Algorithms for Cybersecurity in CAVs Based On Deep Learning and Their Applications

Sara Sawalmeh

Mutah University, Faculty of Science, Mutah, Jordan

Sarahsawalmeh98@gmail.com

Abstract:

This paper is concerned with the study of some novel techniques that using artificial intelligence to protect networks of CAVs from cyberattacks, where we use some machine learning algorithms to detect attacks and compare the machine learning algorithms used for this in terms of accuracy and required operating time. Also, WEKA tool will be used for the desired comparison, as the experiments are carried out on a new dataset, which is a dataset abbreviated from the KDD99 dataset.

Keywords: Cybersecurity; Deep learning; Machine learning; CAVs; Cyberattack

1. Introduction

Digital improvements have turned our world into a digital society, which is vulnerable to various kinds of attacks. Cybersecurity is defined as the protection of systems, networks, applications, data, and all types of data from cyber-attacks. Cybersecurity is essential in the digital world. It is needed in daily activities such as shopping, business, transportation, and all tasks performed and stored on computer devices. The research focuses on autonomous and connected machines (CAVs), which have been the focus of much research and studies [1] [2]. Such networks have the advantages of wireless connectivity and self-driving. Being connected means that mechanisms rely on data sent from other mechanisms to determine the routing of their data and connections within the connected network. While the term autonomous indicates that it can dynamically command tasks and automatically restore events in the real world without the intervention of the driver [17].

Due to their previous characteristics, CAVs networks are exposed to cyber-attacks more often, they are vulnerable to data exchange with the external environment and with other mechanisms along their path [18]. The following paragraphs explain the models of cyber-attacks and how to use artificial intelligence to protect against these attacks.

2. Models of cyber attacks

Attacks range from installing spyware on a personal computer and can end with an attempt to destroy the infrastructure of entire countries. We can illustrate some of the attacks as follows:

a. Computer viruses: it is a self-copying program that can link itself to another program to reproduce it, so it is very difficult to track it because it can change its digital locations at any time.

b. Adware: is a malware known for producing pop-up messages. Hackers create an attractive program, and when the user runs it, they can get into the user's computer and delete or use his data.

DOI: https://doi.org/10.54216/IJAACI.060203
Received: November 19, 2023 Revised: December 18, 2023 Accepted: January 01, 2024

c. Trojan horse: it is a type of malware that presents itself as a useful program and controls systems. He can install the virus into the system, but he cannot reproduce himself. It can delete important files and data from the user's computer and send information to the hacker's system.

d. Ransomware viruses: it is a virus that attacks the user's computer and extorts it to earn money.

e. Phishing emails: used to steal a user's personal information. Fraudulent emails are sent to the user, manipulated as if from administrators. This virus gives hackers information about login details of various social media accounts and other credit card information.

Man-in-the-middle (MITM), denial-of-Service (DoS) attacks, SQL injections and Botnets are other types of cyber threats.

The main function of internet experts is to:

- Find, test and fix vulnerabilities within the company's infrastructure.
- Malicious content monitoring systems.
- Identify network breaches.
- Install software updates, firewalls and virus protection on a regular basis.
- Reinforce areas where attacks may have occurred.

They use various methods to defend systems and networks from attacks. Some of the best practices include:

- Use two-way authentication.
- Install regular updates.
- Use firewalls to disable unwanted services.
- Employ cryptography or cryptography.
- Secure DNS (domain name servers).
- Avoid deception tricks.
- Running antivirus software.
- Secure passwords.

The cyber security system plays a vital role in maintaining peace and order in this dynamic digital world.

2.1. Artificial intelligence in the field of cyber attacks

Many artificial intelligence techniques and methods have been developed over time to counter cyber-attacks. These methods are divided into: artificial neural network (ANN), expert system, intelligent agent, machine language.

