symmetry

MDPI

Article

Autonomous Vehicles: The Cybersecurity Vulnerabilities and Countermeasures for Big Data Communication

Abdullah Algarni * and Vijey Thayananthan

Computer Science Department, King Abdulaziz University, Jeddah 21589, Saudi Arabia
* Correspondence: amsalgarni@kau.edu.sa; Tel.: +966-12-6952000

Abstract: The possible applications of communication based on big data have steadily increased in several industries, such as the autonomous vehicle industry, with a corresponding increase in security challenges, including cybersecurity vulnerabilities (CVs). The cybersecurity-related symmetry of big data communication systems used in autonomous vehicles may raise more vulnerabilities in the data communication process between these vehicles and IoT devices. The data involved in the CVs may be encrypted using an asymmetric and symmetric algorithm. Autonomous vehicles with proactive cybersecurity solutions, power-based cyberattacks, and dynamic countermeasures are the modern issues/developments with emerging technology and evolving attacks. Research on big data has been primarily focused on mitigating CVs and minimizing big data breaches using appropriate countermeasures known as security solutions. In the future, CVs in data communication between autonomous vehicles (DCAV), the weaknesses of autonomous vehicular networks (AVN), and cyber threats to network functions form the primary security issues in big data communication, AVN, and DCAV. Therefore, efficient countermeasure models and security algorithms are required to minimize CVs and data breaches. As a technique, policies and rules of CVs with proxy and demilitarized zone (DMZ) servers were combined to enhance the efficiency of the countermeasure. In this study, we propose an information security approach that depends on the increasing energy levels of attacks and CVs by identifying the energy levels of each attack. To show the results of the performance of our proposed countermeasure, CV and energy consumption are compared with different attacks. Thus, the countermeasures can secure big data communication and DCAV using security algorithms related to cybersecurity and effectively prevent CVs and big data breaches during data communication.

Keywords: cybersecurity vulnerabilities; autonomous vehicles; vehicular communications; security solutions

Citation: Algarni, A.; Thayananthan, V. Autonomous Vehicles: The Cybersecurity Vulnerabilities and Countermeasures for Big Data Communication. *Symmetry* **2022**, *14*, 2494. https://doi.org/10.3390/sym14122494

Academic Editors: Sergei D. Odintsov, Alexander Zaslavski and Adam Glowacz

Received: 19 September 2022
Accepted: 20 November 2022
Published: 24 November 2022

1. Introduction

All future systems will have automated features that allow users, including researchers, to study several automation functions before they operate autonomous systems, such as autonomous vehicles (AVs). All features of AVs, such as functions and connections, safety warnings, and privacy issues, are expected to be secured prior to operation. However, cybersecurity vulnerabilities (CVs) affect these features leading to improper functioning or failed connections. Cyberattacks; threats; and physical failures of unreliable components, systems, and communication services that depend on energy efficiency (EE) further compromise the integrity of AVs. Due to the symmetry between IoT device vulnerabilities and data communication, cybersecurity is becoming an increasingly significant factor in autonomous vehicles and related data communication systems.

Researchers have attempted to design countermeasures for malware infections and cyberattacks, that exploit CVs in data communication between autonomous vehicles (DCAV) and autonomous vehicular networks (AVN) by determining the origin of attacks and analyzing CVs. To detect infections and cyberattacks, the possible threats to the AVN and DCAV need to be predicted. In addition, the energy variations of the predicted attacks must

be observed accurately to improve the efficiency of countermeasures. Basing the countermeasures on energy variations is necessary because unreliable and inefficient technologies increase the energy of cyberattacks and infection in DCAV. However, highly specialized knowledge is required when using conventional detection technologies. Moreover, new types of CVs exhibit extremely short cycles. Therefore, attack trends must be identified and investigated to develop new technologies.

Society will be extremely safe if its use of autonomous vehicles is protected against cybersecurity vulnerabilities. Threats to the cybersecurity of a fleet of autonomous vehicles are conceivable; stealing a fleet of autonomous vehicles could represent a new type of car theft [1]. Such vehicles could be compromised by a lack of security measures [2], e.g., an autonomous vehicle operating system might be compromised, exposing private data on other linked devices. The hacked automobiles can then be diverted to a location where a robbery or assault is intended to take place. In addition, IoT gadgets in homes could be controlled by connected cars, providing hackers access to people's personal computer networks.

In the future, autonomous systems should be able to proactively detect CVs. The strong countermeasures proposed in this study aim to develop attack-free autonomous systems and minimize global warming and carbon footprints. However, the appropriate countermeasures will maximize energy consumption because strong security systems use highly complex designs and algorithms. Therefore, researchers are attempting to improve the security of AVs using simple countermeasures.

1.1. Objectives

The main objective is to propose an efficient countermeasure for securing network data traffic of AVN and big data communication influenced by AVs. In this theoretical research, we aim to measure the energy variation when CVs change due to the cyberattacks created by sudden power attacks and the faulty components used in the AVs. In big data communication, the signal's power is suddenly increased to a peak stage by many factors, including environmental conditions. In this research, we have focused on the following objectives: (1) Propose a model for securing autonomous vehicular networks and data communication, including big data between the AVs, (2) Develop an efficient countermeasure with a strong security algorithm and energy-efficient protocols, (3) Present an analytical approach of energy measurements to validate the model which includes the countermeasure with different attacks and information security, and (4) Verify the efficiency of countermeasure with the vulnerable AVN where different data sizes and densities of data are used.

1.2. Motivation

Autonomous vehicles and their features will depend on the big data traffic when users increase and interact with other mobile devices. The volume of the big data traffic and security issues of vehicular networks motivate us to detect the power attacks which travel through the power cable and increase the heat and damage or explode the electronic elements suddenly. This situation blocks the operational functions of the AVs and disconnects network links that provide autonomous commands. To improve the security solutions, vulnerabilities of the physical components of the AVs must be monitored using efficient countermeasures, which include cybersecurity techniques. The cybersecurity vulnerabilities and countermeasures for big data communication will be an interesting problem in future research and innovation.

1.3. Contributions

The following are the main contributions of this study in terms of countermeasures for CVs in AVs.

1. We propose a model in which we focus on the future security problems of DCAV and the CVs affecting the network functions of AVN.
2. We develop an efficient countermeasure. To develop this, we present a taxonomy of various cyber threat models and countermeasures considered for DCAV. We propose an efficient theoretical model of the best countermeasures that mitigate the highlighted cybersecurity problems.
3. We present an analytical approach with an information security solution that enhances the security of the model depending on the efficiency of countermeasures, security of the DCAV, big data infrastructure, and effectiveness of cybersecurity in AVN.
4. We verify the efficiency of countermeasures in which we measure the EE and CV with different data sizes, existing adversarial cyberattacks, and CVs, emphasizing their relevance for DCAV and AVN.
5. Finally, we have added a few open challenges related to the security solutions of AVN and DCAV.

This paper presents a scheme for managing traffic and is organized as follows: We present a review of the related literature and works in Section 2. In Section 3, we describe the proposed model of countermeasures for big data communication. This model provides the details of the CVs, analysis, and detection, which are part of the countermeasure. In Section 4, we compare the different cyberattacks that create weak links and communication between AVs. The results that verify the proposed countermeasures are presented in this section. Section 5 discusses the security issues involved in AVs, countermeasures for big-data communication, and energy levels. In Section 6, we discuss the challenges of CVs and countermeasures for big data communication features. In addition, it includes the latest solutions to cybersecurity issues with minimal energy consumption. Section 7 presents our conclusions and proposes future research directions to develop AVs with human-like intelligence.

2. Literature Review

This section provides the basic information related to the attacks, vulnerabilities of AVN, and cybersecurity used in the countermeasures. The CVs and countermeasures for big data communication between roadside service units (RSU) and AVs have been the primary focus of research in this field. For instance, an intelligent defense method was proposed based on the proportional overlapping scores scheme that used back propagation neural networks to detect a particular type of attack that frequently occurs called denial of service (DoS). The proposed method safeguards external communications for autonomous and semi-AVs independent of external equipment such as radar, lidar, computer vision, or RSUs [3].

