iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 10 **Issue:** III **Month of publication:** March 2022

**DOI:** https://doi.org/10.22214/ijraset.2022.40863

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 10 Issue III Mar 2022- Available at www.ijraset.com*

# An Intelligent Data-Driven Model to Secure Intra-Vehicle Communications based on Machine Learning

Dr. R. Poorvadevi[1], Bodala Yaswanth Nikhil[2], Darisi Venkata Sravan Kumar[3]
[1]*Assistant Professor, Department of Computer Science and Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya, SCSVMV [Deemed to be University], Kanchipuram, Tamil Nadu*
[2, 3]*Department of Computer Science and Engineering,Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya, SCSVMV [Deemed to be University], Kanchipuram, Tamil Nadu, India*

***Abstract:*** ***The depend on electric vehicles on either in vehicle or between-vehicle communications can cause big issues in the system. The model is constructed based on an better support vector machine model for difference finding based on the controller area network (CAN) bus protocol. In order to improve the capabilities of the model for fast mischievous attack detection and avoidance, a new optimization algorithm based on social spider (SSO) algorithm is developed which will emphasize the training process at. The model results on the real data sets tell the high performance, consistency hacking in the electric vehicles.***
***Keywords: Electric Vehicle, Intra-Vehicle, Controller-AreaNetworks (CAN Bus), Anomaly Detection, Optimiz.***

## I. INTRODUCTİON

Mainly vehicles are composed of many hardware modules namely called electronic control units (ECUs) controlled by different types of software tools. Sensors fixed in a vehicle will send their data to the ECU, where the data are managed and the requiring orders are sent to the relevant sectors .

A complex software data transfer process may happen through the use of different network protocols such as CAN, LIN, etc . Here CAN bus is the most prevalent one not only in vehicles, but also in medical gadgets, agriculture, etc due to its high ability and promising characteristics. Advantages of the CAN bus ordinary may be briefly named as allowing up to 1Mbps data rate transfer, and it will save the cost and time due to easy witting autoretransmission of delete or old messages and it shows the error. Since CAN bus protocol was create at a time vehicles were almost isolated, this create trouble from security issues in the smart technology.This will encourage the hackers to attack the electric vehicles through the ECU and insert malevolent messages into their systems. In some cyber interruption situations are showed and applied on the electric vehicles to assess their susceptibilities and possible side effects getting in the system .The classification method is advanced for cyber interruption finding the vehicles. A data interruption finding system is developed which can identify the cyber attack based on the CAN bus message occurrence increase or CAN message.It help's the person when the attack has occurs. To avoid or escape from interpution can bus should pass the message to data handling system To stop this type of attackes an algorithm is used in the vechile. So while starting stage it is better to use adavnce ECU in the vechile.

To stop the attackes a firewall is needed for the vehicle to sit between the CAN bus and the connecting system and stop the cyber attack orders to the CAN bus.

## II. EXISTINGSYSTEMS

Intelligent and secure method to prepare the electric vehicles with a powerful difference finding and evading machinery. The proposed method is based on support vector machine and this method to avoid any mischievous performance in the vehicle . To understand the frequency of different messages they use supportvector machine at different orders. In demand to get into the extreme capability of the ideal, a fresh optimization algorithm based on social spideroptimization (SSO) algorithm is planned to modify the SVR setting restrictions, correctly.

Dısadvantages

- But hackers are still able to decode encrypted packets and hack communication between ECU and sensors.
- Sensor communicate with each other using CONTROLLER AREA NETWORK (CAN) protocol.
- Mostly hackers still able to hack the system frequently.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 10 Issue III Mar 2022- Available at www.ijraset.com*

*A. Proposed System*

Proposed work using various machine learning algorithms such as Conventional SVM algorithm, Decision Tree, KNN Algorithm and propose Social Spider Algorithm with SVM by selecting optimal features and evaluating their performance with indices such as HR (Hit Rate), MR (Miss Rate), CR (Correct Rejection Rate) and FR (False Alarm Rate).In propose work to secure CAN bus (electric vehicle communication) is doing enhancement to SVM algorithm by analysing frequency of received packets and if received packets from same device ID has high frequency then SVM mark that records as anomaly and propose SVM performance will be evaluated using above four indices such as HR, FR, MR and CR. In propose SVM to select optimal features from dataset is using SOCIAL SPIDER OPTIMIZATION (SSO) algorithm.

