e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 13, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

Efficient Detection of Sensor Attacks in Independent Vehicles Using Ai Approach

S.Rathika[1], A.Keerthana[2], V.Preethi[3], T.Haritha[4], Dr.A.V.Santhosh Babu[5]

Student, Dept. of I.T, Vivekanandha College of Engineering, for Women (Autonomous), Tiruchengode, Tamil Nadu, India[1,2,3]

Assistant Professor, Dept. of I.T, Vivekanandha College of Engineering, for Women (Autonomous), Tiruchengode, Tamil Nadu, India[4]

Professor, Dept. of I.T, Vivekanandha College of Engineering for Women (Autonomous), Tiruchengode, Tamil Nadu, India[5]

ABSTRACT: Intelligent vehicles will evolve more autonomous as they become more digital and networked. However, they are also growing increasingly vulnerable to cyber-threats, which are going to become a greater worry. Using a deep learning methodology, this research provides a sensor-based attack detection system for autonomous vehicles. Global Positioning System (GPS) and Light Detection and Ranging (LiDAR) sensor attacks are investigated in this work. Moreover, deep learning approach is enriched with auto encoder neural network to reduce the dimensionality of the Safety Pilot Model Deployment Data (SPMD) dataset. Once the dimensionality is reduced, the reduced feature set is given as input to classification model. Feed forward neural network act as classifier which outputs two classes: normal and attack. Also, dropout is added in classification model to prevent overfitting of the model. Finally, the performance of proposed work is evaluated in terms of accuracy, training and validation loss

KEYWORDS:

I. INTRODUCTION

In the recent years, Automobile Industries compete with each other to launch the first fully autonomous vehicle. In future we will see lot of self-driving cars around the world. Many companies like GM, Ford, Toyota, Tesla, etc. are taking test drives in recent years. Many Automobile industries have invested for developing Autonomous Vehicle [1]. An autonomous vehicle or a driverless vehicle is one that is able to operate itself and perform necessary functions without any human intervention, through ability to sense its surroundings.

To enable intelligent transportation, autonomous vehicle systems leverage a variety of sensors, such as GPS, LiDAR, camera, etc., to localize themselves and perceive the environment. This increases the exposure of potential vulnerabilities under malicious cyberattacks. Once under attack, vehicles may perform anomalous behaviors, which would cause disruptive consequences and even catastrophic accidents [2].

Sensors observe the environment in which self-driving cars work, and any attack on them would be disastrous, leading the car to make poor judgments with significant repercussion. Attackers can target any sensor on a self-driving car and try to deceive it by presenting it with skewed data. Stop signs with little graffiti or art stickers, for example, may be difficult for computer vision systems to identify. Fake objects may cause the automobile to halt or slow down needlessly, but eliminating a genuine item may result in an accident. The type, functionality and use of a sensor determines the extent to which it could contribute to scoping out cyber threats, as well as the extent to which it could inform potential implications should it be compromised [3].

Therefore, it is of great significance to develop methodologies for the protection of vehicles against sensor attacks in real-time, which belongs to the domain of cyber-security. Model-based approaches compare the actual measurement with the predicted state based on the system model [4]. This detection structure has been used by conventional model-

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

based approaches and its efficacy has been demonstrated in long term practices. Nonetheless, due to the uncertainties including noise and modeling errors in real applications, stealthy attacks may be ignored by conventional model-based detectors, when the deviation between the measurement and the predicted state caused by the attack is overpowered by the uncertainties. So, this work proposes a deep learning-based approach to detect and identify cyber-attacks imposed on sensors for autonomous vehicles.

The contributions of this work are as follows:

- To analyse detect GPS and LiDAR sensor attacks for autonomous vehicles, a new model based on deep learning by monitoring the GPS and LiDAR measurements.
- To evaluate the efficiency of proposed work, it is evaluated in terms of accuracy, training and validation loss

II. Related Work

Chowdhury et. al. [3] analyzed potential cyber-attacks and their repercussions on self-driving vehicles, as well as their weaknesses, are fully presented in the assaults that have previously attacked self-driving cars. This survey contains latest research on how a self-driving car can maintain resiliency in the face of persistent cyber-attacks. They also suggested new research areas for addressing the security concerns raised by self-driving automobiles.
Zhang et. al. [5] proposed a safe vehicle state estimate-based cyber-attack detection technique for autonomous cars, including an example application in the vehicle localization system under attack. The discrepancy between the measurements taken by the onboard sensors and the state estimation is monitored in real time.