To secure the message transfer between wirelessly connected vehicles, a fast and selective authentication of VANETs using digital signatures was analyzed [4]. In addition, the study demonstrated that context-adaptive beacon verification (CABV) with a particle filter could detect and prevent spoofed attacks while reducing computational overhead.

The authors of [5] proposed the Internet of Autonomous Vehicles (IoAV) architecture. They illustrated its layered architecture that included key features such as safe navigation and efficient traffic management in addition to bringing people to their destinations. The performance of IoAV was evaluated based on the transmission time and energy consumption.

2.1. Vulnerabilities Involved in the AVN and DCAV

Autonomous systems and AVs will face many attacks and threats coming from different signals and directions. In the AVN and DCAV, the vulnerabilities are also formed by impacts of faulty components, environmental conditions, and bad signals influenced

by internal and external interferences, which include heat. Power attacks being changed during autonomous operations are suddenly reaching the peak stage (maximum temperature). These power attacks should be detected before they reach some sensible electronic components used in the AVs. For instance, the electronic control module of the AVs sends the control and communication signals, including the power, to the pedals, the gear, or the steering wheel. When these signals are abnormal, components become vulnerable or vice versa.

In another study, cybersecurity vulnerabilities of AVs were studied and classified in terms of their susceptibility to threats and attacks [6]. To improve autonomous vehicle systems, the authors proposed guidelines and mitigation strategies.

Researchers also reviewed several studies based on cyber security vulnerability types that were mostly discovered by white-hat hackers and mitigation techniques in AVs [7]. Based on this review, they identified some knowledge limitations that could assist in investigating cyber security challenges.

Key automotive cyber-attacks, their impact, and corresponding solutions that utilize artificial intelligence (AI)-based deep learning models have also been discussed in depth. One study proposed a roadmap to establish efficient intrusion detection systems for secure AVs and address major challenges [8]. In addition, the vulnerability of AV systems to cyberattacks was examined [9]. The authors investigated attack mechanisms on AVs to raise awareness about cybersecurity threats. In another study, the security vulnerabilities of AVs, cyberattack detection, and mitigation strategies were described [10]. Some emerging technologies, such as AI and blockchain, have been used as security solutions against threats to the transportation infrastructure. An in-depth survey and analysis of the historical evolution, recent research directions, and cybersecurity (threats, vulnerabilities, and attack modeling) of autonomous systems were conducted [11].

The authors in [12] proposed an evaluated framework of cyber-attacks on AVs based on current security attack techniques and their computer vision and networking solutions. In addition, they experimented with physical attacks, such as traffic sign attacks and a variety of network-based attacks, to examine the robustness of AVs against cyber-attack vulnerabilities.

The results of [13] indicate that autonomous vehicle vulnerabilities may jeopardize autonomous services. Accordingly, researchers identified the different types of autonomous vehicle attacks and the corresponding countermeasures. Autonomous control systems, autonomous driving system components, and vehicle-to-everything communications are the three types of attacks suggested by the authors. In [14], the authors provide a comprehensive survey on cyber security and up-to-date countermeasure strategies for securing AVs and their services. In addition, it includes the standards for connected and autonomous vehicles (CAVs) and lists the open challenges that require solutions. Another study established that sensors, operating systems, control systems, and vehicle-to-everything communication are the four dimensions of autonomous driving security [15]. Attack models and countermeasures given in [16] for AVs describe the attacks on electronic control units (ECU), sensors, intra-vehicular links, and inter-vehicular links. In [17], a general overview of security vulnerabilities and countermeasures for data communication was provided for different applications, including AVs. The authors of [18] focused on cybersecurity for robotics and security solutions with multi-factor cryptographic algorithms that enable more secure autonomous systems. In [19], multi-access edge computing (MEC) revealed the security vulnerabilities of 5G-based use cases. MEC supports AVs by improving their quality of services and efficiency in automated driving, augmented reality, and machine-type communication. Another study [20] provided specific details of autonomous systems t to facilitate the development of future autonomous mobility services. CAVs are vehicles equipped with various Internet of Things (IoT) sensors to obtain security and safety information from their surrounding environment. In [21], the authors presented a new model for developing autonomous services. They studied and identified hedonic motivation, trust in AVs, and social influence security issues as significant factors in performance expectation, among other things. Hedonic motivation is a technique used to boost travelers' trust in automated

vehicles. The authors of [22] established a security policy pathway to achieve sustained use of AVs in the future. Policy packages aimed at the superblock vision comprise six themes that detail the processes required to improve the overall transportation regulations described in the vision for 2050. Another study [23] focused on the combination of intelligent transportation systems (ITS) and the integration of AV with maximum security and safety. Transportation systems in the future will depend on this combination and complex engineering systems and will consequently be dynamic and subject to constant transformation and security improvements. By 2030, cybersecurity technology related to selected security issues (CVs and countermeasures for data communication) for autonomous transportation services is expected to overcome several challenges using four modes of countermeasures: AI-supplemented, AI-generated, AI-mediated, and AI-facilitated. The next generation of AVs, CVs, and countermeasures for data communication will be dominated by AI. Thus, the design of autonomous transportation services will have to adhere to stricter standards [24–28].

Some other recent studies have focused on 5G and 6G mobile communication, but they used different techniques, such as heterogeneous networks and mobile ad hoc networks. For instance, Gupta, A. and Gupta, S. K. [29] conducted a thorough technical study to better understand fog computing and its related issues in terms of security, privacy, and risks. After outlining the security risks that the cloud infrastructure has encountered, they proposed control over UAV data based on the architecture of unmanned aerial vehicles (UAVs)-fog, which consists of a four-tier network of smart things, local UAVs, UAV-fog, and cloud servers. By incorporating a functional encryption technique, Sharma et al. [30] suggested a UAV-assisted heterogeneous network model for dense metropolitan regions that provides resistance against intrusion attempts. In Kumar et al. [31], sensitive data and systems at both ends were subject to a thorough study of security measures using a multimodal-based learning framework. They provided examples of frameworks and techniques that may be used in diverse applications to guarantee that multimodal algorithms protect people's privacy and the security of their data.

2.2. Countermeasures for Securing Communication and AVN

All features used in the AVs depend on network traffic involved with big data consisting of petabits to Zetta bits. Many users had cyberattacks using these features through mobile devices, including the recommended mobile applications. These cyberattacks spread throughout mobile applications and systems via big data communication. To prevent the users' data, applications, etc., big data communication and AVN should be secured quickly, proactively, and dynamically. Thus, employing strong security algorithms, autonomous firewalls, and efficient cybersecurity solutions is important. Although existing countermeasures provide the necessary detection and protection to check and identify the vulnerabilities in many systems, they are not that efficient for AVs and AVN because employing security in big data communication is critical.

Managing CVs also requires awareness of phishing attack techniques and countermeasures [32] in the case of autonomous vehicular communications. However, the technique of cyberattack detection and countermeasures for distributed electric springs are available, which can be applied for smart grid applications [33] that support communication related to power distributions in autonomous transport systems. Attack models and countermeasures [34] are the primary focus of proactive systems that prevent data integrity attacks using dynamic state estimation of smart grids. Attack models are evolving continually owing to the development of numerous services and applications where countermeasures are expected to face evolved attacks proactively. Moreover, attacks and countermeasures in IoT-based smart healthcare applications consume a considerable amount of energy and valuable time, which are major problems for vehicular networks integrated with medical communication [35]. Furthermore, recent advances in the Internet of Things (IoT) and machine learning (ML) have facilitated the integration of transportation services involving medical communications, which has led to further vulnerabilities in the systems.