*1) Advantages*

- But mostly hackers are not able to decode encrypted packets and hack communication between ECU and sensors
- dataset is using SOCIAL SPIDER OPTIMIZATION (SSO) algorithm
- Accidents did not take place and they didn't access

*B. Sytem Requirements*

*1) Hardware Requirements*

*a)* Processor - Pentium–III
*b)* Speed – 2.4GHz
*c)* RAM - 512 MB(min)
*d)* Hard Disk - 20 GB
*e)* Floppy Drive - 1.44MB

*2) Software Requirements*

*a)* Operating system - Windows Xp
*b)* coding language – python

*3) Steps And Implementation*

To overcome from this problem author using machine learning algorithms to detect intrusion or anomaly packet received by ECU or sensors. Machine learning algorithms will be trained and model to predict attack based on request frequency received by ECU. All hackers will send packet with high frequency and priority to make ECU busy and to process high priority packets and other genuine sensors request will keep on waiting. To avoid this problem machine learning will build train model with attack class label as 1 when high frequency of packets received with same id or device. If packets receiving in normal mode then class label 0 will be assigned which indicates received packet is normal.

Author using various machine learning algorithms such as Conventional SVM algorithm, Decision Tree, KNN Algorithm and propose Social Spider Algorithm with SVM by selecting optimal features and evaluating their performance with indices such as HR (Hit Rate), MR (Miss Rate), CR (Correct Rejection Rate) and FR (False Alarm Rate).Here HR refers to machine learning metric called TRUE POSITIVE (TP) which means classifier able to predict given record correctly as positive.MR refers to machine learning metric called FALSE NEGATIVE (FN) which means classifier unable to predicted given record correctlyCR refers to machine learning metric called TRUE NEGATIVE (TN) which means classifier able to predict given record correctly as negativeFR refers to machine learning metric called FALSE POSITIVE (FP) which means classifier predicting negative records as positive.

For any classifier whose HR and CR is high then its performance will be consider as better and efficient. In propose work to secure CAN bus (electric vehicle communication) author is doing enhancement to SVM algorithm by analysing frequency of received packets and if received packets from same device ID has high frequency then SVM mark that records as anomaly and propose SVM performance will be evaluated using above four indices such as HR, FR, MR and CR. In propose SVM to select optimal features from dataset author is using SOCIAL SPIDER OPTIMIZATION (SSO) algorithm. In this algorithm dataset features vector will be consider as SPIDERS and fitness will be calculated between all features and features which has high similarity will be consider as related and will have high fitness score and all those high fitness score features will be selected and low fitness features will be removed out.

Comparison between one features to other features will be consider as MALE and FEMALE spiders. After applying SSO algorithm we will have optimal features using which classifier can efficiently predict anomaly from new and old records. To implement this project author using CAN BUS CONTROLLER dataset and below are the dataset examples. I saved this dataset inside 'dataset' folder.

0, 81008449.4467, id3, 0.2, 1.00, 81008456.7515, id9, 0.370002961208173

0, 81008462.011, id5, 0.17304397155148016, 0.874886161240236

0, 81008465.0179, id2, 0.0, 0.7650437326834458, 0.167011072653919620, 81008465.4139, id10,0.37071729639797957 0.0,0.8447834078508285,0.44514720267692903 1,81097085.76, id2, 0.27311659328065624, 0.8500955038906693, 0.15411782622759981, 81097086.3347, id1, 0.8603548622572741, 0.25

In above dataset all bold font names are the dataset column names and all decimal values are the sensor values. In first column we have values 0 which indicates packet is normal and 1 means packet contains attack. Other values are the sensor signal values. We will train all classifier with above dataset.

Whenever new packet received then classifier will applied on that new packet to predict whether packet is normal or attack. We don't have any sensors to get test data so I am using below dummy values as the test data. Test data will contains only signal values and by evaluating those signal values and frequency classifier will classify/predict that test data as attack or normal.

