals to allow retransmission, enabling the vehicle to be hijacked. Also, if you have direct access to the smart car, it will be mounted on the smart car (Fig. 4).

An immobilizer signal can also be duplicated to bypass anti-theft equipment and steal the vehicle. In addition to the vehicle, if the retransmission of the communication signal (WAVE) using the roadside station is possible, the traffic system may be congested by impersonating another vehicle. In this way, an attacker can steal and acquire sensitive data or launch data tampering attacks that communicate with user-vehicle, vehicle-backend systems, which can cause

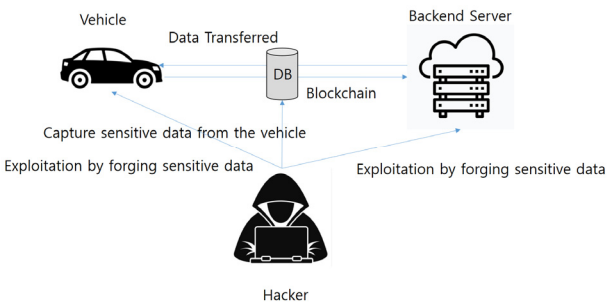

Fig. 4. Man in the middle attack. Hackers show how to hack information on sections transmitted to databases between cars and servers through multiple channels.

secondary damage such as asset infringement and information leakage. Session hijacking also involves attacks that intercept active login status information between smart cars and external servers, or between smart cars and smart cars. Sniffing is called sniping, and a tool to allow such sniping is called sniping. Sniping attacks can occur on the network in various forms, intercepting packets, and then acquiring key information via decoding. A replay attack can be a reuse attack on a smart car or back-and-server communication gateway, allowing an attacker to downgrade the software of the smart car's internal ECU or the firmware of the gateway or disrupt the service of the back-and-server communication gateway. In addition, there are many acts of intercepting data transmitted and attacking back-end servers or smart cars through forged information, which can be defended using blockchain.

3.4. Improper Password Use

Recently, vehicles can receive various types of services through third party operators while using mobile networks. It is possible to use a variety of services via V2X, and when communicating with the vehicle, important information must be encrypted and communicated. Inappropriate encryption algorithms and methods could allow an attacker to easily gain information by accessing a vehicle or back-end system and harm information related to user safety via secondary attacks using key encryption key information and access data information.Expose the encryption key. Expose encryption keys used to encrypt sensitive information due to key-related information leakage due to exposure to encryption keys in smart cars and inadequate management of encryption keys. Furthermore, for the use of vulnerable encryption, a combination of short encryption keys and long expiration periods allows an attacker to extract sensitive information by unencrypting and defend vulnerabilities using low-frequency encryption (weak or soon-to-use encryption) algorithms with blockchain (Fig. 5).

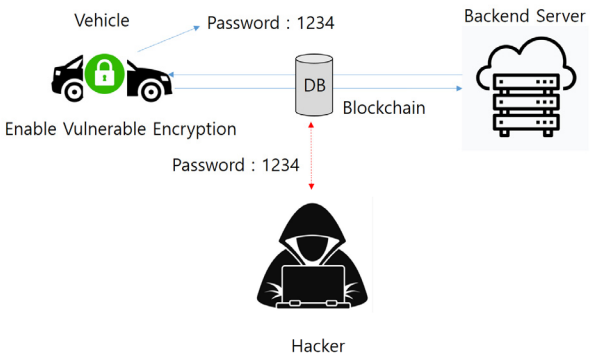

Fig. 5. Improper password use. Hackers show how to hack information on sections sent to the database between the password of the car and the server through multiple channels.