The protocol of the system architecture, illustrated in Figure 1, comprises four main stages: perception, decision and planning, control, and chassis [36]. In this architecture, data fusion enables the sensor and recognition modules to dynamically make accurate decisions and plans once the security features and solutions are enhanced in the full AVs. Accordingly, the design of these modules, interfaces, and functionalities should enable the integration of security algorithms and main sensors to protect the system from cyber-attacks and CVs.

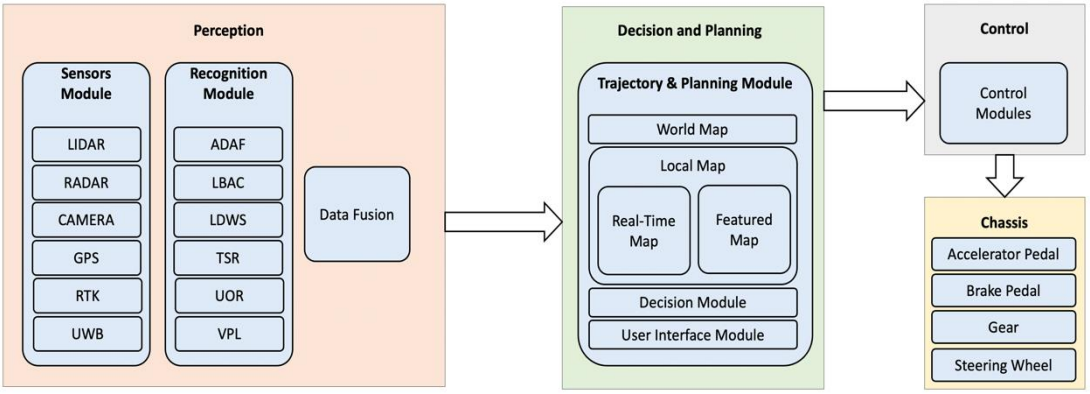

Figure 1. System Architecture for AVs [31].

Figure 1 illustrates the links of all available modules considered for future Avs as detailed in [36]. However, countermeasures for big data communication require many detection points for a fixed frame of data traffic. Thus, the use of numerous detection points in these modules leads to increased overall complexity. Nevertheless, security must be prioritized in the operation of AVs. Therefore, proactive solutions are required to ensure the security of big data communication between the sensors used in AVs that predict and detect threats.

According to Figure 1, the decision module can support autonomous vehicles from the sensors given in the perception. It means that it can make the decision according to the security issues provided by the sensors. The interface module provides the necessary connections between perception and control. Based on the decision, the electronic system of the AVs in the control module creates the control signal for the functioning of the components in the chassis. In one of the conferences, the presenter demonstrated that a control signal embedded with a power attack damaged the component. We need an efficient countermeasure that includes cybersecurity solutions to avoid this situation and improve security.

Table 1 shows the CVs and the corresponding countermeasures that ensure the safety of AVs when their components are subjected to technical errors, purposed attacks, and careless operation.

CVs generally affect the data traffic of vehicular communication networks, and countermeasures for big data communication depend on the data sources used in transportation services. Autonomous services face several types of attacks, such as jamming. However, big data analytics for anti-jamming applications in AVN enable researchers to secure autonomous services in vehicular ad-hoc networks [37].

Improving big data clustering for jamming detection in smart mobility [38] and automobile systems can also be considered while developing countermeasures. Most jamming attacks damage the physical components of autonomous systems, such as AVs.

Countermeasures for cyber immune and attack detection systems, as shown in Figure 2, generally require biometric information, considered big data in AVN and DCAV. Here, big data management typically handles cyber-attacks and gathers reliable data with necessary management procedures related to cybersecurity policies. Attack detection systems using authorized cybersecurity algorithms, in addition to detection techniques and protocols,

detect the CVs present in AVN and DCAV. As shown in Figure 2, AV agents collect the details of encrypted and decrypted data obtained from the cyber-and-attack detection (CAD) system. In this example [39], AV agent management supports the CAD and collects big data from the AV agents.

Table 1. Available countermeasures of cybersecurity vulnerabilities for Component of AV.

Component of AV	Cybersecurity Vulnerabilities	Countermeasures
On-board diagnostics (OBD) II port	In-Vehicle Network Access Attack (malicious behavior of DCAV)	Data management system, a method of attestation with encryption
USB Port which connects the phones within the Avs	Cyber incidents are caused by the virus or malware of USB devices during the vehicular communication	Prevent propagation from a non-critical area to a safety-critical area. Issuing USB devices with certification
Remote Keyless Entry System	Eavesdropping attacks are possible with rolling codes	An efficient receiver is designed with less susceptible to attacks
The keypad is located at or near the driver's door	Repeated use of obsolete devices and techniques, weak cryptographic systems, and implementation flaws	Keyless entry methods. For authenticating devices, digital certificates are used in conjunction with a clustering strategy

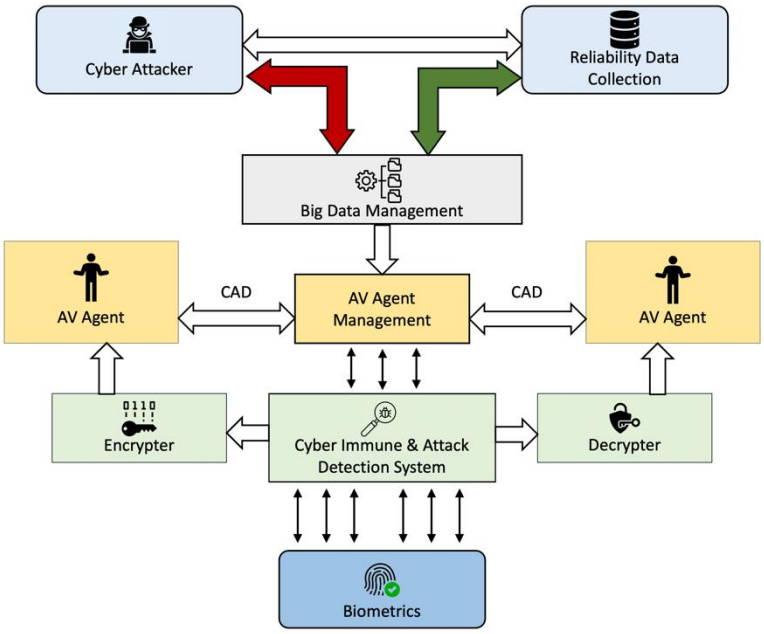

Figure 2. The example system model for big data communication is involved in AVs [34].

3. Proposed Research

In this section, we propose an efficient theoretical model that monitors the CVs associated with big data, mitigates the possibility of breaches, and detects abnormal behavior in the big data communication process and data traffic in DCAV and AVN. Moreover, the proposed model leverages the fact that security solutions based on energy variation enable us to determine CVs.

Future threats with evolving security issues in data communication applications and emerging technologies, such as DCAV and AVN, damage future data communication.

3.1. Research Objectives

The primary objectives of this study are the following:

- Determining potential and future threats with evolving security issues in data communication applications and emerging technologies, such as the vulnerabilities of DCAV

and AVN that damage potential data communication, and countermeasures with energy-efficient security algorithms and technologies that can secure DCAV and AVN.

- Building an efficient model for securing big data and its communication network that eliminates CVs and enables researchers and scientists to update the security in DCAV and AVN.
- Developing cybersecurity countermeasures using security algorithms, intelligent techniques, and emerging technologies that increase the level of security and reduce the energy consumption and cost of DCAV.
- Applying an adynamic cybersecurity solution for data traffic management to improve the security of DCAV and AVN.

