DOI: 10.21917/ijct.2023.0427

DETECTION OF CYBER ATTACK ON INTERNET OF VEHICLE COMMUTERS

H.A. Dinesh[1], S. Radha Rammohan[2], A. Jayanthiladevi[3], S. Kamala[4] and Jackson Akpakaro[5]

[1,2,3,4]*Institute of Computer Science and Information Science, Srinivas University, India*

[5]*Department of Mathematics and Computer Science, University of Africa, Nigeria*

Abstract

The Internet of Vehicles (IoV) is a massive interactive network that can be extended into the realm of smart transportation by utilizing IoV at scale because it is capable of attaining unified management. It is well known that the gathered contents not only contain personal information, but also certain critical data, such as a vehicle running parameter, which is strongly related to traffic safety. This study explains how a network intrusion detection system (IDS) based on artificial intelligence can be deployed over various datasets. The simulation is carried out in an extensive way and the results show that the proposed method achieves a higher rate of accuracy in detecting the instances than the other existing methods.

Keywords:

Internet of Vehicles, Intrusion Detection System, Traffic System, Vehicle Commuters

1. INTRODUCTION

The Internet of Vehicles (IoV), also referred to as a massive interactive network, has emerged as a topic of significant interest in the field of mobile internet in recent years [1]. A variety of sensors and other pieces of equipment send data to a central processing system [2], which then processes the information in order to determine the location of cars, as well as their speed and the route they have taken [3]. After the vehicle data has been processed and analyzed, it is anticipated that there will be a large potential for both scientific value and economic interest [4]. This is the current thinking. IoT can be extended into the realm of smart transportation by utilizing IoV at scale because it is capable of attaining unified management [5].

The road system of a large region can have a major influence on the path that vehicles take when calculating IoV. The exchange of a wide variety of traffic data through IoV helps to facilitate both the intelligent administration of routes and the optimization of such routes [6]. The proliferation of our civilisation has led to a growth in the number of automobiles and roadways, which in turn has resulted in an IoV that encompasses a sizeable amount of the total area of the world. Large volumes of information on a range of topics, including as the characteristics of the vehicles, the present driving circumstances they are in, and the traffic that is surrounding them, are collected by several sensors that are positioned in and around the vehicles [7]. Because of the manner in which the data are reliant on both time and place, it is possible to think of them as having a spatio-temporal structure. Big data of a heterogeneous kind is converging as a result of an ever-increasing number of vehicles collecting data from a range of locations and attributes [8]. Big data of a heterogeneous type converges to have a variety in size, volume, and dimensionality.

With the proliferation and enhancement of IoV, the gathered contents not only contain personal information, such as the real-time position of a vehicle, but also certain critical data, such as a vehicle running parameter, which is strongly related to traffic safety [9]. In addition, the gathered contents contain certain critical data, such as a vehicle running parameter, which is strongly related to traffic safety. This is due to the fact that the gathered contents not only contain the owner personal information, but they also contain the location of the car at any given moment in time. On the other hand, rogue car nodes that have the objective of disrupting the traffic system or stealing data for the purpose of financial gain [10] have the potential to give misleading notifications.

As a consequence of this, the creation of a mechanism to check that the data resource regarding the supplied vehicle contains all of the necessary information is an urgent necessity. There will be an increase in the frequency with which big data is collected between vehicles and application platforms utilizing a range of communication technologies as the Internet of Vehicles (IoV) [11] continues to expand and more big data is used. This will be the case due to the fact that more big data will be used. This, in turn, will result in a rise in the level of sophistication of the attacks on the system security. During the construction of large-scale IoV systems, it is essential to do research into a number of different methods that can protect vast amounts of data.

When employing a system like this, it can be difficult to keep the system secure and to keep information confidential. Sensing, networking, and communication technologies are going to be critically necessary in order to build systems that are totally autonomous and automated [12].

It is common knowledge that the information obtained from the vehicles is collected by sensors connected to the Internet of Things (IoT), which is then sent to the control center through a variety of communication networks. An attack is being carried out against the information that is being transmitted to the command-and-control center from within the communication channel. Attackers will try to trick the command center into believing they have won the war by planting harmful data in the communication network. On the basis of the information that has been obtained, an assessment of the existing circumstance is carried out at the command center [13].

In its most fundamental form, the state estimate technique offers a picture of the situation in which the vehicle is currently functioning. The method for predicting the state of the system yields a graphical representation of the physical system as the end result.