3.5. Use Inappropriate Access Control

Incomplete or illegal service may be provided if personnel with access to vehicle components and back-and-server etc. have malicious intent or poor service equipment proficiency for maintenance of vehicles or transportation services. Vehicle and transportation services may experience functional failures, major information for vehicle services such as firmware and credentials may be leaked, and compromised security management policies for back-end servers in the cloud may be compromised. In the event of an infringement accident such as hacking, personal information leakage, manipulated firmware dissemination, and additional exploitable acts can occur, which can cause a failure of the entire smart transportation system. In addition to this, accidents such as data loss and service failure can occur when managing poor back-end servers such as aging IT(Information Technology) services and lack of professional staff needed for management. Server is unauthorized by backdoor or non-patched system software vulnerabilities, SQL (Structured Query Language) attacks, or other means for logical (network) unauthorized access to the server. Unauthorized physical access to the server by USB (Universal Serial Bus) sticks or other media connected to the server for non-authorised access to sensitive information is also accessed by unauthorized back-end servers with inappropriate security policies. Smart car gateways infected with malicious codes for vehicle system modulation could be abused as zombie cars for DDoS (Distributed Denial of Service attack) attacks or degenerated into user information leakage channels. It can also cause secondary damage by infecting other devices connected to smart car gateways. In addition, blockchain allows malicious attackers to change the unique value of the HW device or safety control to 'overwrite' attacks to demonstrate attacks that result in loss of functionality or fatal harm to the driver's safety beyond the vehicle's safety limits (Fig. 6).

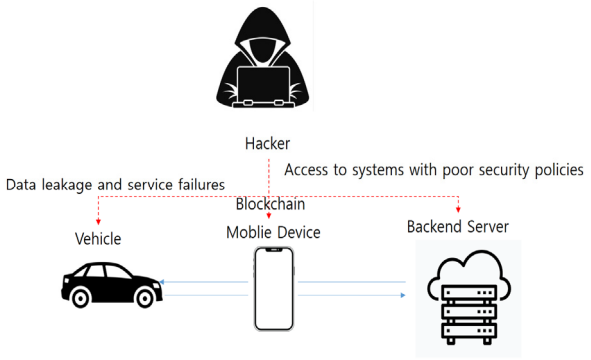

Fig. 6. Use inappropriate access control. Hackers show how to hack through various routes transmitted from cars and mobile devices.

IV. CONCLUSION

This paper studied how to respond to the security items of smart transportation. Smart transportation systems serve vehicles and users through a variety of software. With security in mind, software design, management, and distribution are followed by systematic follow-up management to safely implement the software. Software security should be implemented safely by considering the step-by-step security of the SW Development Lifecycle (SDLC) to minimize security vulnerabilities in the development of in-vehicle firmware and software. And since the more complex the software functions, the more likely the bug is to occur, unnecessary services should be disabled. In addition, audit records generation functions should be implemented using blockchain for security audits, and abnormalities in smart transportation systems should be detected and tracked. And because smart transportation systems store sensitive information, such as personal information, various threats can occur when accessed by unauthorized users. Therefore, safe services should be provided through authentication and access control when accessing smart transportation systems. In addition, it can manipulate smart transportation systems and cause malfunction of vehicles and backend servers through falsification, modulation, and analysis when storing and transmitting important information. Accordingly, important information should be encrypted. In addition, various messages such as CAN messages, PVDs and BSM messages are sent and received inside the vehicle to provide various services using blockchain, and various data such as vehicle information, vehicle location information, and user personal information are included. In addition, safe management of sensitive information is also required in OEM servers and cloud servers that handle user location and user personal information of smart transportation. I would like to learn and study the basic model of transportation for these smart cars. Furthermore, issues on artificial intelligence, big data and security are expected to emerge constantly and apply to many parts of various industrial groups. More than 100 ECUs, complex software, and numerous internal/external connectivity cars are exposed to a variety of security threats. Although various types of security solutions are currently being studied and applied to self-driving cars, there are still technical limitations, with cases of security attacks reported until recently. In this paper, we looked at the recent trends, security threats, and current security technologies of self-driving cars, and looked at analysis technology, vehicle Ethernet security, and V2X security acceleration technology as current security issues. In addition to the issues examined in this paper, there are various security issues such as privacy protection of automobiles /individuals, physical attacks on autonomous sensors, cause analysis of autonomous accidents/malfunctions, and preservation of evidence through forensics, and related R&D is taking place in various forms at research institutes, companies, schools. Self-driving services are technologies that are completed by converging and combining various industries such as automobiles, roads, transportation, and ICT infrastructure, and security technologies are also expected to need to be designed and applied in the form of taking into account various industrial infrastructures.