Xiong et. al. [6] proposed To simultaneously assault the image and LiDAR perception systems in autonomous vehicles, two multi-source adversarial sample attack models, including the parallel attack model and the fusion attack model, were developed. Adversary samples are generated separately from the original picture and LiDAR data in the parallel attack model. Through comprehensive real-data experiments, they validated proposed to break down the perception systems of autonomous vehicles compared with the state-of-the-art.

Farivar et. al. [7] introduced the idea of a clandestine attack against autonomous vehicles that could risk passenger safety. They also devised a stealth attack against autonomous vehicles' lane- keeping systems. They reconstructed road curves and compared them to readings using GPS data and offline maps. The proposed models' validity and effectiveness are confirmed by the findings. Changalvala and Malik [8] proposed a novel semi-fragile data hiding-based technique for real- time sensor data integrity verification and tamper detection and localization. Specifically, the proposed method relies on 3-dimensional quantization index modulation (QIM)-based data hiding to insert a binary watermark into the LiDAR data at the sensing layer.

Because it relies on external data, such as GPS and information from cameras, vehicle location measurement is frequently sensitive to deception attempts. As a result, detection and estimate of position sensor deception attacks for local vehicles in a platoon should be addressed. To address this issue, Ju et al. [9] propose a linearized model to describe the longitudinal dynamics of a local vehicle. Based on analysis results, simulations are conducted to verify the effectiveness of the proposed attack detection and estimation scheme.

He et. al. [10] collected a large set of potential cyber attacks are and investigated from the aspects of target assets, risks, and consequences. Severity of each type of attacks is then analysed based on clearly defined new set of criteria. The levels of severity for the attacks can be categorized as critical, important, moderate, and minor. Mitigation methods including prevention, reduction, transference, acceptance, and contingency are then suggested. It is found that remote control, fake vision on cameras, hidden objects to LiDAR and Radar, spoofing attack to GNSS, and fake identity in cloud authority are the most dangerous and of the highest vulnerabilities in CAV cyber security.

III. Methodology

This section goes over the specifics of a proposed project. After the entire feature set has been extracted, an autoencoder neural network is used to decrease it. The classifier uses the reduced feature set as input to conduct binary classification. Figure 1 illustrates the architecture of proposed work.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

The dataset used is from the Research Data Exchange (RDE) archive for the Safety Pilot Model Deployment (SPMD). Since there is no anomalous dataset available in real-time and anomalous values are injected into the dataset.

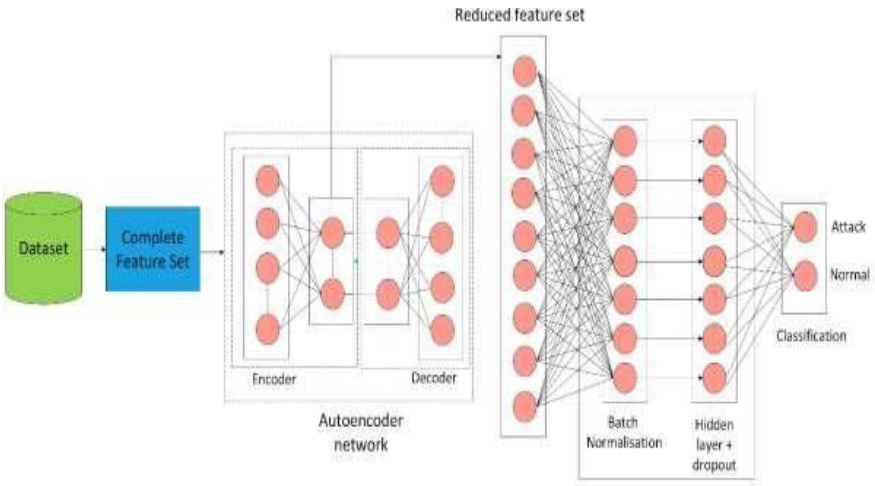

Figure 1: Architecture of proposed work

This data contains high dimensional features and it should be reduced first using by choosing only significant features. So, initially the dimensionality reduction is carried using autoencoder network and then reduced feature set from this module is given as input to classification model.