Security in artificial intelligence ranges from the use of Antivirus/ Malware, data loss prevention, fraud detection / anti-fraud, identity and access management, intrusion detection/ prevention system, risk management. Large companies such as Google, Meta, Microsoft, Amazon, SpacesX and others are interested in owning the threat files of cybercriminals. According to Finch: "artificial intelligence can be used to identify patterns in computer systems that reveal vulnerabilities in software or security software, allowing attackers to exploit newly discovered vulnerabilities. Thus, if cyber experts can think a step beyond the thinking of these criminals, then artificial intelligence alone will enhance cybersecurity. Otherwise, these attackers will rule the world.

The following paragraphs explain the AI methods used to counter attacks.

2.1.1. Artificial neural network (ANN):

It is a statistical educational model that simulates the structural and functional behavior of the human brain, first established as a concept in 1957 by Frank Rosenblatt. ANN has the ability to learn and solve problems in various complex areas. In cybersecurity, artificial neural networks have been used in all four phases of the integrated security approach (a comprehensive classification of the cyber defense framework), consisting of the early warning phase, the prevention phase, the detection phase, and the reaction / response phase. Avoiding intrusion detection techniques also applies to neural networks. These plans have been demonstrated in DoS attack detection, spam filtering, malware analysis, and forensic science.

DOI: https://doi.org/10.54216/IJAACI.060203
Received: November 19, 2023 Revised: December 18, 2023 Accepted: January 01, 2024

2.1.2. Expert system:

Specialization is the most common artificial intelligence method. The Expert Program represents a technique for searching for solutions to problems caused by a client or a particular technique in a particular technology area. They can be used specifically in decision-making assistance, for example, in the field of medical care, banking or virtual worlds.

There are many optimization techniques for solving complex problems from accurate analytical medical diagnostics to highly advanced hybrid systems. The experience scheme includes a knowledge base containing a specialized analysis of a particular field of application. To refer to the knowledge base, this has an engine that offers solutions based on this understanding.

According to the way of thinking, expert systems can solve two types of problems:

- **Attribution-based inference:** this type invokes previous similar problem situations, and assumes that solutions to the previous problem situation can be used to solve a good problem. After that, he will evaluate the new solution and may revise as needed and then add to the knowledge base. This approach helps to constantly improve the accuracy of the system and gradually learns new problems.
- **Rule-based reasoning:** this type uses rules defined by experts to solve problems. The rules consist of two parts: a condition and an action. Analyzes problems in two steps: first, assesses the situation and then takes the appropriate action. Unlike case-based systems, rule-based systems cannot learn new rules or automatically modify existing ones.

2.1.3. Smart agent: a smart agent (IA) is a self-controlled entity with a separate internal decision-making mechanism and a personal goal. He monitors through sensors, monitors the field using triggers and controls its actions towards achieving goals. Smart customers can learn information or use it to achieve their goals. They may also have responsive characteristics, and when communicating with other independent agents they may understand and respond to changes in their field. This enables them to gain experience over time by learning and communicating with their environment. Use IA to avoid distributed denial of service (DDoS) attacks.

2.1.4. Machine language: ML provides systems with the ability to discover and formalize the principles underlying that data, learn from data, and improve from experience without being explicitly programmed. The learning process begins by observing the data through examples to look for patterns in the data and make a better decision in the future based on the examples given. With this knowledge, the algorithm can consider the properties of previously invisible examples. ML uses statistics to extract information, detect patterns and draw conclusions even while using a huge amount of data. There are different types of machine learning algorithms. They can also be classified into three main categories:

- **Supervised learning:** this type has a training process with a large set of titled Data. After the training process; the system should be checked with the test data set. Such learning algorithms are usually used as a classification mechanism or a regression mechanism. The regression algorithm generates output or prediction values, which are one or more numbers of continuous value according to the input. Classification algorithms classify data into categories and unlike the regression mechanism, classification algorithms generate discrete outputs.
- **Unsupervised learning:** unlike supervised learning, unsupervised learning uses an unnamed training dataset. Unsupervised learning is usually used for data aggregation, dimensional reduction, or density estimation.
- **Reinforcement learning:** this type of learning algorithm learns the best actions based on rewards or punishments. Reinforcement can be counted as a combination of supervised learning and unsupervised learning. Reinforcement learning is useful in cases where data is limited or not given.