2. RELATED WORKS

We have developed a potentially hazardous dependence on the capabilities of social media platforms to make information easily accessible and immediately available. Computers are now able to store a bigger quantity of information as a direct result of an increase in the amount of data coming into them. As a result of the broad use of workstations, it is now possible to quickly couple information obtained from a variety of sources [8].

The correlation of data received from significant sources has made it much easier to get any additional information that one would be specifically trying to gain. This applies to any information that one would be especially trying to gain. Because of the proliferation of intelligent computers and automated frameworks, unauthorized access to data, as well as tampering with it, has developed into a problem that is much more difficult to manage and poses a greater risk. Extended connectivity not only allows access to data sets that are larger and more diverse than ever before at greater speeds than ever before, but it also provides a right to further enhance the route to the data from nearly anywhere on the framework [9]. Extended connectivity also provides access to larger and more varied data sets at higher speeds than ever before. Extended connectivity not only makes it possible to gain access to data sets that are larger and more diverse, but it also makes it possible to gain access to larger data sets at quicker rates than in the past [10].

The usage of password authentication, which is supposed to be used in order to protect schemas, has frequently and easily been beaten by framework gate crashers. Password authentication is intended to be used in order to protect schemas. The recent worm attack on the internet serves as a good illustration of this point. Threats such as viruses and worms can replicate themselves and spread to other computers in a network without the assistance of a human being at any point in the process. It may be impossible to verify where they initially appeared on the internet or how much damage they caused if they are only utilized on a single computer after they have been released. It has been demonstrated in the past that certain types of malware, known as Trojans, can masquerade as harmless programs when, in reality, they are designed to cause unchecked damage to the system [11]. This is something that can happen because Trojans are deceptive.

A control component for expansion passages serves as the primary barrier in the vast majority of desk-based systems. This threshold indicates whether or not a particular subject is authorized to access a particular article in the system; however, it does not illustrate or restrict the subject capacity to do anything with the article itself once it has been granted access to control it [9]. Once a subject has been granted access to control an item, this threshold indicates whether or not that subject is authorized to access a particular article in the system. Due to the fact that unlawful data flow can occur with the articles themselves, access control does not demonstrate and is unable to prevent the flow of illegal data that is associated with dispatched entries to the articles. In addition, when access controls are not required, the responsibility for the information protection is transferred to the eventual customer. This occurs when access restrictions are unnecessary. Customers are able to more reliably get an understanding for the security tools given by the systems and learn how to achieve the necessary level of security as a result of this ability. The Bell and Lapadula model [10] for providing a riddle and the Biba model [11] for offering trustworthiness are two examples of how models can be used to information streams in order to increase security. Both of these models are given in the next sentence. In order to achieve the highest possible level of convenience, safety must be compromised [12]. Both approaches take a careful approach, and as soon as it is determined that the data held within the structure is both secure and secret, they promptly put a stop to any read or write activities that were in progress.

Deep learning, often known as deep learning, is a method that has been successfully implemented in a wide number of fields, some of which include clinical image processing, natural language creation, speech recognition, and signal detection, to name just a few of these applications. Convolutional neural networks, also known as CNNs, are one type of the deep learning technique that has seen significant application in PC-based applications like as face and article recognition. This methodology makes use of NIDS strategies, all of which are founded on the detection of anomalies [13]. Convolutional neural networks, also known as CNNs, have been proved to be one of the most successful types of the deep learning technique, particularly when it comes to computer vision tasks such as the detection of faces and objects. The convolutional neural network, or CNN for short, is a type of neural network that possesses the capacity to learn accurate representations of the component components of the input being processed. There are a few key differences between MLPs and CNNs, the most significant of which are the weight distribution and the size of the pool.

3. PROPOSED CYBER DETECTION MODEL

It is vital to note that the precision and accuracy of the measurements, in addition to the sensors, play a key part in the process of evaluating the present condition of the vehicle. This is something that should be kept in mind at all times. The data required for the measures is gathered by the sensors that have been installed; nevertheless, these devices are susceptible to being hacked or failing for a variety of reasons. In addition to causing financial losses, preventing travel, and causing social problems, this might also raise worries about the nation security.

After the necessary safety measures have been taken, one of the most difficult parts of maintaining the resilient operation of an IoV-based automobile is the identification and mitigation of attacks. This is one of the areas that poses the greatest challenge.

The most trustworthy algorithm for predicting the state of a vehicle in the presence of IoV sensing information that is also resistant to cyberattacks, and what is the most reliable control scheme for managing the various states of the system. In the course of this research, these are the topics that will be investigated in further depth.

