Dijlah Journal of Engineering Science (DJES) Vol. 3, No. 1, March, 2026, pp. 117-126
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 116

Increasing Cyber-Security in Independent Vehicles through the Integration of Verification Vector Machines and Defense Multiplicative Adversarial Networks

Kholood J. Mawlood[1]
[1]Department of Mathematics, College of Education for Women , Tikrit University, Tikrit, Iraq

Article Info

Article history:

Received Oct.,19, 2025
Revised Nov., 25, 2025
Accepted Dec., 27, 2025

Keywords:

Autonomous vehicles
Defence mechanisms
threat intelligence
SVM-DGAN
Cyber-attack

ABSTRACT

Autonomous vehicles (AVs) are a significant advancement in transportation technology, offering greater safety, performance and comfort. Traditional cyber-security solutions frequently fail to defend antivirus software from sophisticated assaults that exploit software and communication network flaws. This study proposes using Support Vector Machine Fused Defense Generative Adversarial-Network (SVM-DGAN) to improve cyber-security in autonomous vehicles. In cyber-security, SVMs can be employed for threat intelligence by analyzing data to identify patterns and classify data into different categories, such as normal behaviour or anomalous activities indicating potential cyber threats. Defense GANs are employed for adaptive defense mechanisms to enhance the resilience of machine learning models against adversarial attacks in autonomous vehicle cyber-security. Initially we gather dataset from controller area networks (CAN). Pre-process the gathered data using minimum-maximum normalization. The following elements were used to compare the traditional and proposed methods in terms of accuracy (98.50%), precision (98%), recall (98.25%), and F1-score (97%). It shows that our proposed method is effective in autonomous vehicle cyber-security. The findings of our study affirm the viability and effectiveness of the SVM-DGAN framework as a formidable defence against cyber threats targeting autonomous vehicles.

Corresponding Author:

Kholood J. Mawlood
Department of Mathematics, College of Education for Women, Tikrit University

Tikrit, Iraq
Email: kjamal@tu.edu.iq

1. INTRODUCTION

In an era when technologies which have an impact on the world seem to be advancing everywhere, the autonomous vehicles are in a leadership position promising for a future where travelling is safer, more streamlined and more convenient [1]. Nevertheless, as the vehicles get more featured and integrated into our daily activities, the requirement of increasing the cyber-security becomes inevitable. By cyber security for autonomous vehicles, we mean everything from caveats and weaknesses of driverless cars and their underlying systems that lie in security threats [2]. These threats are also from attacks which aim at taking the commands to the vehicles or the manipulation of the data that mostly happens between various components of the driverless system. The repercussion of a successful cyber-attack on an autonomous vehicle could be a catastrophic situation; that can lead to vehicle's crash, injuries or even damage life [3]. One of the major focuses in information safety for self-driving cars is guaranteeing the accuracy and flexibility of the vehicle's computer software and communication platforms [4]. Different from a manual car, which use software programming and telecommunication infrastructure to regulate its movements, autonomous cars network use both complex software algorithms and interconnected networks to operate and move. In such case any weakness of these systems could be taken advantage with hackers who will attack the system and disturb it functions or will have an access to the information that is supposed to be confidential [5]. In order to

resolve these problems autonomous vehicle makers are working hand in hand with cyber-security experts to develop tailored security measures for autonomous vehicles. Implementation of encryption protocols to top the data exchange between vehicle components, installation of intrusion detection systems that will react and identify the threat in real-time, along with the incorporation of secure software development practices that decrease the possibility of other vulnerabilities that is developed therein [6]. In addition, the division of "threat by design" is getting more popular in the development of autonomous vehicles, representing awareness that security features should be constructed in every phase of the vehicle design and creation process [7]. This approach aims to identify and eliminate the vulnerabilities and providing more time to maintain honourable security practice before the adversaries being able to utilize them [8]. Another noteworthy feature of autonomous vehicle security is the protection of its communication systems by checking actual identity and controlling access to its systems, which might require the application of fingerprint authorization technologies or multi-factor authentication processes that would first determine the client's identity and then authorize them to access sensitive system features [9]. The study contributes to advancing cyber-security in autonomous vehicles by proposing an innovative approach that combines machine learning techniques with adaptive defense mechanisms called SVM-DGAN. The paper's remaining part is organized: part 2 delves into existing literature and research relevant to the study. Methodology, in part 3, describes the approach taken to conduct the research. Part 4 presents the findings and engages in a discussion, analyzing the results. Finally, part 5 wraps up with conclusions drawn from the study's outcomes.