2.2. Classification algorithms

Below we explain a set of algorithms that can be tried as a matter of classification. A standard machine learning classification problem will be used to illustrate each algorithm.

2.2.1. Logistic Regression: is a binary classification algorithm. It assumes that the input variables are numeric and have a Gaussian distribution (bell curve). In the case of the Ionosphere dataset, some input attributes have a distribution similar to the Gaussian distribution, but many do not. The algorithm learns a constant element for each input value, which is linearly integrated into a regression function and transformed using a dependent (in the form of s). Logistic regression is a quick and simple technique, but it can be effective for solving many problems.

2.2.2. Naive Bayes: is a classification algorithm. Input values are traditionally assumed to be nominal, although

DOI: https://doi.org/10.54216/IJAACI.060203
Received: November 19, 2023 Revised: December 18, 2023 Accepted: January 01, 2024

numerical inputs are supported by the distributive assumption. Naive Bayes uses a simple (and therefore naive) application of Bayes ' theorem, calculating the prior probability for each class of training data and assuming that they are independent of each other (technically called conditional independence). This is an unrealistic assumption because we expect variables to interact and be dependent, although this assumption makes probabilities quick and easy to calculate. Even under this unrealistic assumption, Naive Bayes has been proven to be a very efficient classification algorithm.

Naive Bayes calculates the posterior probability for each category and makes a prediction for the category with the highest probability. It supports both binary classification problems and multi-category classification.

2.2.3. Decision Tree: decision trees can support classification and regression problems. Decision trees have recently been referred to as classification and regression trees (CART). It works by creating a tree to evaluate an instance of the data.

The tree turns over starting from the top or root of the tree and then moving down to the leaves so that it can be predicted. The process of creating a decision tree works by greedy selection of the best division point in order to make predictions and repeat the process until the tree has a constant depth. After the tree is created, it is truncated to improve the ability of the model to generalize to new data. The C4.5 algorithm is another, more advanced decision tree algorithm.

2.2.4. k-Nearest Neighbors: the-k nearest neighbor's algorithm supports both classification and regression. It is also called KNN for short. It works by storing and querying the entire training dataset to identify the most similar training patterns when making a prediction. In this way, there is no model other than the initial training dataset and the only calculation performed is to query the training dataset when a prediction is requested.

It is a simple algorithm but it does not assume much about the problem other than that the distance between the data instances is of importance in making predictions. And therefore they often achieve very good performance. When making predictions about classification problems, KNN will take the status (the most common category) of the most similar cases in the training dataset.

2.2.5. (SVR) Support Vector Regression: supporting vector machines have been developed for binary classification problems, although extensions of this technique have been made to support multi-class classification and regression problems.

SVM was developed for numeric input variables, therefore it converts nominal values to numerical values. The input data is also normalized before it is used.

Unlike SVM which finds a line that better separates the training data into classes, SVR works by finding a line of the best t which reduces the error of the cost function. This is done using an optimization process that takes into account only the data instances in the training dataset that are closest to the line at the lowest cost. Such cases are called support vectors, hence the name of the technique.

3. The importance of research and its goals

Initiatives related to connected and autonomous vehicles (CAV) have become one of the fastest expanding in recent years, and are beginning to affect people's daily lives. More and more companies and research institutions announced their initiative. Governments around the world have also introduced policies to support and accelerate the deployment of CAVs. Along with this, issues such as cybersecurity in CAV have become mainstream and are an essential part of the complexities of CAV deployment. However, there is no universally agreed or recognized framework for CAV cybersecurity.

The research aims to compare the performance of machine learning algorithms for protection against cyber-attacks in terms of accuracy and runtime on a new dataset modified from the KDD99 dataset.

4. Reference studies

In [3] the threats on autonomous motor vehicles and cooperative motor vehicles were analyzed. This analysis shows the need for more repetitions more significantly than many expected. He also raised the level of focus to provoke discussion about these threats at this early stage of the development of vehicle automation systems. He concluded that GNSS spoofing and injecting fake messages are among the most serious cyber threats.