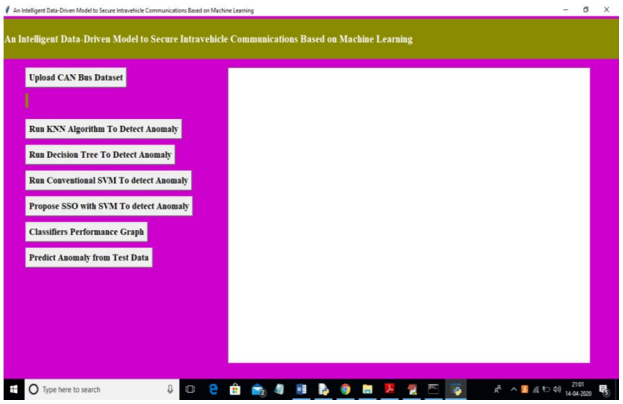
Below are some test data samples.

81219830.4139, id10, 0.3737464000855015, 0.6666666666666666,0 .9991955021452382, 0.475199882830615881219785.4139, id10, 0.3724087697056715, 0.9991955021452382, 0.47420213228827873

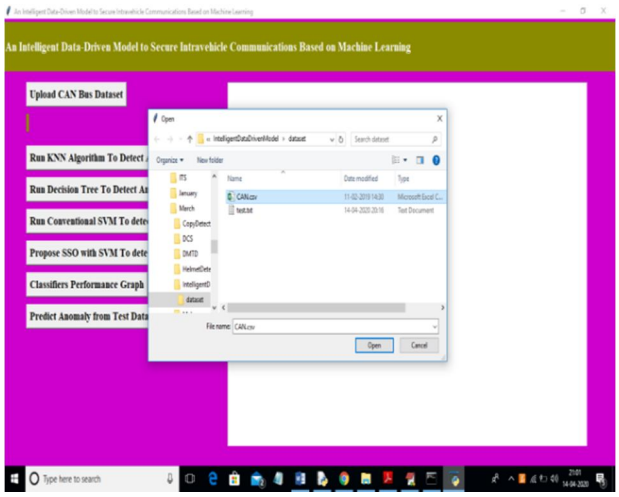
In above test data we can see there is no class label, classifier will predict its class label

Screen shots

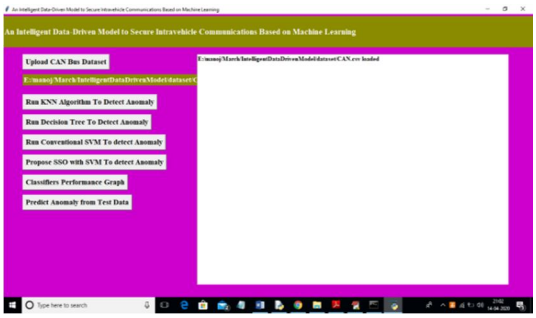
To run project double click on file to get below scr



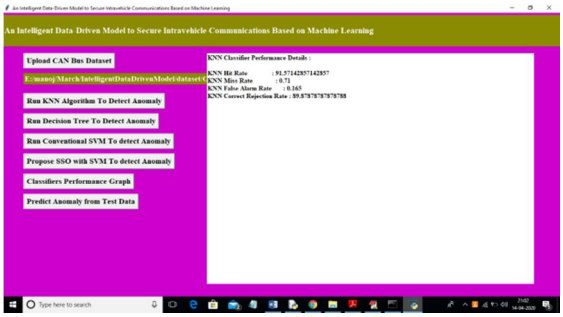

In above screen click on 'Upload CAN Bus Dataset' button and upload dataset



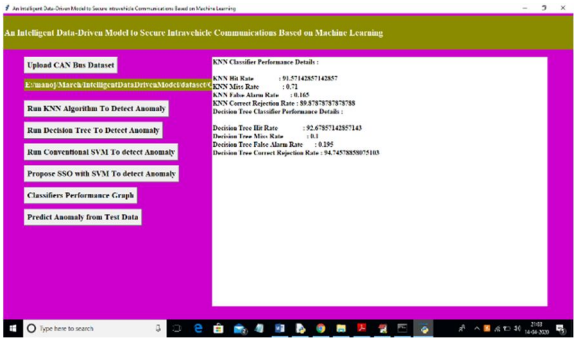

In above screen I am uploading 'CAN.csv' dataset and after uploading dataset will get below screen