3.2. Research Design

Several combinations of selected protocols and energy-efficient algorithms were considered, from which we developed the security design proposed in this study. In this study, existing models were considered as example methods for designing secure DCAV and AVN. In the proposed approach, an energy-efficient security algorithm is deployed to improve the level of countermeasures. In Figure 3, the block diagram of the proposed approach is represented. In future work, we hope to use IoT sensors suitable for improving DCAV because the resultant model will be more secure and economical. Energy-efficient security algorithms and protocols for developing cybersecurity solutions can be developed according to the types of communication and network technologies. Here, security management is required to minimize the overall security costs. Therefore, our research team focused on developing the necessary security policies based on expert knowledge of specific cybersecurity fields such as information security and network security. Furthermore, solutions for cybersecurity issues will depend on efficient designs, architectures, and implementations. Therefore, cybersecurity technology with reliable infrastructure is required to improve the reliability of the DCAV and AVN. Accordingly, we developed an efficient theoretical model to implement appropriate countermeasures in AVs. The model includes energy-efficient security solutions based on the appropriate cybersecurity knowledge and skills (gathered from studies [14–18]) and detection components (from studies [24–28]) with the necessary protocols and algorithms. All the designs in this proposal can be developed using the aforementioned methodology.

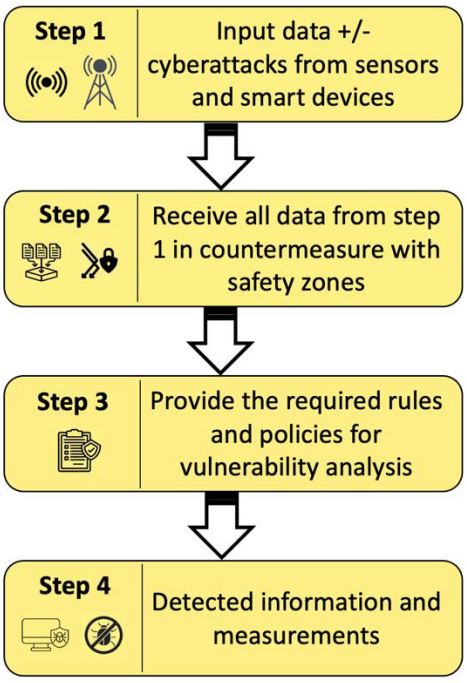

Figure 3. A block diagram of the proposed approach.

3.3. Proposed Model

Figure 4 shows the details of big data and its communication network that provide automated security facilities to AVs. Each layer of this model represents the details of the security systems, tools, and other necessary components in AVs. Black arrows represent the steps of detection for supporting the countermeasure, which monitors the internal cases of CV measurement. Large double-sided arrows show the attacks could have appeared in any of these two directions. Large single-sided arrows represent the steps of detection for supporting the countermeasure, which monitor the external cases of CV measurement. Determining CVs and countermeasures is essential for identifying cyberattacks and mitigating all possible attacks. In the proposed model, countermeasures are expected to be able to detect all prominent attacks (Sybil, DoS, wormhole, jamming, selective forwarding, sinkhole, etc.) that appear in big data communication, DCAV, and AVN.

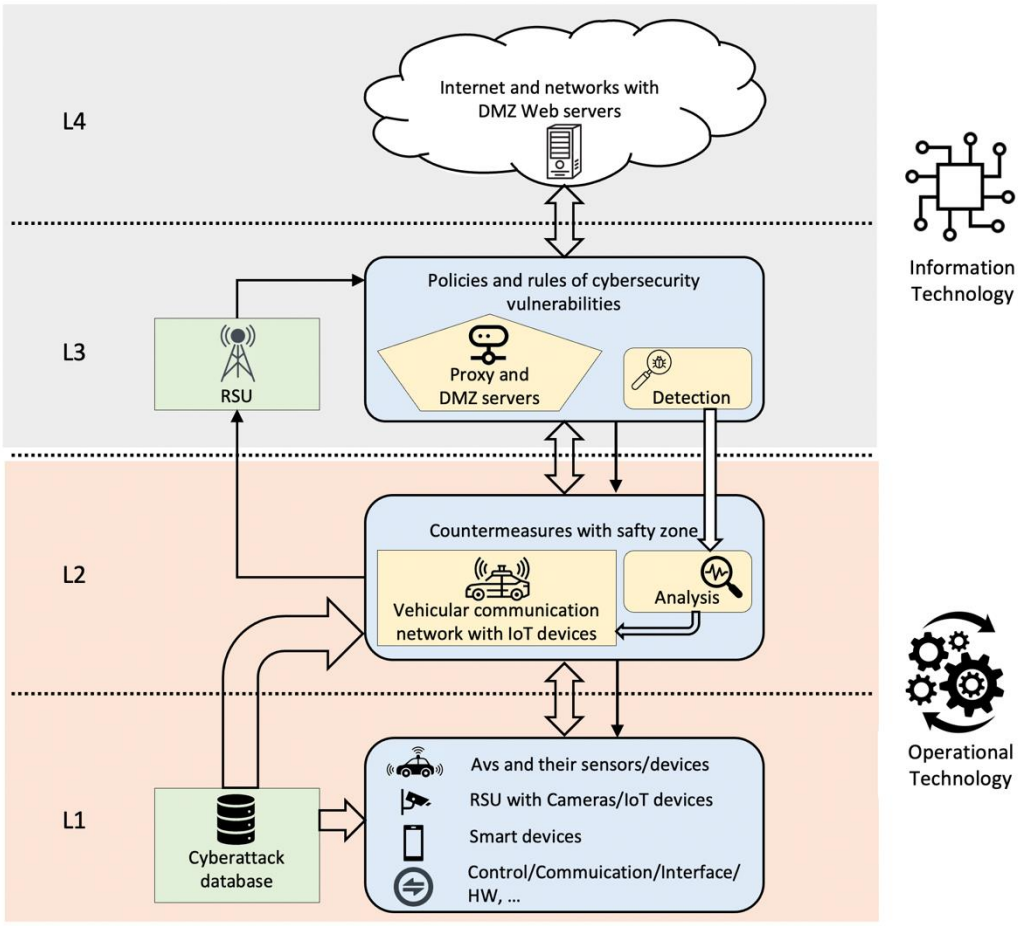

Figure 4. Proposed model for securing autonomous vehicles and big data communication.

Layer (L1) collects all data, including big data considered in DCAV, RSU, and smart devices, to identify cyberattacks. The countermeasure with the safety zone set in layer (L2) receives all data from L1, including the cyberattack database. Layer (L3) provides the necessary policies and rules for CVs along with countermeasure detection steps. Here, RSUs manage the DCAV and collect all big data communications to detect CVs. Layer (L4) sends the collected data from all allocated web servers for analysis and detection. Consequently, CVs are prevented, and the security framework in DCAV and AVN can be updated.

According to [40], Einstein challenged and developed a theory of Brownian motion based on Brownian particle theory, which allowed him to find a physical and mathematical solution for many potential problems. His challenges extend from fundamental physics to

the very dynamics of securing financial markets and autonomous vehicles in modernity. Thus, Einstein's concept allows us to formulate Equation (1) for measuring displacement D of the particles in molecular communication.

$$D = \sqrt{\frac{k_B T \pi \eta R t}{6}} \tag{1}$$

where k_B is Boltzmann's constant, T is the temperature of molecular communication, and h is the viscosity of the liquid used in molecular communication applications. In our study, CV is proportional to η, which affects data communication obtained from smooth and secure data traffic and management. In big data communication, R is the size of the original and clean data, and t is the time. In this theoretical model, energy levels are proportional to CV; therefore, minimizing energy consumption is also important when an attack-detecting device is designed for analyzing countermeasures. In (1), the displacement of the abnormal data bits may be smaller than that of the normal data because the concentration or density of the data must be higher than that of the normal or pure data.