In [4] online cyber-attacks were divided into two main types: passive attacks and active attacks. Active attacks are difficult to recognize, but easy to defend, as attackers do not interact with the data; while active attacks, such as

DOI: https://doi.org/10.54216/IJAACI.060203
Received: November 19, 2023 Revised: December 18, 2023 Accepted: January 01, 2024

modification and spoofing, are easy to recognize, but difficult to defend, as attackers can modify or falsify messages in data transmission. Currently, there is no current global safety standard for CAVs vehicles. Thus, the systematic definition of methods for analyzing attacks is highly desirable for the development of CAVs.

In [5] it was pointed out that the current vehicle safety standard ISO26262 does not take into account security issues to avoid both unintentional and deliberate attacks.

In [6], an overview of the various challenges associated with the application of machine learning in vehicle networks was presented, focusing on the perspective of ML hostile attacks on CAVs and identifying a solution to defend against hostile attacks in multiple places.

In [7] he proposed directed machine learning as a specific anti-jamming protocol for vehicle traffic environments by focusing on detecting and filtering vehicle characteristic signals to detect the exact location of vehicles affected by jamming. A rationalization operator is used to examine the resulting frequency changes in signal strength due to jamming or external attacks. The open-source machine learning algorithm "CatBoost" with an emphasis on the decision tree-based algorithm was used to predict the positions of the jamming vehicle. The assessment certifies the resistant characteristics of the anti-jamming technology taking into account accuracy, memorization, F1 score and delivery accuracy scales. It was concluded that the scheme based on machine learning works effectively against jamming attacks on the CAV site.

According to a survey conducted at the University of Michigan [8], more attention is paid to the material damage caused by CAVs than to the leakage of private information. However, it was found that there is not enough relevant work on the cybersecurity of CAVs networks.

The European Space Agency (ESA) recently provided a call for proposals on CAV cybersecurity solutions using artificial intelligence [9]. And in [16] the researchers identified the principles of cybersecurity of CAVs networks in the UK.

5. Research methods and materials

In this research, we use a data set derived from the KDD99 [20] that is intended for detecting attacks and achieving security in CAVs networks. The new dataset contains 14 types of sub-attacks that threaten CAVs.
After removing duplicates and types of attacks not related to CAVs networks, a new dataset was created that is compatible with the new CAV Cybersecurity Framework. Tables 1 and 2 show the amount of normal data and attack data in each of the training datasets.

Table 1: The amount of normal data and attack data in training datasets

	10% KDD Data	New Data
Attacks	396.743	54.485
Normal	97.278	87.832
Total	494.021	142.317

Table 2: The amount of normal data and attack data in training datasets

	10% KDD Test Data	New Test Data
Attacks	250.436	23.348
Normal	60.593	47.913
Total	311.029	71.261

We compare the performance of the decision Tree and Naive Bayes machine learning algorithms on the new dataset in terms of accuracy and the necessary operating time using the WEKA tool.

- **Types of attacks in KDD99**

The KDD99 dataset contains more than 4 million data records, which is quite large for data processing on personal computers. For this research, a training dataset was used with 10% of the KDD99 dataset.

The attacks in KDD99 are divided into four main types with 39 sub-attacks and are as follows [21]:

1. PROBE, this type of attack scans the system for vulnerabilities to collect information from the system. In KDD99,

DOI: https://doi.org/10.54216/IJAACI.060203
Received: November 19, 2023 Revised: December 18, 2023 Accepted: January 01, 2024

sub-attacks of this type include: ipsweep, mscan, nmap, ortsweep, saint and satin.

2. DoS attack (denial of Service), disrupts the normal use or connection in the system by occupying all resources, so that neither the system nor the communication channel is available for normal use. Typically, attackers send a huge amount of data to flood the communication channel and system. In KDD99, DoS attacks contain apache2, back, land, mailbomb, Neptune, pod, processable, smurf, teardrop and udpstorm.

3. U2R attack (used to root) Attackers aim to gain access to super user accounts. They detect vulnerabilities in the system and then get access to the root of the system. In KDD99, U2R attacks include buffer-overflow, HTptunnel, loadmodule, perl, ps, rootkit, sqlattack and xterm.