The primary focus is placed on the creation of reliable algorithms for the state estimation and feedback control of autonomous electric cars that are operating in a networked environment. Specifically, this area of research aims to improve the safety and efficiency of the transportation industry. The possibility of harmful data being added is something that is given special consideration. In order for the attackers to disrupt the command-and-control server, they inject these malicious packets of data into the network of the victim.

According to the findings of this research, one strategy for improving the classification accuracy of CPS cyberattacks is to make use of the DL model in conjunction with the activation function. This is one of the ways to improve classification accuracy. The approach that is being proposed involves monitoring the behavior of the system in order to identify intrusions at the physical layer.

The Fig.1 is a representation of a thorough approach that a deep hybrid model for the detection of cyberattacks. The process of validating a model requires the creation of a training dataset in addition to a test dataset. Both of these datasets are required.

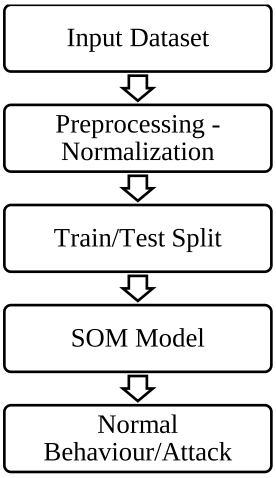

Fig.1. Flowchart of the proposed approach

Assume that the data used for training includes N IoVs, and that the sensor data on failures arrives as a multivariate time series. Every single piece of technology has a plethora of sensors built into it. The time of failure T_n, is represented in the data from each individual device in the following format:

$$x_n = [x_1,x_2,...,xT_n] \in R_m \times T_n \, (n=1,\ldots,N) \qquad (1)$$

where T_n - time of failure.

For each and every moment in time t that is seen, the multidimensional vector of sensor readings is formed using the formula:

$$x_t = [\omega_{1t}, \omega_{2t},...,\omega_{mt}] \in R_{m\times 1} \, (t=1,T_n), \qquad (2)$$

The feature vector that was input goes through preprocessing before any additional analysis is performed. At time t, the x_t sensor of dimension m sends the data to the SOM model so that it can be processed. The model will then determine whether or not the data represent behavior that is typical for the system or whether they represent an attack.

After the DL model has been adequately trained, it can be utilized to make predictions on data sets for which it has not been trained. These data sets include those that are new to the model. The so-called trained model is utilized offline throughout the training phase, and then afterwards it is used online to detect a wide variety of threats of varying types.

The simulated attacks are divided in four major categories:

- *Denial of Service Attack (DoS)*: A denial-of-service attack, often known as a DoS attack, occurs when the perpetrator prevents authorized users from accessing a system or causes the system processing capability or memory to become overburdened with valid demands.
- *User to Root attack (U2R)*: When an adversary has access to a typical client description of the scheme that is being targeted, they are able to carry out what is known as a user-to-root attack, which is a type of attack that can compromise the entire system.
- *Remote to Local attack (R2L)*: When an attacker is able to deliver packages to a mechanism via a framework but does not have a record of the mechanism exploiting some exposure to acquire local access as a user of that engine, the attacker has successfully carried out a remote-to-local attack. The remote-to-local attack can be carried out successfully by an attacker. This suggests that the attacker is able to deliver packets to a mechanism in some way.
- *Probing Attack*: A probing attack is a type of attack that involves making an attempt to evade the safety safeguards that are built into a system. This form of attack requires the perpetrator to coordinate their actions across a large number of machines in order to achieve their goal.

3.1 SOM DETECTION

The initial phase of the SOM information control procedure begins with the presentation of the mode weight vectors in a format of irregular quality. After the SOM has made its appearance, the method of departure by steps is utilized to locate it so that it can be examined. Construct a vector using the training data x, and it is the output to the map in response to a periodic request.

3.1.1 Distance Measure:

Determine the distance between the statistical vector and the separation wall of the SOM in order to acquire an accurate measurement of equivalence. This is important in order to achieve an accurate reading of equivalence. The Euclidean distance is a common criterion that is used when determining the location of a border. The algorithm can be decomposed into the following steps:

$$d_{ij} = \sqrt{\left(x_1 - w_{1ij}\right)^2 + \ldots + \left(x_2 - w_{nij}\right)^2} \qquad (1)$$

where

d_{ij} - neuron partition

$x(n)$ - neuron decision

w_{ij} - SOM give up layer,

i and j - vector organize on the map.