2. RELATED WORK

The study [10] provided a strong threat modelling structure for autonomous vehicle (AV) perception systems by contrasting prevalent techniques in automotive threat modelling with ISO/SAE 21434 standards. It also investigated possible cyber-physical assaults against AV perception systems utilizing sensors and machine learning algorithms. It employed a comparative threat assessment and STPA-Sec methodology. Scope limits and practical implementation issues might be examples of limitations. The study [11] focused on improving the safety and security of self-driving cars through the application of scenario-based assessment for threat analysis in OTA updates. In order to identify cyber targets for highly computerized driving operations, they wish to employ Scenario-based HARA techniques to explain step-by-step TARA processes. Potential constraints can encompass the range of scenarios tackled and the evolving character of cyber-security risks in automotive systems. The paper [12] analyzed ordinarily underlying cyber-attacks against intelligent and autonomous vehicles using threat modelling to pinpoint crucial risks. Through the various virtual scenarios, they were able to demonstrate the potential effects of different attacks. Methodology used looks at threat analysis and simulation. The challenges might be that cyber-attacks varying with time and intricacy of systems of AVs. The research [13] investigated how cyber-physical dangers and vulnerabilities were attached to the connected and CAV ecosystem and also uncovered many of the vulnerabilities and intelligence that can be used to strengthen the security of vehicles. It was designed through an analytical exploration of the IT and OT, coupled with physical domain vulnerabilities, and examination of threat intelligence approaches. Limitations could comprise the variations of CAV technology and the problem of blending up different security approaches. The article [14] requested a privacy risk evaluation of the architecture structure of cross-linked and automatically-driven vehicles to detect problems and hazards in privacy. Walking through the process, the LINDDUN method was applied to the manufacture of modules that meets privacy standards and would serve manufacturers well in their decision making. They were cyclical in nature, as well as industry growth in connected car technology represented the limitation. The paper [15] evaluated a strategic attack amongst which malware sneaks into the Intelligent Transportation Systems' components mainly the ACC to unnoticeably denature the settings, hence producing false statistics of accidents. Original and non-intrusive Intrusion IDS was proposed and evaluated by data analytics which was based on real world data to evidence it success for catch these acts. One of the limitations was the lack of consideration for complexity of the research which has not been considered from reality. The research [16] developed a System Dynamics model that was used for an analysis of cyber-security in roll-out of CAVs. It connected crucial aspects together like the communicational framework, human factors and management rules supposed to understand what leads to effects and what negative outcomes were. It used a theoretical framework as a way of modelling or predicting those cyber-attacks force. Nevertheless, there were also considerations concerning the complexity and unpredictability associated with the modelling of the CAV cyber-security.

The research [17] focused on solving the increasing security problems during massive communication within the autonomous vehicle field, an especially vulnerable area in CVs. They showed an information security methodology

that uses encryption, proactive cyber-security measures and dynamic countermeasures to thwart CVs and data breaches. The method involved the estimation of energy of the impacts and the examination of countermeasure effectiveness. Flexibility and the ability to cope with changing threats were two possible drawbacks. The paper [18] investigated cyber security and privacy issue of CAVs and their influence on public acceptance. Thematic analysis revealed six major themes based on semi-structured interviews with 36 experts from academia, business and policymaking, knowledge, training, safeness, duty, regulation and credibility. Limitations such as expert bias and of course the dynamic nature of technology should be borne in mind.