False data injection (FDI) is detected in this work. In a FDI attack, the attacker injects malicious measurements to replace normal sensor outputs, in order to compromise the closed-loop control system. In autonomous driving applications, the position measurement may be biased to another lane by a FDI attack.
In real applications, the position and orientation of the vehicle can be observed by sensors, such as GPS, LiDAR, IMU, camera, etc, which are corrupted with noise. Thus, the measurement equation can be given as,

As GPS and LiDAR are vulnerable to these FDI attack, anomalous measurements may occur. Consequently, the following modified measurement equation is given to describe the sensor observation under attack.

A. Dimensionality reduction

Dimensionality reduction is a technique for reducing a model's complexity and avoiding overfitting. A neural network architecture called an autoencoder (AE) is used to learn new features. The fact that the AE training procedure can be done without supervision is one of its defining features. Following that, a sequence of transformations connects the initial feature representation to a new feature space, and the autoencoder's quality is assessed by inspecting the rebuilt data for accuracy. The weights can be modified repeatedly using the computed error until the desired performance is attained. AEs are neural networks with at least one hidden layer and two subnets: an encoder subnet and a decoder subnet. This reduced feature set from autoencoder is forwarded to classification model.

B. Classification

The core deep neural network design of the classifier is a feedforward neural network architecture, with primary layers depicted in Figure 1 and full explanations below:

C. Input layer

This is the beginning point for the complete neural network, and it consists of numerous nodes equal to the number of features in the dataset in question.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

D. Batch normalization layer

This layer, which comes before each dense hidden layer, improves the training phase of the neural network by raising the training velocity and allowing for the adoption of higher learning rates as well as the saturation of any nonlinearities. Because of the robust gradient propagation within the deep neural network, this usually results in improved accuracy on both validation and test sets.

E. Hidden layers

These are a variable number of thick layers made up of artificial perceptrons (MLP) that output a weighted sum of their inputs after being processed by an appropriate activation function. The entire neural network is made up of at least five densely coupled layers of perceptrons.

F. Dropout layer

This layer is closely connected to and immediately follows the one preceding it. Many copies of the triple batch normalization layer-dense hidden layer-dropout layer were made. By shutting off a Bernoulli probability distribution function at random several neurons in the linked dense layer, the dropout layer avoids overfitting.

G. Output layer

It consists of a number of nodes that correspond to the number of classes and offers the final classification. Here, the binary classification is performed and if the anomalous readings is detected by the model, then classifier classifies the output to be „attack" or else to be „normal". Sigmoid is an activation function used in this layer.

Results and Discussion

The performance of proposed is evaluated using following metric:

(i) Accuracy

(ii) Training and validation loss

The following Table 1 denotes the hyperparameters of the proposed model.

Table 1: Hyperparameters and its value

Hyperparameters	Value
Batch size	256
Activation function	Sigmoid
Dropout	0.1
Optimizer	SDG
Learning rate	0.01

Table 2: Performance of classifier vs. number of features

Features	Accuracy		
	PCA	AE 3 layers	AE 9 layers
50	0.992	0.994	0.995
40	0.990	0.989	0.992
30	0.993	0.991	0.994
20	0.993	0.992	0.994
10	0.995	0.994	0.997