4. R2L attack (from remote to local) Attackers aim to gain access to the system and send packets using a remote connection, the attacker does not have an authorized account in the system, but can access it locally.

In KDD99, these files contain ftp write, guess password, imap, multihop, phf, and send mail, sumpgetattack, snmpguess, spy, Warezclient, warezmaster, worn, xlock and xsnoop.

KDD99 provides a comprehensive dataset covering a variety of types of attacks in computer networks. However, the dataset cannot be used directly for CAV cybersecurity, due to the peculiarities of CAVs mentioned above.

In this research, we adapt the KDD99 dataset and process it by removing unrelated types of attacks.

Table 3 shows the possible types of attacks in KDD99 that may also occur in CAV. In Table 3, I classified the possible types of CAV attacks into three levels: H for High, P for Possible, and I for unrelated attacks (Irrelevant). After processing the data, the total number of types of CAV attacks decreased from 39 to 14, with 19 types of possible CAV attack and 6 types of unrelated attack.

Data processing on various types of attacks can be justified according to the previous figure as follows:

1. Some of the attacks were without a clear definition. Since the data is taken from the KDD99 dataset, the definitions of the attacks refer to their original descriptions. Some sub attacks lack clear definitions, and therefore cannot be classified as P-type in CAV attacks. The type of attack can be changed as soon as a clear definition is available.

2. Some attacks do not fit into the CAV Cybersecurity Framework. However, since KDD99 is a data set about computer and network security, TPC/IP protocols are older, and it can only be found in an older Linux operating system called SunOS 4.1.

As soon as the protocol and the environment expire, the possibility of this attack may also disappear. These types of attacks do not fit into the CAV framework, so they have been removed.

3. Some attacks were not compatible with CAV attack points. To conduct an attack, except for physical damage, attackers need to find one of the weak points of the CAV system. These attack points can be in physical parts, software, data, or a communication channel.

Table 3: Possible KDD99 sub attacks in CAVs networks

	Attack	Possibility		Attack Yypes	Possibility
PROBE	Ipsweep	H	U2R	Ps	I
	Mscan	P		Rootkit	P
	Nmap	H		Sqlattack	P
	Portsweep	P		Xterm	I
	Saint	P	R2L	ftp-write	H
	Satan	P		Gues-passwd	H
DOS	Apache2	P		Imap	I
	Back	P		Multihop	P
	Land	P		named	P
	Mailbomb	H		phf	I
	Neptune	H		Sendmail	P
	Pod	H		Snmpgetattack	P
	Processtable	P		snmpguess	P
	Smurf	H		Spy	P

DOI: https://doi.org/10.54216/IJAACI.060203
Received: November 19, 2023 Revised: December 18, 2023 Accepted: January 01, 2024

	Teardrop	H		wareezclient	P
	udpstorm	H		warezmaster	P
U2R	Buffer-overflow	H		Worm	H
	httptunnel	H		Xlog	P
	Loadmodule	I		Xsnoop	H
	perl	I			

In KDD99, some attacks can occur only under specific conditions and platforms, and therefore do not apply to Cav attack points. The probabilities of such attacks in CAV are low; for example, an apache2 attack can occur only in an Apache web server. If the CAV does not use the Apache web server, the attack cannot be carried out.

6. Results and discussion

Two machine learning algorithms developed on the WEKA simulator were used to build classification models, the first is Naïve bayes and the second is Decision Tree to detect anomalies in the data. The experiments were carried out on Intel Core 2duo, 2 GHz experiments with the windows7 64bit operating system.

WEKA is an open source data mining tool developed by the University of Waikato and widely used in research and studies necessary for the analysis and development of machine learning models.

After processing the original KDD99 data, the number of attack types was reduced to 14. The new dataset was used to build detection models, which were tested on the test dataset. The training set first uses 10-fold 10-folds cross validation to build the model. The machine learning model is then validated in a test dataset. The overall accuracy and runtime of the Decision Tree and Naive Bayes network models are compared in Table 3.

Accuracy refers to the ratio of the correct rated attacks to the total number of rated.