$d(k_1,k_2)$ - The winning SOM neuron, where k_1 and k_2 are indices of the winning neuron. This neuron is the one that has a base partition to the data neuron.

$$d(k_1,k_2) = m_i n_{i,j} d_{ij} \qquad (2)$$

3.1.2 Update Rule:

The next phase, which takes place after the identification of the component that gives the best match, is to adjust the state of the winning neuron in such a way that it more closely resembles that of the data neuron. This stage takes place after the identification of the component that provides the best match.

$$w_{ij}(t+1) = w_{ij}(t) + \alpha(t)/h(\rho,t)(X_1(t)\text{-}w_{ij}(t)) \qquad (3)$$

where

$\alpha(t)$ - tempo boundary.

One other example would be the fact that $h(\rho, t)$ identifies the location of the minimal value in the area. In order to solve this problem, you will need to utilize the equation

$$h(\rho,t) = \exp\left(\frac{\frac{\rho^2}{\sigma_t^2}}{\frac{1-2\sigma_t^2}{2\rho^2}}\right) \qquad (4)$$

where

ρ^2 - Euclidean distance

σ - range.

3.2 SOM ALGORITHM

The SOM process is challenging to implement when there is no character present. Additionally, it is possible that it will be required in the majority of instances. The direct node verification can be completed in a short amount of time. The SOM has shown itself to be a reliable instrument for the processing, analysis, and collecting of mental image data as a result of these qualities. Following this train of thought leads to the conclusion that the SOM is as follows:

- *Initial Stage*: Utilizing the data vectors at this point allows for the neurons in the map to be assigned a beginning position that is completely at random.
- Data Normalization: In order to present a more convincing illustration of the differences between the groups, it is required to normalize the data. The extent method, which entails normalizing the complete illumination vector such that it is somewhere inside the range [0, 1], is the one that we will use for the most majority of calculations.
- *SOM Training*: SOM training, which entails selecting an information vector x at random from a data collection. We are able to determine a BMU inside the guide that serves as the best possible match for this data vector by making use of the metric that was produced as a result of the analysis.

$$||x-m_c||=\min_i\{\|x-m_c\|\}|| \qquad (5)$$

where mc - reference vector.

- *Change Step*: In this step, the reference vectors for BMU and the surrounding area are adjusted in line with the following:

$$m_i(t+1)=\{m_i(t)+\alpha(t).h_{ci}(t).[x(t)\text{-}m_i(t),i\in N_c(t)\ m_i(t),\ i\in N_c(t) \qquad (6)$$

where

$h_{ci}(t)$ - neighborhood function

c - winner neuron and

t - time.

$x(t)$ - information vector

$\alpha(t)$ - learning rate

$N_c(t)$ - area.

The mathematical statement that is unusual in terms of its extent reflects the progress around it are making toward the information vector. The internal organization of the guide was largely influenced by this alteration, which brought it into alignment with the information vector structure.

- *Data Visualization*: The results of steps three and four will stay the same for an amount of time that is equivalent to the number of years or trials that you select. After the completion of all of the possible routes, the guide will then reveal themselves to the random distribution of the data set. The amount of clusters that are repeated can be discovered in this location. As a result of running the SOM, one ends up with a set of reference vectors that are able to be irrevocably linked to the guide units. These guidelines are collected into a single document that is referred to as a codebook. In order for us to identify the clusters as well as the outliers that were found by the SOM, it is important for us to go back and look at the codebook. The strategy known as the U-Matrix is the one that is utilized over here in this location the substantial majority of the time.

4. RESULTS AND DISCUSSION

There are a total of 494,020 records available within the 10% KDD data set that can be used to train the preparation engine. These records can be used in a variety of ways. These files include information that is unrelated to attacks, in addition to details regarding four unique forms of attacks (DoS, Probe, U2R, and R2L). DoS stands for denial of service, Probe for obtaining information, U2R and R2L stand for user to server. In each of the trials, the standard minutes (the amount of time spent not being attacked) as well as the relevant statistics were used. In this particular instance, a non-standard record type is chosen to be used as opposed to the testing that was done in the past, which made use of the different sorts of evidence that were readily available.

The development of cybersecure nodes is represented in the diagram that is given with this article. After then, a mechanism known as clustering can be used to collect the nodes that were used in an intrusion attack. The utilization of cluster mapping makes it possible to carry out precise grouping of the data. If you so choose, the area that will be selected can have a red circle superimposed over it before the selection is made. Using colors like yellow, red, and green, it is feasible to visually discern between the various cluster grouping components. This is possible because to the use of color.