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

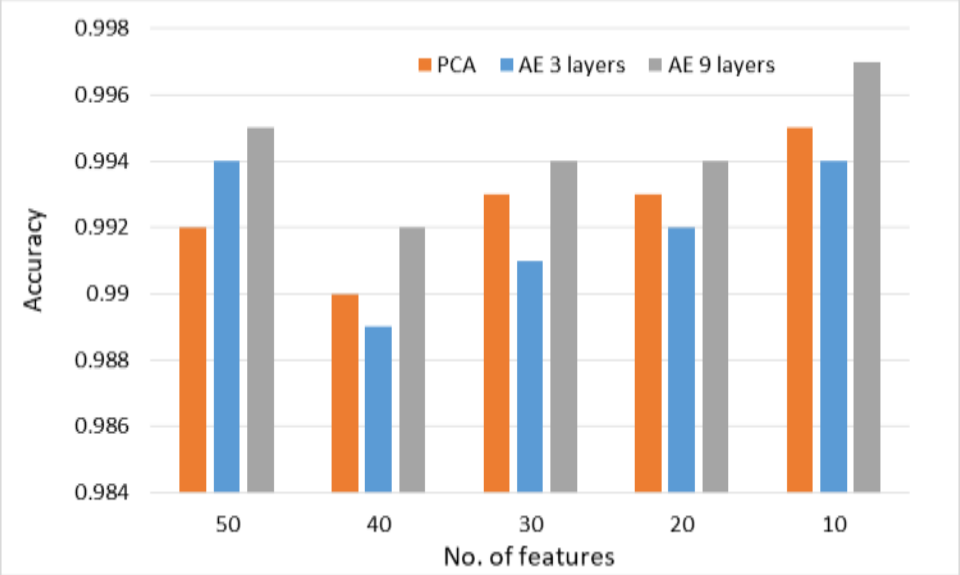

Figure 2: PCA and autoencoders improve classifier performance when the amount of features is altered

Table 2 shows the accuracy for a varied number of features obtained using PCA, an autoencoder with three layers (AE 3layers), and a nine-layer autoencoder (AE 9layers) for binary classification. For both PCA and AE 9layers, the accuracy remains rather consistent as the number of features is reduced, with high values of 99.5 percent and 99.7%, respectively, when the number of features is 10 which is shown in Figure 2. This might mean that initial features could be removed or integrated into more important ones without affecting overall performance.

Table 3: Training and validation loss for proposed work

epochs	Training loss	Validationloss
0	0	0
10	0.58	0.55
20	0.55	0.53
30	0.53	0.51
40	0.52	0.49
50	0.51	0.48
60	0.48	0.46
70	0.5	0.48
80	0.55	0.53
90	0.53	0.52
100	0.52	0.5

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

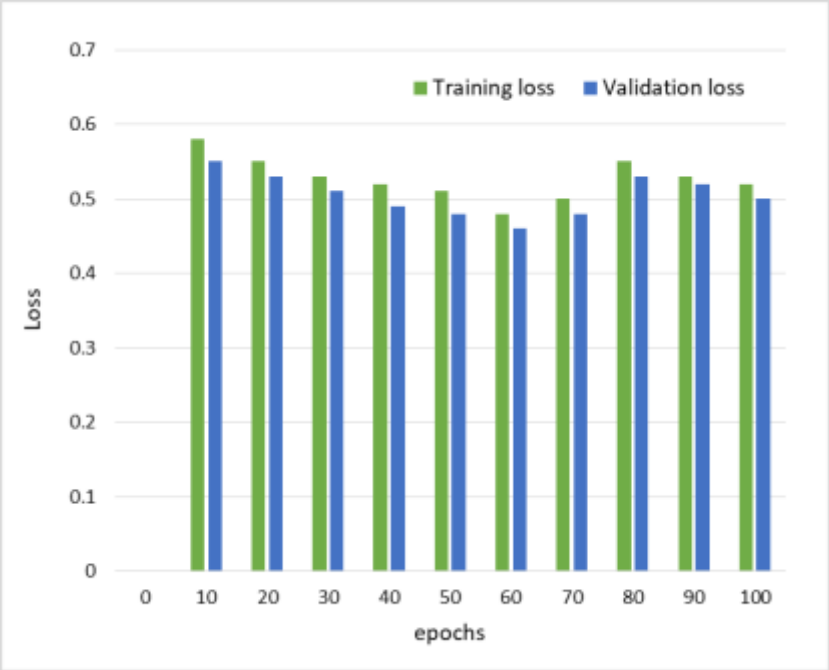

Figure 3: Training and validation loss for proposed work

IV. CONCLUSION

In this work, deep learning based model has been proposed to detect sensor based attacks in autonomous vehicle. By introducing autoencoder network before classification, reduced feature set is obtained which reduces high dimensionality of the dataset. FDI attack has been detected using this proposed work. Experimental results demonstrated the efficiency of the proposed work in terms of accuracy, training and validation loss. In future, other attack types such as DoS, stealthy and replay attacks will be identified to ensure the safety of the vehicle.