Table 3: Accuracy and runtime of two machine learning algorithms on test data

	Accuracy on the Testing Data Set	Time to Build Model(s)	Time on the Testing Data Set(s)
Naïve Byes	85.8%	0.06	3.2
Decision Tree	93.9%	0.59	0.4

From Table 3 it can be seen that the decision tree model achieved a higher accuracy than the Naïve bayes model, while the runtime differed. In a real-time driving environment, especially when CAVs vehicles are traveling at high speed, as they can cover a long distance of more than 30 meters in less than a second, we note that Naïve buys took longer to identify attacks (the last column), so Decision Tree was more efficient for cyber security in CAVs.

In addition, due to the distinctive characteristics of CAVs, the false positive attack rating rate (FP) is also an important metric for evaluating the performance of models. In a real-world environment, the consequences can be serious if the machine learning model classifies the attack data as ordinary data. Based on this, table 4 shows the false positive rate FP.

It can be seen that with 10-folds cross validation, all types of attacks have been analyzed and trained. The false positive rate of both models in the test dataset is similar and achieves good accuracy.

Based on these results, a false positive rate is acceptable for both models.

Table 4: false positive rate for J48 and Naive buys

Table 4: False positive rate for J48 and Naive byes

	TP Rate on the Testing Data Set	**FP Rate on the Testing Data Set**	**Precision on Testing Data Set**
Naïve Byes	81.1%	22.5%	85.8%
J48	94%	22.2%	93.9%

DOI: https://doi.org/10.54216/IJAACI.060203
Received: November 19, 2023 Revised: December 18, 2023 Accepted: January 01, 2024

By returning the previous results on a reduced data set for KDD99 by 20 percent, the results shown in Table 5 can be obtained

Table 5: False positive rate for J48 and Naive byes

	TP Rate on the Testing Data Set	FP Rate on the Testing Data Set	Precision on Testing Data Set	Time to build the model
Naïve Byes	96.6%	3.8%	96.7%	0.19
J48	98.3%	1.8%	98.3%	1.58

Table 6: Results for each type of attack

	DT FP Rate	NB FP Rate	DT accuracy	NB accuracy
PROBE	0.18%	0.81%	98.3%	92.7%
DoS	0.4%	1.06%	99.6%	89.6%
R2L	0.18%	1.06%	98.3%	89.6%
U2R	0.4%	1.06%	99.6%	89.6%

From Table 6, it can be seen that both models of machine learning classification have high accuracy. False positive rates were low in all attack data. When identifying PROBE attacks, DT's excellent performance was better than NB's. When determining DoS attacks, the resolution of the decision tree was much higher. The decision tree model also performed better in U2R and R2L attacks

Based on the previous results, it can be said that the decision tree algorithm achieved better results regarding communication-based attacks in the CAV environment. The decision tree model can detect the attack in a short time with good accuracy. However, it should also be noted that both models have obtained unsatisfactory results when predicting invisible attacks, which needs further studies in future works.

7. Conclusion

CAVs networks are an important topic, and due to their characteristics of wireless connectivity and self-driving, they are vulnerable to various types of attacks. The research demonstrated how artificial intelligence techniques can be used to detect four types of attacks by comparing the Naïve buys and decision tree algorithms. From the results obtained, it turned out that the decision tree algorithm is more accurate in classification. It is possible to study other techniques to detect other types of attacks as well, especially attacks that are invisible to the techniques studied.

References

[1] Guerra, E. Planning for cars that drive themselves: Metropolitan Planning Organizations, regional transportation plans, and autonomous vehicles. J. Plan. Educ. Res. 2016, 36, 210–224.

[2] Gov.UK. Center for Connected and Autonomous Vehicles. 2018. Available online: https://www.gov.uk/government/organisations/centre-for-connected-and-autonomous-vehicles (accessed on 9 December 2018).

[3] Petit, J.; Shladover, S.E. Potential cyberattacks on automated vehicles. IEEE Trans. Intell. Transp. Syst. 2015, 16, 546–556.

[4] He, Q.; Meng, X.; Qu, R. Survey on cyber security of CAV. In Cooperative Positioning and Service (CPGPS); IEEE: Harbin, China, 2017; pp. 351–354.