The nodes of cyberattacks are displayed in a confusion matrix further up. It is possible to utilize a method known as a confusion matrix to express odd predictions and test outcomes and then compare these to the standards that have been set. Uncertainty matrices can be useful in a variety of applications of artificial intelligence, including data analysis, data mining, and other types of machine learning models. (AI). Both error matrix and uncertainty matrix mean the same thing and can be substituted for one another without any loss of meaning.

The diagram that has been shown here illustrates how long it takes to travel between the cyber nodes and the calculated distance between them. The amount of heat that is transported between two consecutive nodes in a stationary wave is equivalent to one-half of a wavelength. Because of this, the space that exists between a node and the anti-node that follows it is equal to a quarter of a wavelength. This is the distance that exists between the two.

The rationale that was offered in the introduction for the production of the graph that is located in Figure 6 is repeated here. You can find it at the bottom of the page. The procedures for training and evaluating are completely identical. The only important distinction between the two is that indicator variables are utilized for the pre-processing of data while conditional probability is employed for the post-processing of data. The only other significant difference is that conditional probability is utilized for the post-processing of data. The number of people who will be trained will be 10 percent higher than the total number of people who will be tested.

The data is dispersed across the 30x30-dimensional space that was selected as the dataset for SOM training when the input is preprocessed using conditional probability and then given to SOM. This makes it possible for SOM to learn from its errors in a more efficient manner.

Table.1. Experimental Testing Datasets

Type	Experiment	Number	Number
All Attacks	1	65,593	401,195
DOS	2	92,874	280,504
Probing	3	92,827	4107
U2R	4	92,873	188
R2L	5	92,877	1126

Table.2. Results of Experiment 1 and 2

Test	TN	TP	FN	FP	DR	CR
All attacks	96.90	87.77	0.95	10.08	87.77	92.34
DOS	96.90	97.22	0.95	0.63	97.22	97.06
Probing	96.90	55.92	0.95	41.93	55.92	76.41
U2R	96.90	0.00	0.95	97.85	0.00	48.45
R2L	96.90	0.00	0.95	97.85	0.00	48.45

Table.3. Results of Experiment 3 and 4

Test	TN	TP	FN	FP	DR	CR
All attacks	98.42	64.72	0.40	34.09	64.72	81.57
DOS	98.42	98.06	0.40	0.75	98.06	98.24
Probing	98.42	17.52	0.40	81.29	17.52	57.97
U2R	98.42	0.00	0.40	98.81	0.00	49.21
R2L	98.42	0.00	0.40	98.81	0.00	49.21

Table.4. Results of Experiment 4

Test	TN	TP	FN	FP	DR	CR
All attacks	97.26	69.47	0.59	28.38	69.47	83.37
DOS	97.26	68.79	0.59	29.06	68.79	83.02
Probing	97.26	80.14	0.59	17.71	80.14	88.70
U2R	97.26	89.53	0.59	8.32	89.53	93.40
R2L	97.26	60.18	0.59	37.67	60.18	78.72

Table.5. Results of Experiment 5

Test	TN	TP	FN	FP	DR	CR
All attacks	97.55	74.85	0.29	22.99	74.85	86.20
DOS	97.55	0.02	0.29	97.83	0.02	48.79
Probing	97.55	70.06	0.29	27.79	70.06	83.81
U2R	97.55	91.00	0.29	6.85	91.00	94.28
R2L	97.55	60.18	0.29	37.67	60.18	78.86

Table.2. Comparative Analysis

Attack	Method						
	SVM	**FFNN**	**LSTM**	**BPNN**	**DNN**	**CNN**	**SOM**
All attacks	0.795	0.500	0.977	0.977	0.977	0.972	0.902
DOS	0.907	0.978	0.338	0.977	0.978	0.966	0.496
Probing	0.905	0.574	0.932	0.904	0.932	0.912	0.876
U2R	0.589	0.978	0.958	0.976	0.977	0.946	0.741
R2L	0.912	**0.912**	0.963	0.983	0.981	0.944	0.982

From the results of Table.1 – Table.5, the values have processing all of the neurons that are being input, the graph will then exhibit each output neuron in turn. Using the Euclidean distance formula, the positioning of each output neuron is presented, and the input neuron that is indicated for placement of the output neuron is the one that is considered to be the closest to the output neuron.

If the result that SOM provides for the output neuron matches with the value of the real neuron, then the output neuron is not displayed and instead receives the same yellow or red color as the input neuron to which it was mapped. This occurs only if the value of the actual neuron is equal to the result that SOM offers for the output neuron.