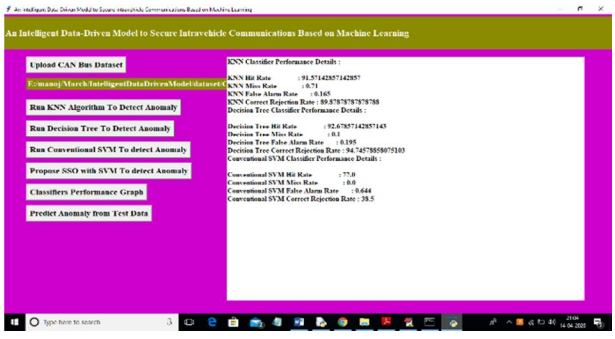

Now click on 'Run KNN Algorithm To Detect Anomaly' button to build KNN classifier train model to detect anomaly and evaluate



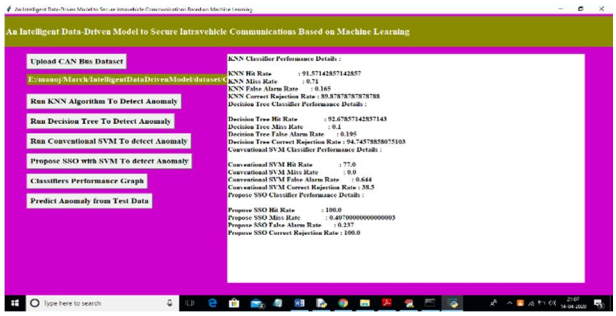

In above screen we got 4 indices values for KNN algorithm and now click on 'Run Decision Tree To Detect Anomaly' button to evaluate decision tree performance



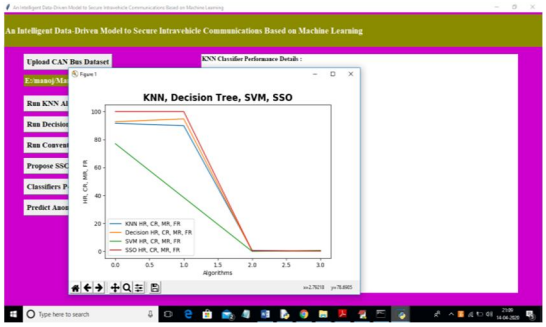

In above screen we got decision tree data and now click on 'Run Conventional SVM To detect Anomaly' button to evaluate conventional SVM performance.



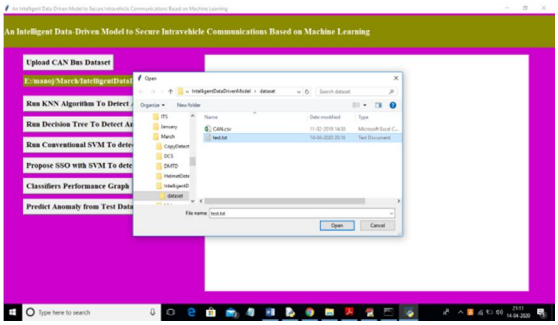

In above screen we got SVM performance data and now click on 'Propose SSO with SVM To detect Anomaly' button to run propose SSO with SVM classifier and evaluate its performance. (Note: when u run SSO then application will open 4 empty windows and you just close newly open empty window and keep working from first window only).



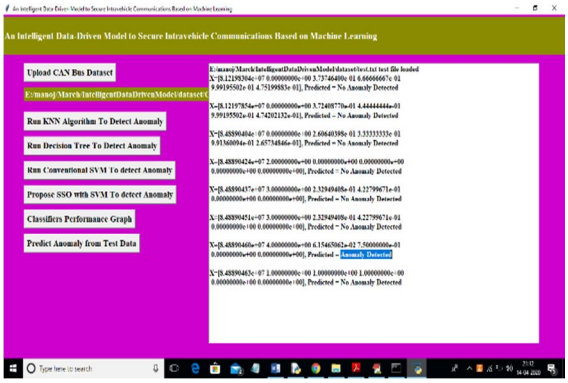

In above screen for SSO we got performance metric as 100% and MR and FR is not mandatory so we can ignore as said in paper. Now click on 'Classifiers Performance Graph' button to get performance graph between all classifiers