In order to cope with the rapidly evolving threats in self-driving cars, the need to protect AI systems is increasing, and in particular, it is necessary to integrate existing cybersecurity principles with new AI cybersecurity. As self-driving cars' dependence on AI increases, attacks targeting AI algorithms increase, and serious damage is expected. In order to effectively cope with these attacks, a comprehensive approach that considers the diversity and interaction of AI systems, an integrated security system that considers all stages of AI systems, and in-depth defense strategies are needed. Even if the vehicle system is designed and developed in consideration of security, equipment is added over time, software and major function changes occur, requiring an integrated security approach throughout the life cycle, prevention of AI system modulation, and confidentiality and integrity guarantees. In addition, despite the widespread awareness of security vulnerabilities in many organizations, security awareness and response efforts to vulnerabilities in AI systems in particular are quite insufficient. Lack of sufficient knowledge of AI security risks or widespread awareness of underestimating risks can amplify AI security risks. In order to improve false perceptions of cybersecurity situations, education to raise awareness is essential. Cybersecurity high processing and response plans related to AI-based digital components should be considered in autonomous vehicles. The growing number of actors who lack experience in security incidents in the automobile sector raises the need to establish a cybersecurity culture that can understand the potential vulnerabilities of the system and the fundamental threats inherent in the system. All stakeholders involved in the self-driving car supply chain need to recognize an increasing AI threat environment to link risks and attacks to business operations, and promote security program development across the entire supply chain by spreading lessons learned from AI security incidents.

REFERENCES

[1] L. Andrei, D. L. Baldean, and A.-I. Borzan, "Designing an artificial intelligence control program model to be tested and implemented in virtual reality for automated

chevrolet camaro", *Multidiscplinary Digital Publishing Institue Proceedings,* vol, 63, no. 1, p. 44, 2020.

[2] F. Delli Priscoli, A. Giuseppi, and F. Lisi, "Automatic transportation mode recognition on smartphone data based on deep neural networks", *Sensors*, vol. 20, no. 24, 2020.

[3] N Kshetri, "Blockchain's roles in meeting key supply chain management objectives," *International Journal of Information Management*, vol. 39, pp. 80-82, 2018.

[4] A. Savelyev, "Copyright in the blockchain era: Promises and challenges," *Computer Law & Security Review, Elsevier*, vol. 34, no. 3, pp. 550-561, 2018.

[5] PLC network base technology for smart grid system, The *Journal of Supercomputing*, vol. 72, no. 5, pp 1862-1877, 2016.

[6] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 20-23, 2017.

[7] S. K. Kim, U. M. Kim, and J.-H. Huh, "A study on improvement of blockchain application to overcome vulnerability of IoT multiplatform security," *Energies*, vol. 12, no. 3, pp. 1-29, 2019.

[8] J. H. Huh and K. R. Seo, "A typeface searching technique using evaluation functions for shapes and positions of alphabets used in ancient books for image searching," *International Journal of Hybrid Information Technology*, vol. 9, no. 9, pp. 283-292, 2016.

[9] R. B. Levin, P. Waltz, and H. LaCount, "Betting blockchain will change everything - SEC and CFTC regulation of blockchain technology, handbook of blockchain," *Digital Finance, and Inclusion, Elsevier*, vol. 2, pp. 187-212, 2017.

[10] J. H. Huh, "Server operation and virtualization to save energy and cost in future sustainable computing," *Sustainability*, vol. 10, no. 6, pp. 1-20, 2018.

[11] C. Prybila, S. Schulte, C. Hochreiner, and I. Webe, "Runtime_verification for business processes utilizing the bitcoin blockchain," *Future Generation Computer Systems,* Elsevier, vol. 107, pp. 816-831, 2017.

[12] S. K. Kim and J. H. Huh, "A study on the improvement of smart grid security performance and blockchain smart grid perspective," *Energies*, vol. 11, no. 7, pp. 1-22, 2018.

[13] Y. Chen, "Blockchain tokens and the potential democratization of entrepreneurship and innovation," *Business Horizons*, vol. 61, no, 4. pp. 12-13, 2017.

[14] J. H. Huh, S. Otgonchimeg, and K. R. Seo, "Advanced metering infrastructure design and test bed experiment using intelligent agents: Focusing on the PLC network base technology for smart grid system", *The Journal of Supercomputing*, vol. 72, no. 5, pp. 1862-1877, 2016.

[15] Z. Wang, J. L. Peterson, C. Rea, and D. Humphreys "Special issue on machine learning, data science, and artificial intelligence in plasma research", *IEEE Transactions on Plasma Science*, vol. 48, no. 1, pp. 1-2, 2020.