From (1), the kinetic energy of the molecules can be shown to depend on the temperature, which affects the energy levels when the components in the AV become heated. AV sensors collect the average energy of the CV at various points of data communication between the AVs and RSU. Albert Einstein's famous formula, given by (2), can be used as a theory that formulates and enables us to analyze the energy levels when CV affects AVN and DCAV. Using countermeasures in our proposed theoretical model enhances the accuracy of measuring CV levels in data communication.

$$E = mc^2 \tag{2}$$

where E, m, and c are energy, mass, and the speed of light, respectively. In each communication channel, the volume of big data traffic (v) of clean data can be measured using (3).

$$m = dv \tag{3}$$

where d is the density of the clean data. If the data comprise CVs, the density of data in the communicating channel will be high. Therefore, the mass will increase, and the energy of the clean and attacked data is calculated using (4).

$$E = dvc^2 \tag{4}$$

This proposed model can effectively counteract the changing energy levels by using dedicated sensors allocated for monitoring CV that measure the energy levels before and after cyberattacks. If the energy level exceeds the threshold limit, the CV level is considered high. Otherwise, the CV level is considered normal. Here, the rate of data communication can also be considered using time-dependent data and information.

In (1), displacement D depends on the density of the data, which allows us to calculate the energy using (4). In this model, (1) provides the CV of the data communication when the channel is exposed to man-made attacks or exhibits abnormal behavior. The proposed model can resolve all such dynamic and static attacks, provided it employs efficient tools and stronger countermeasure algorithms.

Using (2), energy can be compared with the threshold limit, which allows users to analyze the CV values. The energy is proportional to the mass of the data.

$$\frac{E_a}{E_T} = \frac{m_a}{m_T} \tag{5}$$

In this experiment, the threshold value is set for the pure data (m_T), which is the size of the data assumed as a mass of the data. Also, the threshold energy of the pure data is set

as E_T. When attacked data size (m_a) is known, the energy of the attacked data is measured from (5).

$$\frac{E_a}{E_T} = \frac{d_a}{d_T} \tag{6}$$

Assume that volume of attacked and pure data is the same. Here, energy is proportional to the density of the data. When the density of the attacked data (d_a) and pure data (d_T) are known, and the energy of the attacked data is measured from (6).

4. Results

According to the research, theoretical findings, and analysis, the big data communication of autonomous vehicles will be secured with the minimum energy consumption. Therefore, when society uses autonomous vehicles, there will be a secure environment with low energy costs.

Although the algorithms used in the countermeasures require strong detection capability, the types of cyberattacks still affect the detections, as shown in Figure 5. In this study, we used three different types of attacks (light, mild, and strong) detected using the proposed model, including a specific algorithm for countermeasures. The cyberattacks may be classified into CA1 (light), CA2 (mild), and CA3 (strong) to measure CV, which depends on the density of data.

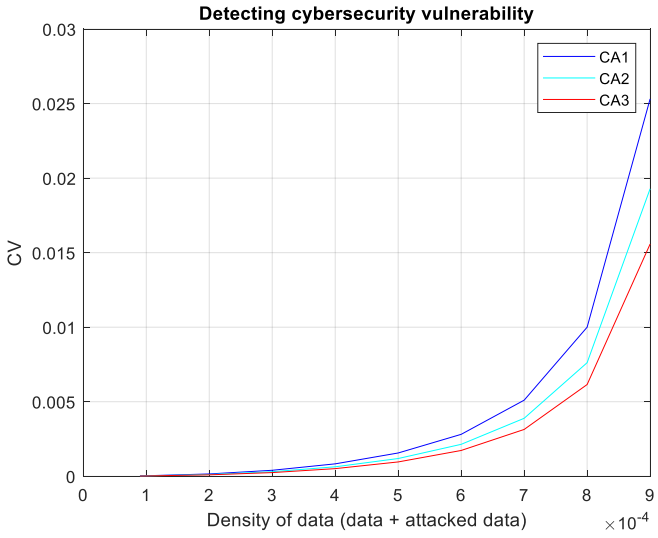

Figure 5. Detection of different cyberattacks.

Figure 6 shows the different energy levels when DCAV faces cyberattacks or threats classified into the following categories:

1. Strong threats: These threats damage the DCAV and AVN configurations, where specific onboard diagnostics (OBD) hacks prevent interior features from functioning. In AVs, V2V hacks, V2I hacks, OBD, GPS spoofing, and MITM increase the strength of threats and CVs.
2. Mild threats: These threats weaken and slow down the interior and exterior systems of AVs. In autonomous services, key fob hacking, attacks on the control area network (CAN) bus, and entertainment system hacking limit the efficiency of the services.
3. Light threats: Selected components such as airbags and brakes are hacked when AVs are on the move because DCAV and AVN depend on all features and services used in the AVs.

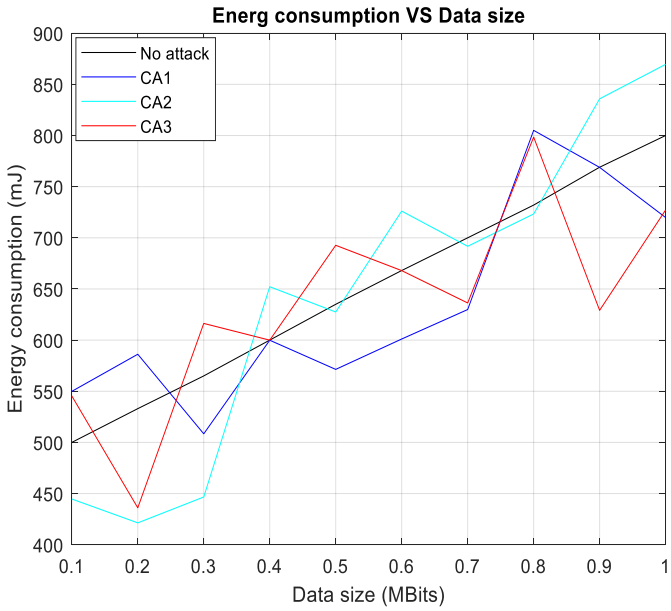

Figure 6. Energy with cyberattacks.

Figures 6 and 7 show that the energy levels differ when DCAV faces different attacks with a fixed CV level.

- In Figure 6, the data size is fixed to compare the energy levels.
- In Figure 7, CV levels (CV level 1, CV level 2, CV level 3, and CV level 4) are considered fixed weights to illustrate the energy level results and comparisons.

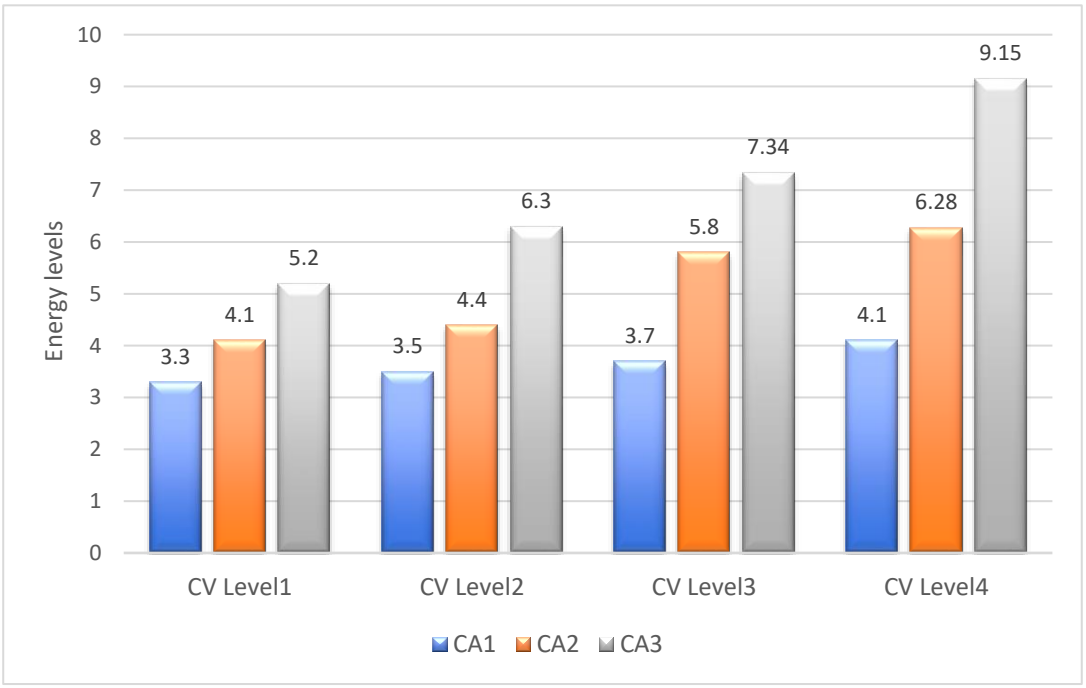

Figure 7. Energy levels variations for different cyberattacks.