REFERENCES

1. Devi, S, Malarvezhi, P, Dayana, R & Vadivukkarasi, K 2020, „A comprehensive survey on autonomous driving cars: A perspective view", Wireless Personal Communications, vol.114, no.3, pp. 2121-2133.
2. Wang, Y., Liu, Q., Mihankhah, E., Lv, C., & Wang, D. (2021). Detection and isolation of sensor attacks for autonomous vehicles: Framework, algorithms, and validation. IEEE Transactions on Intelligent Transportation Systems, 1-13. https://doi.org/10.1109/tits.2021.3077015
3. Chowdhury, A, Karmakar, G, Kamruzzaman, J, Jolfaei, A & Das, R 2020, „Attacks on Self- Driving Cars and Their Countermeasures: A Survey", IEEE Access, vol. 8, pp. 207308-207342.
4. F. van Wyk, Y. Wang, A. Khojandi, and N. Masoud, "Real-time sensor anomaly detection and identification in automated vehicles," IEEE Trans. Intell. Transp. Syst., vol. 21, no. 3, pp. 1264– 1276, Mar. 2020.
5. Zhang, J, Lou, Y, Wang, J, Wu, K, Lu, K & Jia, X 2021, „Evaluating adversarial attacks on driving safety in vision-based autonomous vehicles", IEEE Internet of Things Journal, pp.1-1.
6. Xiong, Z, Xu, H, Li, W & Cai, Z 2021, „Multi-Source Adversarial Sample Attack on Autonomous Vehicles", in IEEE Transactions on Vehicular Technology, vol. 70, no. 3, pp. 2822- 2835.
7. Farivar, F, Haghighi, MS, Jolfaei, A & Wen, S 2021, „Covert Attacks Through Adversarial Learning: Study of Lane Keeping Attacks on the Safety of Autonomous Vehicles", in IEEE/ASME Transactions on Mechatronics, vol. 26, no. 3, pp. 1350-1357.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