3. METHODOLOGY

In this section, the study aims to enhance cybersecurity in AVs using the SVM-DGAN framework, integrating SVM for threat detection and DGAN for defense mechanisms. The collected data from CAN is pre-processed using min-max normalization. Figure 1 illustrates the SVM-DGAN algorithm-based architecture of CAN-based IDS.

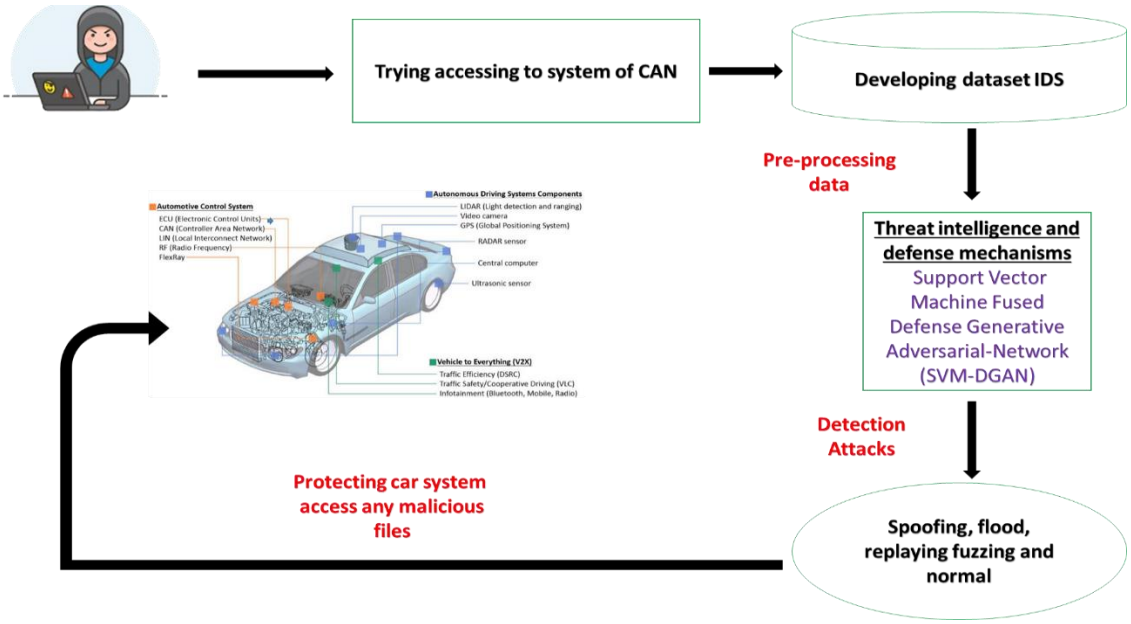

Figure 1. CAN- centric IDS Framework

3.1 Data Set

3.1.1 Dataset of Car Hacking

Standard data sources were used to produce experimental datasets [19], which were then processed using specific Raspberry Pi devices. One device captured network data, while the other acted as the attack node, feeding bogus data into the car's internal systems via the OBD-II relation. The CAN bus detected 26 distinct CAN IDs. Distributed denial of RPM meter spoofing, fuzzy attacks, service and drive gear spoofing were the four assault types that were modelled. With median intrusion duration of 3-5 seconds, 300 illegal messages were injected into each dataset over the course of 30–40 minutes.

3.2 Pre-processing Using Min-Max Normalization

Because CAN traffic data is highly complicated, the pre-processing phase is critical for enhancing classification algorithms. The dataset includes elements such as hexadecimal DLCs and 3 label spoofing, flooding, replay and classes; they turn category factors into numeric variables to aid the proposed system in detecting assaults. Maximum-minimum normalization techniques were employed to try avoiding training process convergence brought by large dataset modification. Scaling the dataset from 0 to 1 assisted maintain everything in the same range during the normalization process.

$$\text{Normalization} = \frac{u - u_{min}}{u_{max} - u_{min}} \left(w_{max_w} - w_{min_w}\right) + w_{max_w} \quad (1)$$

Whenever, u_{min} and u_{max} are the data values' minimum and maximum, equation (1).