[5] Integrating Autonomous Vehicle Safety and Security, 2017. Available online: https://www.researchgate.net/publication/321323032_Integrating_Autonmous_Vehicle_Safety_and_Security (accessed on 10March 2022).

[6] Qayyum, A.; Usama, M.; Qadir, J.; Al-Fuqaha, A. Securing Connected Autonomous Vehicles: Challenges Posed by Adversarial Machine Learning and theWay Forward. IEEE Commun. Surv. Tutor. 2020, 22, 998–1026.

[7] Kumar, S.; Singh, K.; Kumar, S.; Kaiwartya, O.; Cao, Y.; Zhou, H. Delimitated Anti Jammer Scheme for Internet of Vehicle: Machine Learning based Security Approach. IEEE Access 2019, 7, 113311–113323.

DOI: https://doi.org/10.54216/IJAACI.060203
Received: November 19, 2023 Revised: December 18, 2023 Accepted: January 01, 2024

[8] Cybersecurity Concerns with Self-Driving and Conventional Vehicles, 2017. Available online: http://umich.edu/~umtriswt/PDF/SWT-2017-3.pdf (accessed on 26 March 2019).

[9] Cyber Security and Space Based Services—ESA Business Applications, 2019 Available online: https://business.esa.int/funding/invitation-to-tender/cyber-security and-space-based-services (accessed on 31 May 2022).

[10] Hall, M.; Frank, E.; Holmes, G.; Pfahringer, B.; Reutemann, P.; Witten, I.H. The WEKA data mining software: An update. ACM SIGKDD Explor. Newsl. 2009, 11, 10–18.

[11] Arockia Panimalar.S, GiriPai.U, Salman Khan.K, ―ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY‖, International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue:03 | Mar-2018, e-ISSN: 2395-0056, p-ISSN: 2395- 0072.

[12] Chung, S. (2021). AI-Based CYBERSECURITY: Benefits and Limitations.]

[13] Ansari, Dash, Sharma, &Yathiraju. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review.

[14] Das, Rammanohar & Sandhane, Raghav. (2021). Artificial Intelligence in Cyber Security. Journal of Physics: Conference Series. 1964. 042072. 10.1088/1742- 6596/1964/4/042072.

[15] Atiku, Shidawa.B., Aaron, Achi.U., Job, Goteng.K., Shittu, Fatima, Yakubu, Ismail.Z. (2020). Survey On The Applications Of Artificial Intelligence In Cyber Security, International Journal of Scientific & Technology Research, 9,10, 165-170.

[16] GOV.UK. The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles. 2017. Available online: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connectedandautomated-vehicles/the-key-principles-of vehicle-cyber-security-for-connected-and-automated-vehicles (accessed on 6 August 2022).

[17] The Pathway to Driverless Cars Summary Report and Action Plan. 2018. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uplods/attachment_data/file/401562/pathway-driverless-cars-summary.pdf (accessed on 6 August 2022).

[18] Parkinson, S.; Ward, P.; Wilson, K.; Miller, J. Cyber threats facing autonomous and connected vehicles: Future challenges. IEEE Trans. Intell. Transp. Syst. 2017, 18, 2898–2915.

[19] Schatz, D.; Bashroush, R.;Wall, J. Towards a more representative definition of cyber security. J. Digit. Forensics Secur. Law. 2017, 12, 8.

[20] UCI kdd cup 1999 Data Data Set, 1999. Available online:https://archive.ics.uci.edu/ml/datasets (accessed on 1 June 2022).

[21] Arora, I.S.; Bhatia, G.K.; Singh, A.P. Comparative Analysis of Classification Algorithms on KDD'99 Data Set. Int. J. Comput. Netw. Inf. Secur. 2016, 8, 34.

[22] Charchekhandra, B. (2023). Align and fusion two thermal and visual images. Pure Mathematics for Theoretical Computer Science, 1(1), 17-31. **DOI:** https://doi.org/10.54216/PMTCS.010102

DOI: https://doi.org/10.54216/IJAACI.060203
Received: November 19, 2023 Revised: December 18, 2023 Accepted: January 01, 2024