8. Changalvala, R & Malik, H 2019, „LiDAR Data Integrity Verification for Autonomous Vehicle", in IEEE Access, vol. 7, pp. 138018-138031.
9. Ju, Z, Zhang, H & Tan, Y 2020, „Deception Attack Detection and Estimation for a Local Vehicle in Vehicle Platooning Based on a Modified UFIR Estimator", in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 3693-3705.
10. He, Q, Meng, X & Qu, R 2020, „Towards a severity assessment method for potential cyber- attacks to connected and autonomous vehicles", Journal of Advanced Transportation,1-15.
11. Chatrath, SK 2021, 'Behavioral Analysis Of Customer Through Customer Review And Profile Using Chi-Square Method', International Journal of Pharmaceutical Research, vol. 13, no. 1, pp. 4341-4349. https://doi.org/10.31838/ijpr/2021.13.01.661
12. Chatrath, SK, Kaur, A & Singh, H 2021, 'Effect of Overtime and Work Load Balance on the Well–Being of Nurses', PalArch's Journal of Archaeology of Egypt/ Egyptology, vol. 18, no. 7, pp. 550-571. <https://archives.palarch.nl/index.php/jae/article/view/7768/7297.
13. Chatrath, SK, Kaur, A, Srivastav, S & Batool, SA 2020, 'A Study on Life and Struggle of Covid-
14. 19 Warriors', Psychology and Education, vol. 57, no. 9, pp. 4914- 4924. https://doi.org/10.17762/pae.v57i9.1924
15. Chatrath, SK, Kaur, A & Singh, H 2020, 'A comparative Analysis Regarding Testing the Awareness about Black Friday among Indian and Australian Customers', Systematic Reviews in Pharmacy, vol. 11, no. 12, pp. 2118-2127. https://doi.org/10.31838/srp.2020.12.324
16. Chatrath, SK, Kaur, A & Singh, H 2020, 'Study On Impact Of Social Networking Sites On The Performance Of employees In The Banking Sector', International Journal of Pharmaceutical Research, vol. 12, no. 4, pp. 4377-4390. https://doi.org/10.31838/ijpr/2020.12.04.599
17. Santhosh Babu A V, Meenakshi Devi P & Sharmila B 2018, 'Efficient enhanced Intrusion identification and response system for MANETs', International Journal of Business Information Systems, (E ISSN No: 1746-0980), vol. 29, no. 4, pp. 535-546.
18. RG Journal Impact: 0.72 - SCOPUS Indexed Journal, Google Scholar Indexed
19. A Journal Indexed in Scopus (Elsevier) DOI NUMBER: 10.1504/IJBIS.2018.096036
20. Santhosh Babu A V & Meenakshi Devi P 2015, 'Energy aware Intrusion Detection System for MANETs', International Journal of Applied Engineering Research, (E ISSN No: 0973-4562), vol. 10, no. 29, pp. 22300-22304.SCOPUS Indexed Journal, Google Scholar Indexed
21. Santhosh Babu A V & Meenakshi Devi P 2017, 'Gene Populated Spectral Clustering for Energy Efficient Multiple Intrusion Detection and Responsive Mechanism for MANET' Journal of Electrical Engineering, (P ISSN No: 1582-4594), vol. 17, no. 4, pp. 1-13. Journal Impact Factor: 0.78 - COSMOS Indexed Journal
22. Santhosh Babu A V & Meenakshi Devi P 2019, 'Swarm Optimized Energy Hubness Clustering to Detect And Respond Intrusive Attack Variants in MANET', International Journal of Business Innovation and Research, (E ISSN No: 1751-0260), vol. 18, no. 3, pp. 369-391.
23. RG Journal Impact: 0.64 - SCOPUS Indexed Journal, Google Scholar Indexed
24. A Journal Indexed in Scopus (Elsevier) DOI NUMBER: 10.1504/IJBIR.2019.098253
25. Santhosh Babu A V, Meenakshi Devi P, Sharmila B & Suganya D 2019, 'Performance Analysis on Cluster based Intrusion Detection Techniques for Energy Efficient and Secured Data Communication in MANET', International Journal of Information Systems and Change Management, (E ISSN No: 1479-3121), vol. 11, no. 1, pp. 56-69. RG Journal Impact: 0.53 - SCOPUS Indexed Journal, DOI NUMBER: 10.1504/IJISCM.2019.101649
26. Santhosh Babu A V, Meenakshi Devi P & Sharmila B 2016, 'Comparative Study of MANET Routing Protocols', Asian Journal of Research in Social Sciences and Humanities, (E ISSN No: 2249-7315), vol. 6, no. 6, pp. 1924-1934. Scientific Journal (SJ) Indexed Journal DOI NUMBER: 10.5958/2249-7315.2016.00337.3
27. Birundha K, Harini S, Hemalatha G, Kalaiselvi P & Santhosh Babu A V 2018, 'A New Technique for Secured Authentication with PC Control through SMS', International Journal of Engineering Research in Computer Science and Engineering, (E ISSN No: 2394-2320), vol. 5, no. 3, pp. 445-447. Journal Impact: 4.890 - COSMOS Indexed Journal, Google Scholar Indexed DOI NUMBER: 01.1617/vol5/iss3/pid18246
28. Pavanya U, Ramya M, Surya N & Santhosh Babu A V 2019, 'Protecting Location Privacy for Task Allocation', International Journal of Innovative Research in Information Security, (E ISSN No: 2349-7017), vol. 6, no. 3, pp. 208-214. Journal Impact: 4.34 - Google Scholar DOI NUMBER: 10.26562/IJIRAE.2019.MRIS10084
29. Dr.G.Saravanan, Dr.A.V.Santhosh Babu 2023, Workload prediction for enhancing power efficiency of cloud data centers using optimized self-attention-based progressive generative adversarial network, International Journal of Communication Systems, (Print ISSN:1074-5351), Volume 37, Issue 1 DOI NUMBER: https://doi.org/10.1002/dac.5634
30. Monieesh S, Dr.G.Saravanan, Savitha R, Dhanapal M, Dr.A.V.Santhosh Babu 2023, INFY GEN: Enhancing Network Stability upto Infinity with the Built-in Material Graphene, Journal of Namibian Studies, ISSN: 2197-5523 (online)

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com