[16] Y. Wang, S. Kwong, H. Leung, J. Lu, M. H. Smith, and L. Trajkovic, "Brain-inspired systems: A transdisciplinary exploration on cognitive cybernetics, humanity, and systems science toward autonomous artificial intelligence", *IEEE Systems, Man, and Cybernetics Magazine*, vol. 6, no. 1, pp. 6-13, 2020.

[17] T. Watkins, "Cosmology of artificial intelligence project: libraries, makerspaces, community and AI literacy", *ACM AI Matters*, vol. 4, no. 5, pp. 134-140, 2019.

[18] Y. S. Seo and J. H. Huh, "Automatic emotion-based music classification for supporting intelligent IoT applications," *Electronics,* vol. 8, no. 2, pp. 1-20, 2019.

[19] E. Šabanovič, V. Žuraulis, O. Prentkovskis, and V. Skrickij, "Identification of road-surface type using deep neural networks for friction coefficient estimation", *Sensors*, vol. 20, no. 3, p. 612, 2020.

[20] I. S. Andrades, J. J. Castillo Aguilar, J. M. V. García, J. A. C. Carrillo, and M. S. Lozano, "Low-cost road-surface classification system based on self-organizing maps", *Sensors*, vol. 20, no. 21, p. 6009, 2020.

[21] B. Varona, A. Monteserin, and A. Teyseyre, "A deep learning approach to automatic road surface monitoring and pothole detection", *Personal and Ubiquitous Computing*, vol. 24, no. 4, pp. 519-534, 2020.

AUTHORS

Seong-Kyu Kim was born in Seoul, Republic of Korea. In Feb. 2006, he gradu ated from Sungkyunkwan University at Seoul, Department of Information Communication Engineering in Korea and received his master degree. In Aug, 2019, He graduated (Ph.D) from Sungkyunkwan University at Suwon, Department of Electronic and Electrical Computer Engineering. He started his career as a ICT in 1999, and he was before worked Hyundai Information Technology.

He has worked on Hyundai Motor IT R & D Research, Hyundai Construction IT R & D Research, Korea Railroad IT Project, Korea Highway Corporation IT Project, and Ministry of Public Administration and Security IT Project.

He worked at Samsung during 1999 ~ 2017. He was responsible for Saudi Aramco security (physical and information protection) projects, Kuwait KNPC security (physical and information protection) projects, and Singapore Changi Airport security (physical and information protection) projects.

He also lectured on "Introduction to Public Computers" at Songdam University, Yongin. (2010 ~ 2011). Lectured "Security System" at Sungkyunkwan University Graduate School of Information and Communication (2015).

CISA, PMP, CISSP, and CPPG lectures were conducted at Wise Road, an accredited Ministry of Employment and Labor (2010-2016). Computer Engineering Lecture at the Hackers Lab, an accredited Ministry of Employment and Labor (2016). Lectured on industrial security management at "Edu" educational institution certified by Ministry of Employment and Labor (2010 ~ 2016). In addition, he received the Best Paper Award at the Korea Multimedia Society (MITA) in 2019.

He has international certifications such as CISA(Certified Information Systems Auditor), CISSP(Certified Information Systems Security Professional), PMP(Project Management Professiona), ITIL Foundation, CCNP, SCJP, ISE, CPPG, ISO 27001, ISO 19011, ISO 20000, ISO 9000, ISO 22301 has etc.

Currently he is Assistant Professor (Tenure Track) of Department of Information Security, Joongbu University, Gyeonggi-do, Republic of Korea" His research interests are Blockchain, AI, Big Data, Smart Grid, Network Security, IoT, App, System Architecture.

Eun-Sill Jang was born in Seoul, Republic of Korea. In Aug. 2001, she received her master's degree in Computer Education Major, Department of Curriculum Education from Dongguk University. In Aug, 2007, she graduated Ph.D. in Department of Computer Engineering from Dongguk University.

She worked as a full-time researcher at Dongguk University's Institute of Industrial Technology from 2008 to 2011. She served as the Director of Development Support Team in Myungli from 2016 to 2018.

She served as a visiting professor in the Department of Software at Sungkyunkwan University from 2018 to 2020, and she served as a professor in charge of software education at Hanyang University from 2020 to 2021.

Currently, she is an assistant professor in the Department of Student Growth and Liberal Arts at Joongbu University. Her research interests are SW education, SW convergence education, computing-based problem solving, data analysis education, AI education, AI ethics, etc.