The experimental setups and actual parameters for AVs considered in each result prove that awareness of the energy levels enables us to develop low-cost countermeasures with strong detection capabilities.

Ideal countermeasures should be able to detect all changes in energy levels accurately and quickly because a tiny change in the energy level has a significant impact on recognizing the effect of these attacks. All vulnerabilities created by cyberattacks in DCAV and AVN should be evaluated using accurate measurements of each energy level. When the proposed network was used to identify which information was visible to attackers, it showed a variation in energy levels in the affected components. In comparison, conventional networks showed no change in energy levels. In this study, we modified an AVN using updated security solutions and emerging technology.

When we use the digital signature algorithm, we may employ specific *and asymmetric* cryptographic schemes (DSA, RSA, ECDSA, etc.) within the cybersecurity solutions, which allow researchers to measure the security levels against the cost depending on the complex design and algorithms. According to the [40,41], ECDSA improves the EE with the limited data sizes, but it may not support the big data. The other symmetric and asymmetric cryptographic schemes may increase the EE with the increasing data sizes. Still, the design of the schemes must be smart and supports the low-complex structure and minimum energy consumption. Thus, our proposed scheme provides both maximum security and EE when we increase the data sizes considered in the communicating components of autonomous vehicles.

$$Energy\ (\mathrm{mJ}) = Power\ (\mathrm{mW}) \times time\ (\mathrm{s}) \tag{7}$$

The power of the scheme depends on the processing power of the pure data and attacked data which rely on cyberattacks. Attacked data contain more data than pure data. Therefore, the size of the data varies the power and time (7) in different systems where attacks are. Time considered during the operations and allocated or fixed time for processing may be varied with the time complexity and delays that occurred in the cyberattacks. Using the proposed model, we use low-complex algorithms to detect cyberattacks and energy-efficient components that support the countermeasures for minimizing cybersecurity vulnerabilities. Getting rid of the cyberattacks and data breaches in autonomous vehicular communication is the challenge of analyzing tiny energy variations that happen during the autonomous service. Here, we can use the countermeasure with two parameters: power and time. To focus on the power, we can keep the fixed time and measure the power of the pure and attacked data. If we want to focus on time, we can keep the fixed power and measure the time complexity of the pure and corrupted or attacked data. Assume that pure and attacked data have different data sizes in terms of data/big data properties such as volume.

In Figure 7, the volume of data is fixed with four different CV levels (CV level 1, CV level 2, CV level 3, and CV level 4). Assume that volume of data is increasing with the data sizes. Within the volume, pure and attacked data have different data sizes or percentages according to the attacks.

According to the [41–44], comparison studies show that energy consumption (mJ) increase with the data sizes. To determine the energy consumption, as in Figure 6, the threshold energy property of data (volume, size, etc.) and energy of the pure data should be considered with the existing results [42].

5. Discussions and Analysis

When developing countermeasures, measuring and analyzing the energy levels of each component in AVs exposed to cyberattacks is important. Based on the measurement results, the following parameters were considered. Types of CVs induced by cyberattacks, energy levels of each cyberattack, and the detecting conditions and abilities of the countermeasures.

More than 90% of automotive innovations contribute to making transport autonomous, such as regular transportation services that depend on software-driven electronic components. However, security risks and CVs created by faulty components increase the safety and security costs incurred by AVs. Purposed attacks are also increasing with the growing number of hackers working to obtain financial benefits or enter the competition.

Nevertheless, the energy levels of each attack are different; therefore, the countermeasure integrated with the proposed approach detects the abnormal traffic associated with big data communication. The energy levels of normal and abnormal data can be compared dynamically, and setting the energy level threshold enables the system to detect abnormal behavior more efficiently and proactively.

5.1. Current Status of Countermeasure Technology Development

AVs require appropriate countermeasures that incorporate privacy-protective authentication technology. The current status of countermeasures and their functions still have fixed hardware and software technology, where the legacy of the overall system is upgradeable. However, data breaches due to CVs are escalating owing to numerous unavoidable attacks that behave like real network communication requests. These situations may be classified based on the following cases.

Privacy protective authentication technology in DCAV: Although countermeasures detect the changes in energy levels to identify attacks, basic security features such as authentication are still required. In authentication technology, the analysis of CV, as shown in Table 2, can be improved with the following: (i) user verification to prevent Sybil occurrences and eliminate malicious units, (ii) verification of the source of the messages to ensure that they were generated by genuine ITS units, and (iii). Location verification to protect the reliability and significance of the current data.

Table 2. Possible CAs of CV and countermeasures for Component of AV.

DCAV and Big Data Components	Possible Attacks for Cybersecurity Vulnerabilities	Countermeasures
Radars and Cameras	Blind spot and false image	Energy levels of data risk false reactions and breaches at various points
GPS	Spoofing and jamming	Inaccurate or wrong location data create impacts on energy levels
LiDAR	Jamming and smart materials	False detections during the big data change the energy performance
Sensors	Interference and fake sounds	Sensor malfunctions increase the extra energy during data communications

Autonomous activations in AVN: In big data communications, using countermeasures at various points will improve the capacity of cybersecurity solutions that enhance autonomous activations in vehicular networks.

5.2. Countermeasures with Proposed Model

According to the results, countermeasures and their future technology will support secure AVs with many modern features that proactively detect cyberattacks and CVs. In addition, appropriate security solutions and countermeasures are required for the following:

Twitter and Tesla AVs: When continuous Twitter data between AVs and RSUs are collected, big data communications can be achieved in vehicular communication.

Although AVs and RSUs depend on the interior and exterior AVN and their devices, such as sensors, the main communication shown in Figure 8 allows AVs to function properly and proactively with maximum secure services. In Figure 8, thick arrows representing the attacks could have appeared in any of these two detections when vulnerabilities are low or below the threshold. Dotted line arrows also collect the attacks according to the priority of vulnerabilities.

Emerging technology with proactive detection approaches: Interior and exterior attacks on AVs weaken transportation services depending on emerging technologies. Countermeasures using the proposed model should be designed to proactively detect interior and exterior attacks.

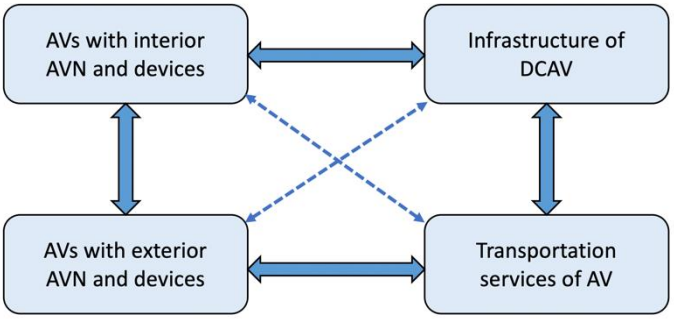

Figure 8. Main communication domains of AVs.

5.3. Applications Influenced by the Proposed Research

Figure 9 shows the tentative applications of the proposed research (secure communication integrated with autonomous vehicles, secure services as features of autonomous vehicles, and secure communication integrated with autonomous vehicles using vulnerability evaluation, respectively), which provides secure communication through the countermeasure and its efficient cybersecurity vulnerabilities evaluation. Building countermeasures with efficient security algorithms is considered a proposed model in this research.

Figure 9. *Cont.*

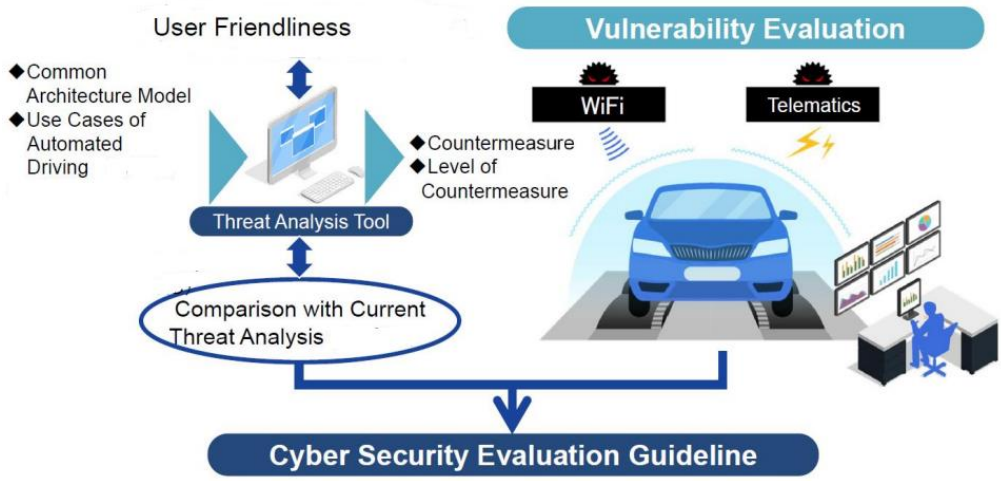

Figure 9. Used security applications of autonomous vehicles of the proposed research.

6. Open Challenges

The architecture proposed in this study will introduce new opportunities for analyzing CVs and countermeasures in potential autonomous systems and future applications, including security solutions for AVs and DCAVs. However, the development of countermeasures for big data communication faces the following challenges.

- Cyberattacks influence sudden changes in energy levels which could damage the communication devices used in autonomous systems and vehicles. In the future, hydrogen-based energy can be used for power transmission and communication, which might be attacked when the level of energy is exceeded suddenly during the operation of autonomous systems.
- The basic and luxury features of AVs also affect the latest gadgets, such as the remote keyless entry (RKE) system. Although cryptographic algorithms are applied in RKE development, the rolling codes used in RKE systems are vulnerable to all cyberattacks, including eavesdropping and RKE cloning. Therefore, countermeasures must include strong encrypted rolling codes and clone-resistant methods. Also, quantum-safe algorithms may be employed based on Symmetric Key and Asymmetric Key Encryption methods [45].
- Efficient and proactive countermeasures are also required for the AVN, big data communication networks, and related platforms used in AVs.
- Intelligent features and proactive cybersecurity solutions can be obtained only by securing big data communication through artificial intelligence (AI) integrated with AVN. Although it is difficult to implement, AI can effectively secure AVs and AVN, where intelligence approaches are considered in cybersecurity solutions, countermeasures, and threat intelligence. This is because AI enhances the capacity of the detection techniques used in the countermeasures and facilitates automated remediation, which supports proactive cybersecurity solutions.
- The proposed model primarily focuses on the security challenges of data communications. Other challenges, such as cryptography with AI, network security with low complexity, software vulnerability detection, and malware detection, need to be addressed in future work. Furthermore, the reliability of AVs requires further investigation.

We hope that the above-mentioned points will raise many research questions that will contribute to improving future transportation policies.

7. Conclusions and Future Work

This study presented a high-level overview of the CVs that threaten modern AVs, DCAVs, and automated driving features within AVN. Cybersecurity was enhanced by considering the symmetry of data communication and the vulnerabilities present in the advancement of autonomous vehicle security systems. Regarding the study of security analysis, asymmetric key encryption will be better for the security solution of countermeasure because asymmetric key encryption is far more secure than symmetric key encryption.

An appropriate theoretical model with necessary rules and policies was proposed to detect CVs and develop countermeasures for big-data communication to secure the data of the autonomous vehicle. Furthermore, this study proves that the level of cybersecurity solutions directly influences the energy levels that are accidentally created during abnormal operations and cyberattacks. The analytical approach of energy measurements is presented that energy consumption increases when cyberattacks occur in the AVN and big data communication.

The paper has a distributed cyber-attack detection architecture for AVNs was proposed as a countermeasure and practically evaluated. A countermeasure strategy based on the persistence of three different attacks (light, mild, and strong) was developed and implemented to verify the proposed model.

In future work, the features of countermeasures that achieve minimum energy consumption, maximum security, and proactive detection of CV, including power-based cyberattacks within AVs, will be considered. Therefore, it is possible to test the cybersecurity vulnerabilities caused by evolving cyberattacks as well as implement the practical countermeasure using cybersecurity algorithms.

Author Contributions: Conceptualization, A.A. and V.T.; methodology, A.A. and V.T.; validation, A.A. and V.T.; formal analysis, A.A. and V.T.; investigation, A.A. and V.T.; writing—original draft preparation, A.A. and V.T.; writing—review and editing, A.A. and V.T.; visualization, A.A.; supervision, V.T.; project administration, A.A.; funding acquisition, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by King Abdulaziz University, grant number D-147-611-1440.

Data Availability Statement: Not applicable.

Acknowledgments: This project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under grant no. D-147-611-1440. The author, therefore, gratefully acknowledges the DSR technical and financial support.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wiseman, Y. Autonomous Vehicles. In *Encyclopedia of Information Science and Technology*, 5th ed.; IGI Global: Hershey, PA, USA, 2020; Volume 1, pp. 1–11. Available online: https://u.cs.biu.ac.il/~{}wiseman/Autonomous-Vehicles-Encyclopedia.pdf (accessed on 3 October 2022).
2. Bakhtina, M.; Raimundas, M. Information Security Risks Analysis and Assessment in the Passenger-Autonomous Vehicle Interaction. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2022**, *13*, 87–111.
3. KAlheeti, M.A.; McDonald-Maier, K. Intelligent intrusion detection in external communication systems for autonomous vehicles. *Syst. Sci. Control Eng.* **2018**, *6*, 48–56. [CrossRef]
4. George, N.; Thomas, J. Authenticating communication of autonomous vehicles with artificial intelligence. *IOP Conf. Ser. Mater. Sci. Eng.* **2018**, *396*, 012017. [CrossRef]
5. Jameel, F.; Chang, Z.; Huang, J.; Ristaniemi, T. Internet of autonomous vehicles: Architecture, features, and socio-technological challenges. *IEEE Wirel. Commun.* **2019**, *26*, 21–29. [CrossRef]
6. Yağdereli, E.; Gemci, C.; Aktaş, A.Z. A study on cyber-security of autonomous and unmanned vehicles. *J. Def. Model. Simul.* **2015**, *12*, 369–381. [CrossRef]
7. Parkinson, S.; Ward, P.; Wilson, K.; Miller, J. Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Trans. Intell. Transport. Syst.* **2017**, *18*, 2898–2915. [CrossRef]
8. Kukkala, V.K.; Thiruloga, S.V.; Pasricha, S. Road map for Cybersecurity in Autonomous Vehicles. *arXiv* **2022**, arXiv:2201.10349.
9. Petit, J.; Shladover, S.E. Potential cyberattacks on automated vehicles. *IEEE Trans. Intell. Transp. Syst.* **2014**, *16*, 546–556. [CrossRef]

10. Chowdhury, M.; Islam, M.; Khan, Z. Security of connected and automated vehicles. *arXiv* **2020**, arXiv:2012.13464.
11. Farha, J.; Sun, W.; Niyaz, Q.; Alam, M. Security modeling of autonomous systems: A survey. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–34. [CrossRef]
12. Khadka, A.; Karypidis, P.; Lytos, A.; Efstathopoulos, G. A benchmarking framework for cyber-attacks on autonomous vehicles. *Transp. Res. Procedia* **2021**, *52*, 323–330. [CrossRef]
13. Kim, K.; Kim, J.S.; Jeong, S.; Park, J.-H.; Kim, H.K. Cybersecurity for autonomous vehicles: Review of attacks and defense. *Comput. Sec.* **2021**, *103*, 102150. [CrossRef]
14. Sun, X.; Yu, F.R.; Zhang, P. A survey on cyber-security of connected and autonomous vehicles (CAVs). IEEE Trans. *Intell. Transport. Syst.* **2021**, *23*, 6240–6259. [CrossRef]
15. Gao, C.; Wang, G.; Shi, W.; Wang, Z.; Chen, Y. Autonomous driving Security: State of the art and challenges. *IEEE Internet Things J.* **2021**, *9*, 7572–7595. [CrossRef]
16. Chow, M.C.; Ma, M.; Pan, Z. Attack models and countermeasures for autonomous vehicles. In *Internet of Things*; Springer: Cham, Switzerland, 2021; pp. 375–401. [CrossRef]
17. Nguyen, H.P.D.; Nguyen, D.D. Drone application in smart cities: The general overview of security vulnerabilities and countermeasures for data communication. *Stud. Syst. Decis. Control.* **2021**, *332*, 185–210. [CrossRef]
18. Yaacoub, J.A.; Noura, H.N.; Salman, O.; Chehab, A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *Int. J. Inf. Secur.* **2022**, *21*, 115–158. [CrossRef]
19. Ranaweera, P.; Jurcut, A.; Liyanage, M. MEC-enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures. *ACM Comput. Surv.* **2022**, *54*, 1–37. [CrossRef]
20. Campisi, T.; Severino, A.; Al-Rashid, M.; Pau, G. The development of the smart cities in the connected and autonomous vehicles (CAVs) era: From mobility patterns to scaling in cities. *Infrastructures* **2021**, *6*, 100. [CrossRef]
21. Ribeiro, M.A.; Gursoy, D.; Chi, O.H. Customer acceptance of autonomous vehicles in travel and tourism. *J. Travel Res.* **2022**, *61*, 620–636. [CrossRef]
22. Brovarone, E.V.; Scudellari, J.; Staricco, L. Planning the Transition to Autonomous Driving: A Policy Pathway Towards Urban Liveability. *Cities* **2021**, *108*, 102996. [CrossRef]
23. Aldakkhelallah, A.; Simic, M. Autonomous vehicles in intelligent transportation systems. In *Smart Innovation, Systems and Technologies*; Springer: Singapore, 2021; pp. 185–198. [CrossRef]
24. Thayananthan, V. Advanced Security Issues of IoT based 5G Plus Wireless Communication for Industry 4.0. ISBN 978-1-53615-538-9. Available online: https://novapublishers.com/shop/advanced-security-issues-of-iot-based-5g-plus-wireless-communication-for-industry-4-0/ (accessed on 3 October 2022).
25. Shaikh, R.A.; Thayananthan, V. Trust Evaluation Wireless Network for Routing Data Packets. US10225708B2, 5 March 2019. Available online: https://patents.google.com/patent/US10225708B2 (accessed on 3 October 2022).
26. Algarni, A.; Thayananthan, V. Improvement of 5G transportation services with SDN-based security solutions and beyond 5G. *Electronics* **2021**, *10*, 2490. [CrossRef]
27. Shaikh, R.A.; Thayananthan, V. Risk-based decision methods for vehicular networks. *Electronics* **2019**, *8*, 627. [CrossRef]
28. Thayananthan, V.; Yazdani, J. Secure Cyber-Physical Systems for improving transportation facilities in Smart cities and industry 4.0. In *Secure Cyber-Physical Systems for Smart Cities*; Advances in Computer and Electrical Engineering; IGI Global: Hershey, PA, USA, 2019; pp. 1–26, ISBN 13: 9781522571896. [CrossRef]
29. Gupta, A.; Gupta, S.K. Flying through the secure fog: A complete study on UAV-Fog in heterogeneous networks. *Int. J. Commun. Syst.* **2022**, *35*, e5237. [CrossRef]
30. Sharma, D.; Gupta, S.K.; Rashid, A.; Gupta, S.; Rashid, M.; Srivastava, A. A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4114. [CrossRef]
31. Santosh, K.; Chaube, M.K.; Nenavath, S.N.; Gupta, S.K.; Tetarave, S.K. Privacy preservation and security challenges: A new frontier multimodal machine learning research. *Int. J. Sens. Netw.* **2022**, *39*, 227–245.
32. Alharbi, A.; Alotaibi, A.; Alghofaili, L.; Alsalamah, M.; Alwasil, N.; Elkhediri, S. Security in social-media: Awareness of Phishing attacks techniques and countermeasures. In *2022 2nd International Conference on Computing and Information Technology (ICCIT)*; IEEE: Tabuk, Saudi Arabia, 2022; pp. 10–16.
33. Chen, J.; Gallo, A.J.; Yan, S.; Parisini, T.; Hui, S.Y.R. Cyber-attack detection and countermeasure for distributed electric springs for smart grid applications. *IEEE Access* **2022**, *10*, 13182–13192. [CrossRef]
34. An, D.; Zhang, F.; Yang, Q.; Zhang, C. Data integrity attack in dynamic state estimation of smart grid: Attack model and countermeasures. *IEEE Trans. Automat. Sci. Eng.* **2022**, *19*, 1631–1644. [CrossRef]
35. Haque, K.M.B.; Bhushan, B.; Nawar, A.; Talha, K.R.; Ayesha, S.J. Attacks and countermeasures in IoT based smart healthcare applications. In *Intelligent Systems Reference Library*; Springer: Cham, Switzerland, 2022; pp. 67–90. [CrossRef]
36. Ahangar, M.N.; Ahmed, Q.Z.; Khan, F.A.; Hafeez, M. A Survey of Autonomous Vehicles: Enabling Communication Technologies and Challenges. *Sensors* **2021**, *21*, 706. [CrossRef]
37. Bangui, H.; Ge, M.; Buhnova, B.; Trang, L.H. Towards faster big data analytics for anti-jamming applications in vehicular ad-hoc network. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4280. [CrossRef]

38. Bangui, H.; Ge, M.; Buhnova, B. Improving big data clustering for jamming detection in smart mobility. In *IFIP Advances in Information and Communication Technology IFIP International Conference*; Springer: Cham, Switzerland, 2020; pp. 78–91. [CrossRef]
39. Raiyn, J. Data and cyber security in autonomous vehicle networks. *Transp. Telecommun. J.* **2018**, *19*, 325–334. [CrossRef]
40. Renn, J. Einstein's invention of Brownian motion. *Ann. Phys.* **2005**, *14*, 23–37. [CrossRef]
41. Bokhari, S.; Hamrioui, S.; Aider, M. Cybersecurity strategy under uncertainties for an IoE environment. *J. Netw. Comput. Appl.* **2022**, *205*, 103426. [CrossRef]
42. Potlapally, N.R.; Ravi, S.; Raghunathan, A.; Jha, N.K. nalyzing the energy consumption of security protocols. In Proceedings of the 2003 International Symposium on Low Power Electronics and Design, Seoul, Korea, 25–27 August 2003; pp. 30–35.
43. Oussous, S.A.; Hamza, F.Z.; Beloualid, S.; El Allali, A.; Bajit, A.; Tamtaoui, A. Green Smart City Intelligent and Cyber-Security-Based IoT Transportation Solutions for Combating the Pandemic COVID-19. In *Computational Intelligence Techniques for Green Smart Cities*; Springer: Cham, Switzerland, 2022; pp. 129–146.
44. Said, D.; Elloumi, M.; Khoukhi, L. Cyber-Attack on P2P Energy Transaction between Connected Electric Vehicles: A False Data Injection Detection based Machine Learning Model. *IEEE Access* **2022**, *10*, 63640–63647. [CrossRef]
45. Srivastava, S.; Tiwari, A.; Srivastava, P.K. Review on quantum safe algorithms based on Symmetric Key and Asymmetric Key Encryption methods. In Proceedings of the 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 28–29 April 2022; pp. 905–908.