In above graph propose SSO has given high performance compare to other algorithms. In above graph y-axis represents HR, MR, FR and CR values. Now click on 'Predict Anomaly from Test Data' button to upload test data and predict it label

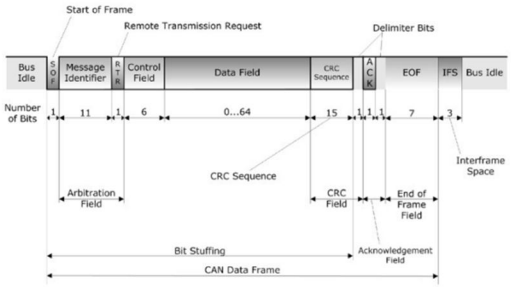



In above screen I am uploading 'test.txt' file and now click on 'Open' button to predict uploaded test file class label.




In above screen in text area we can see uploaded test data and its predicted class label.All records contains normal packet data accept one record. So by using machine learning algorithms we can analyse packets and if packet contains attack then we ignore processing such packets.

## III. SYSTEMARCHICTURE




## IV. LITERATURE SURVEY

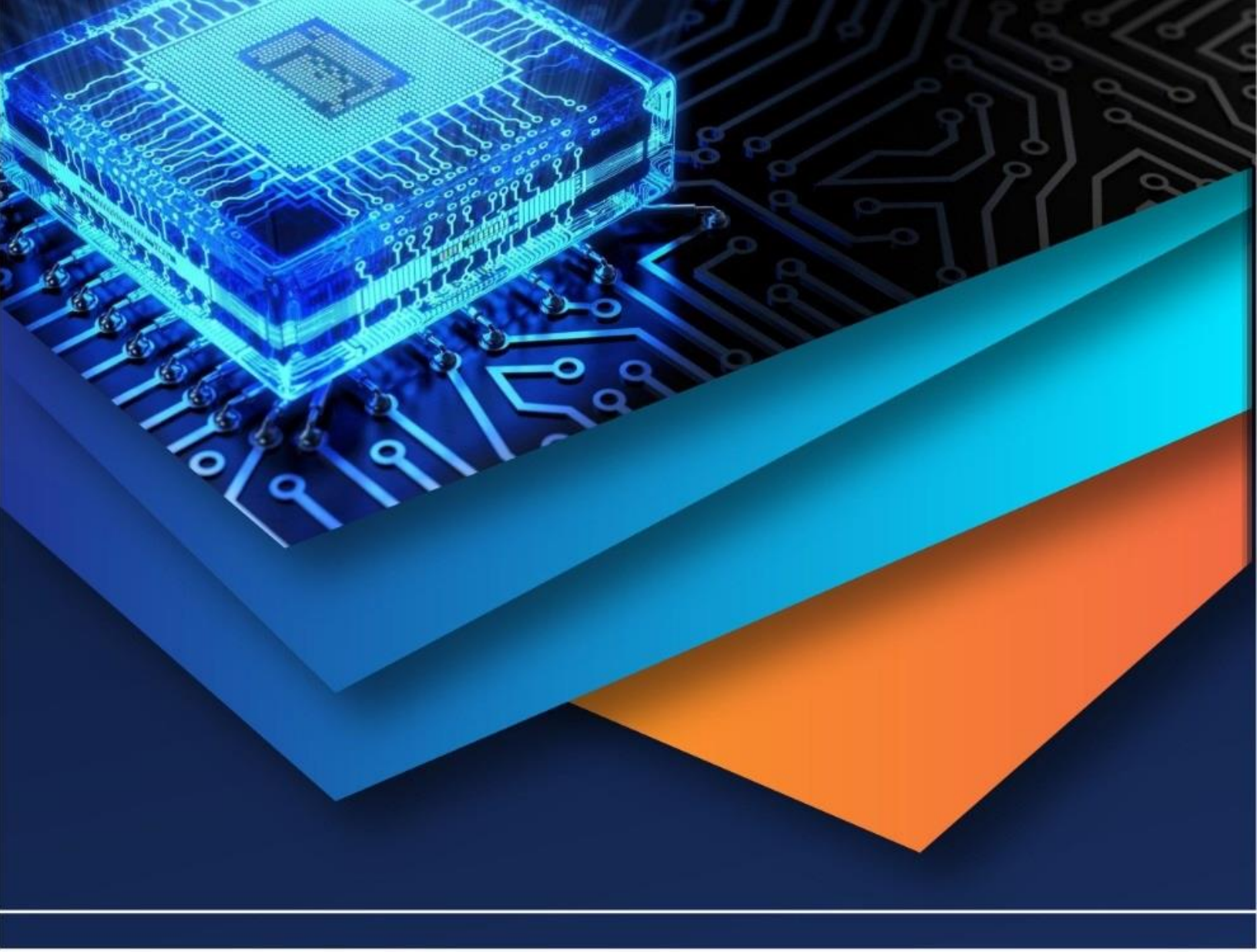
Momdooh is an assistant professor at the Electrical Engineering Department at King Saud University. He is also the Instructor of the Saudi Electricity Company Chair in Power Scheme Consistency and Safety. Dr. received his Ph.D. from McMaster University, Canada in 2007. As part of his work at King Saud University, he has been intricate in research and improvement activities in the areas of maintainable energy technologies, smart grid and renewable energy implementation, dependability and security charge of power supply systems, design and operation of spreading system, application of artificial intelligence in power system plan, and load management. Ali M. Eltamaly (PhD - 2000) is a occupied professor at King Saud University and Mansoura university, Egypt. He expected the B.Sc. and M.Sc. Egypt in 1992 and 1996, correspondingly. He received his Ph.D. Degree in Electrical Engineering after Texas A&M University in 200. His current research comforts include renewable energy, smart grid, power electronics, motor drives, power quality, artificial intelligence, evolutionary and experiential optimization techniques, and circulated generation. He published 20 book and book chapters and he has authored or coauthored more than 150 refereed journal and session papers. He distributed number of patents in USA patent office. He has managed a number of M.S. and PhD ideas, operated on number of National/International technical projects. He got extricate professor award for scientific excellence, Egyptian supreme council of Universities, Egypt, June, 2017 and he has awarded many prizes in different universities in Egypt and Saudi Arabia. He is take part as an editor and subordinate editors in many international journals and chaired many international assemblies' sessions. He acknowledged the B.Sc. and M.Sc. gradations from Minia University, Minia, Egypt in 2006 and 2010. He acknowledged the Ph.D. gradation from King Saud University, Riyadh, Saudi Arabia in 2016. He joined the Department of Electrical Engineering, Fuzhou University, China as a Postdoctoral Investigation related in 2018. He is presently a talent member in the Department of Electrical Engineering, College of Engineering, Minia University, Minia, Egypt, since 2008.