The output neuron can be colored the same as the input neuron. False positive connections occur when a regular connection neuron is supplied to the map, but it is triggered by SOM as an attack connection neuron. This causes the map to interpret the neuron as being part of an attack connection. Because of this, a false positive association is established.

When an attack link is sent to the map, but the SOM wrongly perceives it as a normal connection, a connection of this sort is formed. Those connections are referred to as undecided since the SOM is not be able to choose which neuron will act as their output.

5. CONCLUSION

This study explains how a network intrusion detection system (IDS) based on artificial intelligence can be deployed by applying a range of different adaptive approaches, as are demonstrated throughout the course of the study. The research reveals the significant effects that were brought about by the alterations that were made to the characteristics of the dataset. It is highly unlikely that it will perform as well as SOM, which makes use of unsupervised learning. It has been demonstrated that the CNN algorithm performs significantly better than a considerable number of alternative neural network-based calculations. The effect of an adjustment in the provisional probability if an attack is identified by SOM has the same magnitude as the effect of a change in pointer variables. Given that there are already two classes, normal and abnormal, the conditional probability transformation cuts the number of typical characteristics down to two by replacing each typical characteristic with two attributes. This results in a total reduction in the number of typical characteristics from four to two. This has the consequence of narrowing the scope of the features that are considered to be typical. It is essential that there be a reduction in the total number of false positives if the project is to be successful.

REFERENCES

[1] S. Wasserman and K. Faust, “Social Network Analysis: Methods and Applications”, *Cambridge University Press*, 1994.

[2] K. Praghash and T. Karthikeyan, “Data Privacy Preservation and Trade-off Balance Between Privacy and Utility using Deep Adaptive Clustering and Elliptic Curve Digital Signature Algorithm”, *Wireless Personal Communications*, Vol. 78, 1-16, 2021.

[3] N.V. Kousik, M. Sivaram and R. Mahaveerakannan, “Improved Density-Based Learning to Cluster for User Web Log in Data Mining”, *Proceedings of International Conference on Inventive Computation and Information Technologies*, pp. 813-830, 2021.

[4] G. Dhiman, A.V. Kumar, R. Nirmalan and S. Sujitha, “Multi-Modal Active Learning with Deep Reinforcement Learning for Target Feature Extraction in Multi-Media Image Processing Applications”, *Multimedia Tools and Applications*, Vol. 23, pp. 1-25, 2022.

[5] V. Saravanan and A. Neeraja, “Security Issues in Computer Networks and Stegnography”, *Proceedings of International Conference on Intelligent Systems and Control*, pp. 363-366, 2013.

[6] B. Zou, “Cyber Resilience of Autonomous Mobility Systems: Cyber-Attacks and Resilience-Enhancing Strategies”, *Journal of Transportation Security*, Vol. 2021, 1-19, 2021.

[7] L. Yang and A. Shami, “A Transfer Learning and Optimized CNN based Intrusion Detection System for Internet of Vehicles”, *Proceedings of IEEE International Conference on Communications*, pp. 2774-2779, 2022.

[8] V. Saravanan and P. Jayashree, “Security Issues in Protecting Computers and Maintenance”, *Journal of Global Research in Computer Science*, Vol. 4, No. 1, pp. 55-58, 2013.

[9] S. Ullah and W.J. Buchanan, “HDL-IDS: A Hybrid Deep Learning Architecture for Intrusion Detection in the Internet of Vehicles”, *Sensors*, Vol. 22, No. 4, pp. 1340-1354, 2022.

[10] A. Zacharaki and D. Tzovaras, “Complex Engineering Systems as an Enabler for Security in Internet of Vehicles: The nIoVe Approach”, *Proceedings of International Conference on Societal Automation*, pp. 1-8, 2019.

[11] M.M. Moussa and L. Alazzawi, “Cyber Attacks Detection based on Deep Learning for Cloud-Dew Computing in Automotive IoT Applications”, *Proceedings of IEEE International Conference on Smart Cloud*, pp. 55-61, 2020.

[12] M. Elsisi and M.Q. Tran, “Development of an IoT Architecture based on a Deep Neural Network against Cyber Attacks for Automated Guided Vehicles”, *Sensors*, Vol. 21, No. 24, pp. 8467-8474, 2021.

[13] A. Castiglione, “Securing the Internet of Vehicles through Lightweight Block Ciphers”, *Pattern Recognition Letters*, Vol. 135, pp. 264-270, 2020.