3.3 Support Vector Machine-fused Defense Generative Adversarial Networks (SVM-DGAN)

SVM-DGAN combines the threat intelligence capabilities of SVM with the adaptive defense mechanisms called Defense GANs to improve cyber-security in autonomous vehicles, enabling them to identify and respond to potential threats more effectively.

3.3.1 Support Vector Machine (SVM)

This strategy's main goals are to shorten the distance between the hyper-plane focuses and increase the gap between the classes. The rationale for this proposed classifier is that different configurations of these characteristics can call for different notions of similarity (different parts). It is not required to make assumptions about the utilitarian kind of change, which renders information immediately detachable, because the bit undoubtedly contains a non-straight change. The kernel functions in the SVM classification are initiated to carry out the non-linear operation. This study employs the RBF and linear kernel functions for the classification procedure. These classification methods are support vectors with c acting as a constant and δ acting as a kernel variable in the end.

(a) Linear Kernel

Since the two classes can be separated linearly, it is possible to find at least one hyper-plane, represented by a biased vector that can separate the classes error-free. The simplest and fastest-processing kernel is V, which is also the fundamental kernel, equation (2).

$$\text{Lin}\,(x, y)\; xVy + z \tag{2}$$

(b) RBF Kernel

In the paper, the Gaussian or radial basis function kernel was used to aid in the classification process of support vector machines. Since the external summations are random concerning the test vector, the classification for a test vector can particularly make use of the findings of external summations found disconnected, equation (3).

$$\text{RBF}\,(x, y)\; \exp(\delta \,||\, x + y \,||), \quad \delta < 0 \tag{3}$$

3.3.2 Defence mechanisms using Generative Adversarial Networks (GANs)

The neural network consists of two: F and E. The function F: $N_k \rightarrow N_n$ translates a low-dimensional latent area into x's high-dimensional sample space. D operates as a binary neural network classifier. Adversarial learning is typically used in the training phase to learn F and E from input data sample x and vectors of chance z. For z, an isotropic Stochastic prior is usually assumed. While D learns to distinguish between "real" and "fake" samples, F learns to produce outputs with a distribution similar to x. To reduce the ensuing min-max loss, E and G undergo training in an alternating manner:

$$\min_F \max_E V\,(E, F) = \mathbb{E}_{x\sim \text{pdata}(x)}[\log E(X)] - \mathbb{E}_{Z\sim P_Z(Z)}\left[\log\left(1 - E\big(F(z)\big)\right)\right] \tag{4}$$

It was proven that the best GAN is attained when the resultant generator distribution, $p_f = \text{pdata}$, equation (4-5). However, GANs were challenging to train in reality, prompting the development of alternate formulations. One type of GAN that uses the Wasserstein distance to generate a loss function with the required properties is called a Wasserstein GAN (WGAN).

$$\min_G \max_D V\,(D, G) = \mathbb{E}_{x\sim \text{pdata}(x)}[E(X)] - \mathbb{E}_{Z\sim P_Z(Z)}\big[E\big(F(z)\big)\big]$$

(5)

Because WGANs' training techniques are stable, we adopt them as our generative model in this study, particularly when utilizing the methodology. One defense technique against adversarial assaults on classification networks, known as defense-GAN, aims to counter both white-box and black-box threats. An image x to be categorized and a trained GAN generating G are provided at inference time. The initial step is to find z^* to minimize.

$$\min_z \|G(z) - x\|_2^2 \tag{6}$$

After that, the classifier receives $G(z^*)$ as its input, equation (6). Using the supplied classifier training dataset, the GAN is trained in an unsupervised method. There should be no difference in performance between the two trained classifiers studied in this study.

The unique instance SVM-DGAN technology serves as a breakthrough in the early warning system for autonomous cars' cyber-security measures. The novel framework that comprises of SVM methods and DGANs approach improves both the detection and the response to anomalies to which autonomous vehicles are potentially targeted by cyber-attacks. SVMs can be used for threat intelligence in cyber-security for AVs find trends and group data points

into distinct groups, such as typical conduct or unusual activity indicating to possible cyber threats. Defensive GANs are used as adaptive defensive mechanisms in autonomous vehicle cyber-security to strengthen SVM resistance to adversarial attacks. It is brought via the system's capacity to own the responsibility of retaliating and changing to cyber threats coming out, thus guaranteeing robust and secure autonomous vehicle operations in complex cyber environments.

4. Performance Analysis

Therefore, such a system would be capable to work effectively on a Windows operating system with 8GB RAM and an Intel Core i7 CPU, as well languages such as Python and Jupyter via implementation. This part investigates the result of our suggested approaches and highlights the efficiency assessments. The proposed method evaluate in key finding metrics such as accuracy (%), F1-score (%), recall (%) and precision (%). The existing methods are CNN [20] and CNN-LSTM [20]. Accuracy evaluates the model's accuracy by dividing the number of correctly predicted cases by the overall amount of instances, taking account of both true positives and negatives. In terms of cyber-security, it assesses how well a system distinguishes between risks and non-threats, equation (7). Figure 2 and Table 1 illustrate the accuracy values. Compared with our proposed method (SVM-DGAN-98.50%) and existing methods such as CNN (86%) and CNN-LSTM (97.30%), our method significantly outperforms them. This highlights the effectiveness of SVM-DGAN in assessing the system's ability to identify and mitigate various cyber-security threats.

$$\text{accuracy} = \frac{\text{Number of Correct Predictions}}{\text{Total Number of Predictions}} \quad (7)$$

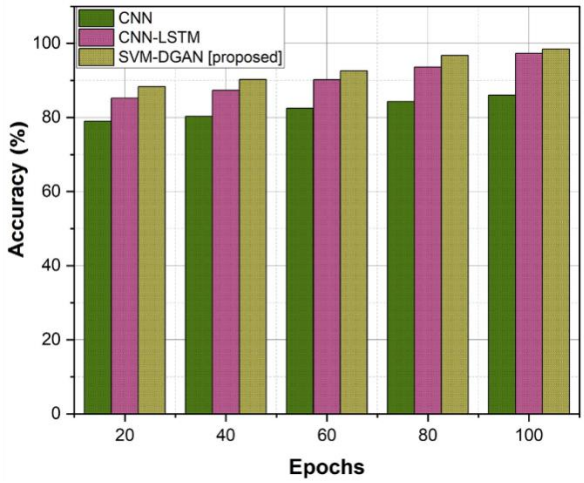

Figure 2. Accuracy outcome

Precision measures how well a system predicts the future with an acceptable result. The system's ability to prevent false positives is shown by the ratio of accurately predicted positive observations to the total anticipated positives. Precision in cyber-security refers to how dependable a system is when it identifies a threat, equation (8). Figure 3 illustrates the precision values. Our proposed method, SVM-DGAN, achieves a remarkable precision of 98%, surpassing existing methods like CNN (75%) and CNN-LSTM (97%). This indicates the superior performance of SVM-DGAN in enhancing the resilience of cyber-security systems, ensuring the safety, reliability and security of autonomous vehicle.

$$\text{precision} = \frac{\text{True Positives}}{\text{True Positives+False Positives}} \quad (8)$$

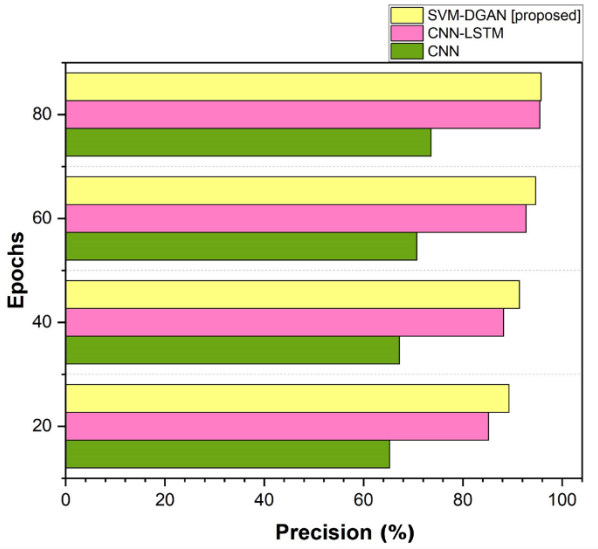

Figure 3. Precision outcomes

Recall, commonly referred to as sensitivity, is a measure of a classification model's completeness. It computes the true positive/false negative ratio. It assesses a model's capacity to accurately detect all instances of a class, such as security concerns in autonomous vehicle cyber-security as shown in equation (9). Figure 4 and table 1 illustrate the recall values. When we compare the proposed SVM-DGAN method (98.25%) with conventional approaches such as CNN (86%) and CNN-LSTM (97%), our approach consistently outperforms others. This demonstrates SVM-DGAN's in efficacy of cyber-security measures and adaptive defense mechanisms in autonomous vehicles, ultimately enhancing their resilience to evolving threat landscapes.

$$\text{Recall} = \frac{\text{False Positives}}{\text{True Positives+False Negatives}} \tag{9}$$

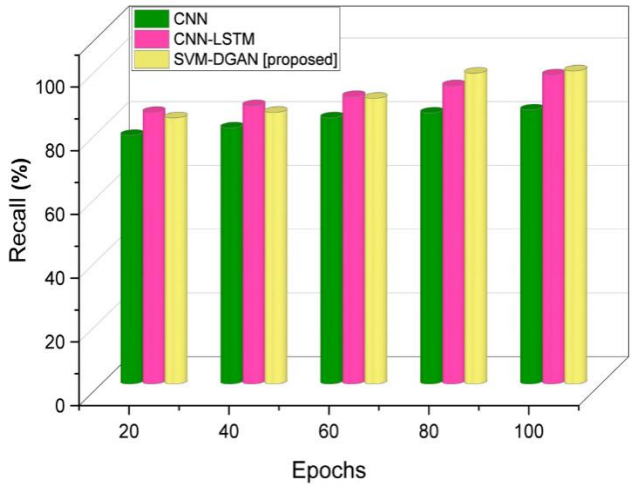

Figure 4. Outcome of recall

The F1 score is determined by computing a harmonic average of recall and accuracy. When the courses are out of balance, it performs extremely well since it finds a balance between recall and accuracy. Figure 5 and Table 1 illustrate the comparison values. The comparison between our proposed method (SVM-DGAN-97%) and existing methods like CNN (80%) and CNN-LSTM (96%) shows that our approach outperforms them. This demonstrates the

effectiveness of SVM-DGAN in improving cyber-security measures to ensure the safety and security of autonomous vehicles.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (10)$$

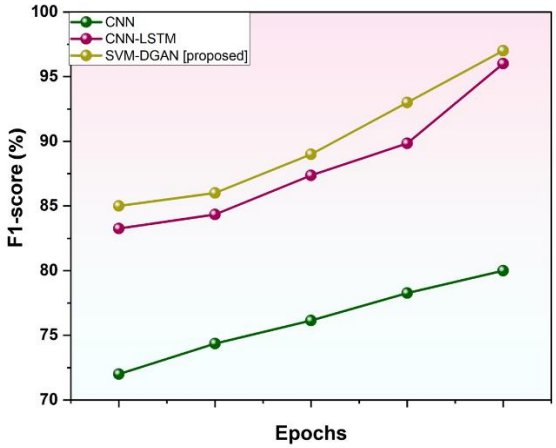

Figure 5. Outcome of F1-score

Table 1. Proposed method compared with existing methods

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
CNN	86	75	86	80
CNN-LSTM	97.30	97	97	96
SVM-DGAN [Proposed]	98.50	98	98.25	97

4.1 Discussion

Current approaches for autonomous vehicle cyber-security, such as CNN and CNN-LSTM have limitations. While CNNs [20] might struggle with detecting sophisticated adversarial attacks designed to deceive perception systems in autonomous vehicles. Similarly, CNN-LSTMs [20] improve sequential learning but are computationally costly, restricting real-time applications in highly dynamic situations. As consequence, these solutions might be insufficient to address the increasingly complex cyber-security vulnerabilities that self-driving vehicles experience. SVM-DGAN improves by combining SVM and DGAN, enhancing defenses mechanisms cyber-attacks with powerful, adaptable and proactive processes. The strategy described in this study use SVM-DGAN models to identify AV cyber-security assaults and safeguard the network.

4.2 Limitations

Autonomous vehicles are constructed around complex sensors, software and communication networks. Each component includes potential flaws that cyber criminals might exploit. Sensors and vision systems are critical to autonomous cars' ability to understand their environment. Cyber-security faces a great deal of difficulty from adversarial assaults, which comprise manipulating sensor inputs to trick the vehicle's perception systems.

5. CONCLUSION

Ensuring autonomous vehicle cyber-security is important for their safe integration into our transportation system. The research introduces the SVM-DGAN system, which makes substantial progress in improving the cyber-security of autonomous cars. The technique, which combines SVM and DGAN, provides an improved security framework against complex cyber-attacks by training threat intelligence and competitive models. The SVM-DGAN system outperforms traditional methods in metrics such as accuracy -98.50%, precision-98%, F1

scores-97% and recall-98.25% demonstrating cyber-security for autonomous vehicle. SVM-DGAN effectively mitigates common attack vectors such as remote hijacking, tampering with sensor data and denial-of-service attacks. The SVM-DGAN structure not only enhances security but also increases the dependability of autonomous transport systems, paving the stage for a safer and more robust mobility response in the future.

REFERENCES

[1] Hossain, K.A., 2023. Practices and Challenges of Modern Leadership in the Era of Technological Advancement.

[2] Channon, M. and Marson, J., 2021. THE liability for cybersecurity breaches of connected and autonomous vehicles. Computer Law & Security Review, 43, p.105628.

[3] Giannaros, A., Karras, A., Theodorakopoulos, L., Karras, C., Kranias, P., Schizas, N., Kalogeratos, G. and Tsolis, D., 2023. Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. Journal of Cybersecurity and Privacy, 3(3), pp.493-543.

[4] Liu, L., Lu, S., Zhong, R., Wu, B., Yao, Y., Zhang, Q. and Shi, W., 2020. Computing systems for autonomous driving: State of the art and challenges. IEEE Internet of Things Journal, 8(8), pp.6469-6486.

[5] Yaacoub, J.P.A., Noura, M., Noura, H.N., Salman, O., Yaacoub, E., Couturier, R. and Chehab, A., 2020. Securing internet of medical things systems: Limitations, issues and recommendations. Future Generation Computer Systems, 105, pp.581-606.

[6] Palombo, H., Tabari, A.Z., Lende, D., Ligatti, J. and Ou, X., 2020. An Ethnographic Understanding of Software ({In) Security} and a {Co-Creation} Model to Improve Secure Software Development. In Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020) (pp. 205-220).

[7] Li, G., Yang, Y., Li, S., Qu, X., Lyu, N. and Li, S.E., 2022. Decision making of autonomous vehicles in lane change scenarios: Deep reinforcement learning approaches with risk awareness. Transportation research part C: emerging technologies, 134, p.103452.

[8] Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G. and Ghani, N., 2019. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials, 21(3), pp.2702-2733.

[9] Mohammed, A.H.Y., Dziyauddin, R.A. and Latiff, L.A., 2023. Current multi-factor of authentication: Approaches, requirements, attacks and challenges. International Journal of Advanced Computer Science and Applications, 14(1).

[10] Ghosh, S., Zaboli, A., Hong, J. and Kwon, J., 2023. An integrated approach of threat analysis for autonomous vehicles perception system. IEEE Access, 11, pp.14752-14777.

[11] Khatun, M., Glaß, M. and Jung, R., 2021, February. An approach of scenario-based threat analysis and risk assessment over-the-air updates for an autonomous vehicle. In 2021 7th International Conference on Automation, Robotics and Applications (ICARA) (pp. 122-127). IEEE.

[12] Malik, S. and Sun, W., 2020, February. Analysis and simulation of cyber attacks against connected and autonomous vehicles. In 2020 international conference on connected and autonomous driving (MetroCAD) (pp. 62-70). IEEE.

[13] Basnet, M. and Ali, M.H., 2023. A deep learning perspective on connected automated vehicle (CAV) cybersecurity and threat intelligence. In Deep Learning and Its Applications for Vehicle Networks (pp. 39-56). CRC Press.

[14] Chah, B., Lombard, A., Bkakria, A., Yaich, R., Abbas-Turki, A. and Galland, S., 2022. Privacy Threat Analysis for connected and autonomous vehicles. Procedia Computer Science, 210, pp.36-44.

[15] Haghighi, M.S., Farivar, F., Jolfaei, A., Asl, A.B. and Zhou, W., 2023. Cyber attacks via consumer electronics: Studying the threat of covert malware in smart and autonomous vehicles. IEEE Transactions on Consumer Electronics.

[16] Khan, S.K., Shiwakoti, N. and Stasinopoulos, P., 2022. A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles. Accident Analysis & Prevention, 165, p.106515.

[17] Algarni, A. and Thayananthan, V., 2022. Autonomous vehicles: The cybersecurity vulnerabilities and countermeasures for big data communication. Symmetry, 14(12), p.2494.

[18] Liu, N., Nikitas, A. and Parkinson, S., 2020. Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. Transportation research part F: traffic psychology and behavior, 75, pp.66-86.

[19] Alsaade, F.W. and Al-Adhaileh, M.H., 2023. Cyber-attack detection for self-driving vehicle networks using deep autoencoder algorithms. Sensors, 23(8), p.4086.

[20] Aldhyani, T.H. and Alkahtani, H., 2022. Attacks to automatous vehicles: A deep learning algorithm for cybersecurity. Sensors, 22(1), p.360.

Appendix I

abbreviation	discerption
OTA	Over-The-Air
HARA	Hazard Analysis & Risk Assessment
TARA	Threat Analysis and Risk Assessment
CAV	connected and autonomous vehicle
IT	informational technology
IDS	Detection System
CAV	Connected and Autonomous Vehicles
CAN	Controller area networks
WGAN	Wasserstein GANs
CNN	Convolutions neural network
LSTM	Long short term memory
ACC	Adaptive Cruise Controller
STPA-Sec	system-theoretic process analysis for security
DLC	Data Length Code
OT	Operational technology
OBD-II	On-Board Diagnostics II

LINDDUN	Linkability, Identifiability, Non-repudiation, Detectability, Unobservability, and Non-compliance
RBF	Radial bias function
RPM	Revolutions Per Minute
ISO/SAE	International Standards Organization/ Society of Automotive Engineers

BIOGRAPHIES OF AUTHORS

Lec. Kholood J. Mawlood , Received her Msc. degree in the Computer Science from Al- Nahrain University, College of science, Baghdad – Iraq in 2008, She has been a full-time lecturer in Mathematical Dept.- College of Education for Women – Tikrit University, Tikrit, Iraq, since June 2009. She can be contacted at email: kjamal@tu.edu.iq.