## V. CONCLUSION

It offers a unique intelligent and secured anomaly prototype for cyber attackes in the electric vehicles. The projected is constructed based on an upgraded support vector machine model protected by the SSO algorithm. From the bases of cyber security, the projected sense cruel manners while allowing the positive message frames recording in the protocol. The high HR% FR% MR% and CR% indices are there to identify whether the anomaly is detected or not.The authors will judge the outcome of other cyber attacks on the presentation of changed irregularity detection models in the future works**.**

## REFERENCES

[1] Monot ; N. Navet ; B. Bavoux IEEE Trans. Industrial Computer electronics, vol. 59, no. 10. Pp. 3934-3942, 2012.
[2] T.Y. Moon; S.H. Seo; J.H. Kim; S.H. Hwang; J. Wook Jeon, "Gateway system with investigative persistence for LIN, CAN and FlexRay", 2007 International Meeting on Control, Computerization and Organizations, pp. 2844 – 2849, 2007.
[3] B. Groza; S. Murvay, "Efficient Protocols for Secure Broadcast in Controller Area Networks", IEEE Trans., pp. 2034-2042, 2013.
[4] B. Mohandes, R. Al Hammadi, W. Sanusi, T. Mezher, S. El Khatib, "Advancing cyber–physical sustainability through integrated analysis of smart power systems: A case study on electric vehicles", International Journal of Critical Infrastructure Protection, vol. 23, pp. 33-48, 2018



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY