IMPROVE: Intelligent Machine Learning based Portable, Reliable and Optimal VErification System for Future Vehicles

Shreyas Madhav A V
School of Computer Science and Engineering,
Vellore Institute of Technology,
Chennai Campus, Chennai, 600127, Tamilnadu, India.
shreyas.madhav@gmail.com

A.Mohan
Department of Information Security, Institute of Computer Science and Engineering, SIMATS School of Engineering, Saveetha University, Chennai - 602105
annamalaimohan@gmail.com

Amit Kumar Tyagi [0000-0003-2657-8700]
Department of Fashion Technology,
National Institute of Fashion Technology, New Delhi,
Delhi, India
amitkrtyagi025@gmail.com

Abstract. The technological progress over the past decade has revolutionized the transportation domain. Autonomous and semi-autonomous vehicles have now gained the global spotlight for facilitating personal transportation with minimal manual intervention. The digitization of this industry has been accompanied by significant security challenges in terms of ensuring reliable transmission and robust communication networks which are critical for the proper functioning of the smart vehicle. The CAN bus architecture responsible to establishing connectivity within the various vital components of the car's internal architecture is a prime target for intrusions. Secure connections must also be established between the vehicle and external devices such as smartphones for enhancing the travel experience. Hence a complete security intrusion detection framework for self-driving cars is of dire need. This article introduces an Intelligent Machine Learning based Portable, Reliable and Optimal VErification System (IMPROVE) for Future Vehicles that aims to provide a viable solution to resist vehicular cyberattacks both on the internal network of the vehicle and the vehicle to device network established. The proposed framework is twofold in nature- The initial module focusses on ensuring Controller Area Network (CAN) security through machine learning modelling for intrusion detection. The second module is oriented towards utilizing data analysis to detect and block malicious behaviour on networks established with external/internal devices.

Keywords: Autonomous vehicle security, intrusion detection system, CAN Bus, machine learning, malware detection.

I. INTRODUCTION

Efficient transportation has become essential for the smooth functioning of humanity and its lifestyle choices. With the advent of new commercial automotive requirements and communication technology, the industry has entered a new era in machine anonymity. Vehicles are now being modified to relieve passengers from the stress of driving and navigating, helping them to focus their time on learning, working or relaxing. Automated transportation promotes road safety, eliminating accidents caused due to error in human judgement. It is estimated that the widespread production and application of self-driving cars could reduce fatal traffic accidents by upto 93% by removing human error from the driving process [29]. Financial burdens relating to vehicle repair, insurance and maintenance also decrease drastically with optimization automation of personal vehicles. The boost in complete electric vehicle production helps combat environmental degradation caused by vehicle air pollution.

979-8-3503-4821-7/23/$31.00 ©2023 IEEE

Autonomous cars have now been provided with the ability to analyse surrounding information, traffic patterns and internal resource requirements to make optimized decisions to self-drive the passengers to their destination efficiently.

The race towards launching autonomous cars to the general mainstream population is accelerating and increasing the requirement of robust and real time networks architectures for its feasible functioning. The organization of high-performance clusters that are connected through a central gateway operating upon a high-speed backbone. The arrangement of actuators and group sensors is carried out hierarchically. Autonomous vehicles employ a wide range of sensory devices like Light Detection and Ranging (LiDAR), Radio Detection and Ranging (RADAR) and high-resolution cameras which generate large amounts of data from which useful information can be extracted. The data flow structures of the vehicle run in different or parallel directions and require well organized electrical support with high-speed links, nodes, assemblies and cables. Vehicle networks are established for real time and high-speed communication within the vehicle and with external nodes of the network (V2X). V2X communication networks must provide real time inputs and analysis of the complete surrounding environment in addition to other data transmissions that enhance driver comfort [30, 31]. The environmental inputs assist the self-driving cars to decide whether they should accelerate decelerate or stop themselves. While the sensors help the vehicles interact with their surroundings, radio systems help vehicles communicate and exchange information with other similar vehicles or traffic related infrastructure/devices. The information assists vehicles in determining the most optimal route to the destination based upon road terrain, traffic congestions and slowdowns. The communication networks can be categorized based upon the nodes in the network and their range.

1.1 In-Vehicle Communication Systems

A typical in-vehicle communication system is comprised of internal wired connections within the different components of the vehicle. In the automotive domain, vehicle buses are special purposed internal networks for vehicle component interconnections. The facilitation of these connections is primarily achieved by CAN bus connection networks in autonomous cars Controller Area Networks or CANs are enabling reliable communication between devices/ embedded system devices without the requirement of a host computer. Durable and inexpensive network connections can be established and has propelled the mass production of it in the automotive sector. Autonomous vehicle has five electronic control units (ECU0 through ECU4) will communicate over a CAN bus. Every con-

trol unit ECU0 and ECU1, controls three of the ultrasonic sensors installed in the front and back of the vehicle. The middle ECU2 consists of ultrasonic sensor and global positioning system (GPS) to provide the main control unit ECU4 with current location to take the decision to move and send it to the moving control unit ECU3. ECU3 controls the motor drivers, that able to take a fast decision depending on the data collected from other ECUs. Figure 1 depicts in-vehicle communication layout incorporated in CAN based vehicles. With increase in the number of internal components, the wirings required also increases. Hence wireless mediums of communication are also being explored for widespread application in the automotive industry.

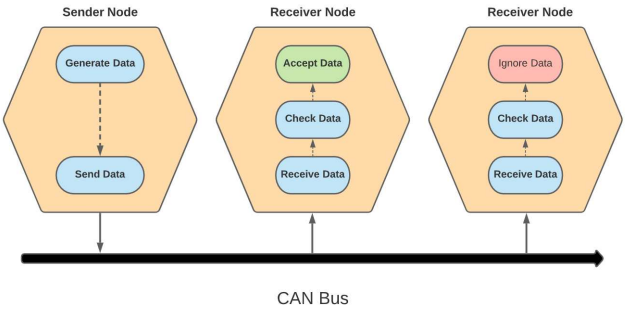

Fig. 1. In vehicle communication using CAN

1.2 Vehicle Device Communication

A specific type of communication in the category of vehicle to everything communication is vehicle to device communication, where transmission of information is carried out between a external device and the vehicle. Smartphones and personal tablets are device most often communicating with the vehicle. Vehicle to Device (V2D) communication can help diagnose abnormalities or faults in the internal systems, identify the operational information and control interior entertainment systems. The development of mobile applications for control and ease of usage has found its way into the automotive sector. The interaction between the vehicle and passenger is simplified and provides an increase in overall comfort. The introduction of mobile connectivity also accompanies with it the vulnerabilities of mobile application hacking and malware.

1.3 V2V Communication

The V2V communication [25] modules enable nearby vehicles to shared relevant information with each other. The information transmitted between vehicles can be regarding travel routes, locations, acceleration and individual car conditions that may help modify the decision-making processes of the vehicle to obtain ideal results. If a vehicle is involved in a road accident or has encountered an unpredicted obstacle, it can notify other vehicles that might be following a similar navigation path to avoid certain actions during their travel for the optimal results. V2V communications is heavily dependent on wireless communication mediums like Bluetooth, Wi-Fi or Cellular connections [26]. The allocation of separate frequency ranges for automotive communications are being established in recent times. In the United States of America, a 75MHz band of the 5.9GHz spectrum is utilized for vehicle communications and intelligent transportation systems possessing a total range of 300 meters. DSRC, a wireless protocol similar to WiFi is used in V2V communication along with GPS to provide a complete surrounding analysis of similar vehicles within their range of communication. Along with speed and acceleration related info, sophisticated vehicle systems transmit control data such as vehicle path history, path prediction, transmission state and steering wheel angle. With the combinational analysis of path prediction and past path, the vehicles are provided with real-time route strategy, complete path assessments and predicting dangerous accident possibilities. The communicated information over the network is anonymous is majority of the cases to safeguard personally identifiable information.

1.4 Vehicle to Infrastructure (V2I) Communication

Vehicle to Infrastructure (V2I) is another categorical division in vehicle information communication systems, where the connection establishment is achieved between the vehicle and external infrastructure centres for real time monitoring of location information and statistical analysis. This communication provides vehicles with the ability to interact with different devices that are part of the city's smart traffic system (Parking meters [15], traffic lights, cameras, streetlights, signs etc.,). Powered by an integrated structure of firmware, software and hardware, V2I transmissions are mostly bidirectional and wireless through ad hoc networks. The safety of each individual vehicle can be ensured by vehicle specific real time updates provided by the infrastructure. The distance of communication is farthest in this type of structure when compared to previous communication categories [27]. Extended wireless communication networks are used for the conveying of sensory inferences which may include traffic conditions, road preferences and availability of parking or repair services. City Traffic management systems in smart cities can utilize the data for traffic planning, dynamic speed limit determination, traffic signal timing optimization and overall vehicle movement control.

1.5 Vehicle Security

The maintenance of data integrity in the critical systems present in the autonomous vehicles is essential for the prevention of accidents or passenger injury. As the life safety of the passenger directly depends upon the secureness of the autonomous system, robust security features are regarded to be of high interest and requirement in self driving vehicles [28]. Secure transfer of data across the physical layer and across personal device networks play a major role in maintain the confidentiality of the transmission. Companies are looking into optical fibre-based connections as a methodology to combat electromagnetic interference, signal distortion and crosstalk. This property of optic networks becomes beneficial for vehicular transmissions due to large number of high-power devices [16] in the surrounding environment that may lead to transmission interference issues. Third party suppliers are now shifting their focus primarily towards encrypted data transfer enabled in-vehicle networks abiding by Global Ethernet standards [18] for automotive vehicles. This helps provide a stronger layer of protection against unauthorized interceptions during transmission. Software involved in the systems should be protected and updated regularly [18]. Malicious applications from a connected device can ambush and exploit the information available leading to further installation of malware modifications. Malware applications replicate the original software but breach the privacy guidelines by stealing account data, activating unnecessary systems or providing the intruder with more vulnerabilities.

Machine learning algorithms [17] play a significant role in autonomous vehicles and are being deployed in several different stages of the vehicle's production. Machine learning plays a significant role in the working of the Electronic Control Units (ECU)s in smart vehicles. Object recognition and classification of imaging data retrieved from the visual sensors of the vehicles are essential for understanding the landmarks around the vehicle. Surrounding object localizations and movement predictions can help the vehicle adjust its speed and navigation accordingly the ability of machine learning algorithms to understand and learn underlying patterns helps monitor the vital systems of the vehicles for any faults or repairs required. The same property of learning models can be applied to network security of the vehicles. Predictive modelling to identify anomalous or malicious behaviour can help prevent cyberattacks on the transmission networks of the vehicles. In this article, a novel framework for intrusion detection in internal and external vehicular networks is proposed.

II. RELATED WORKS

Network security for vehicle communications has recently gained interest due to the rapid development and production of autonomous smart vehicles. Reconfiguration of ECUs coupled with attack packet deactivated was proposed as a means to combat vehicle networks intrusions by Kwon et., al [1]. A mitigation module was also part of the system in order to recuperate the network and its stability back to normal by eliminating possible damages caused by the malware. Their architecture helps command travel for reconfiguration of electronic control units with the control to delete or deactivate packets upon analysis. Survival Analysis based abnormality detection systems have been developed for vehicular networks in the past [2]. The methodologies focus on the identification of attacks that obtain unauthorized control through malware packets (malfunction attacks, fuzzy attacks and flooding attacks). However, this technique was limited to the above three mentioned techniques alone. Recent advances in intelligent transformation systems have resulted in the introduction of vehicular cloud computing [3]. Implementation of intelligent transportation systems fueled by storage and computing capacities provide higher real time efficiency by reducing latencies and improves Quality of Service (QoS) to the passengers [4]. The traffic management system is also secured with the application of VCC to wireless sensor networks [5].

A cloud-based malware protection solution was established by Zhang et.al [6] for resource constrained autonomous systems. The system was also provided with the ability to detect new malware and update the existing malware database for future ease in detection. A single gateway architecture was demonstrated for monitoring and controlling all external transmissions of the vehicle. However, the system is dependent on having constant access to the secure cloud and alternate ways of malware inspection have not been explored. CAN Bus architectures are well regarded for their performance and efficiency but fall a bit short in terms of security. The vulnerabilities of the system can be protected with the help of intrusion detection systems geared towards protecting the CANs. This becomes particularly helpful for combatting unknown attack malware whose properties are not initially stored in the detection system. The exploration of deep learning methods for intrusion detection were also explored implementing GANs (General Adversial Networks) to generate possible solutions for unknown attacks [7].

A dual generator Discriminator structure is characteristic of GANs enabling the visualizing similar images [8]. This functions by considering the hexadecimal data flowing through the CAN as one hot encoded image data. Many studies have utilized the recent advances in high performance computing and graphical processing technology for creation of complex models like deep artificial neural networks that provide real time results. Artificial neural networks demonstrate great efficiency but are limited by their high-cost expectations. ANN based IDS systems have been implemented in autonomous vehicles along with Long Short-Term Memory and Inception Resnet Models [9].

Traditional Machine learning models were also tested. The results of the paper showed that the reduced architecture of Inception Resnet portrayed the maximum operability and performance. Fuzzy and DoS attack identification systems for the CAN bus structure have been proposed in the past to combat the unauthenticated nature of dataflow [10]. The CAN ID data is dominated as 0x000 in the case of DoS attacks. The CAN bus structure allows communication in broadcast and rapid phase. The common patterns of their interactions can be observed and used for identifying possible anomalies [11]. Every CAN ID send s a message at a specific period of time. All likely transactions of the CAN IDs have been transformed into a matrix based on exchange of packets in the training phase of the IDS. The success of artificial neural networks has propelled the study unsupervised modelling for intrusion detection in vehicular CAN [12]. The proposed CANet is a combination of a dual specialized ANN structure. The combined ANN networks were a LSTM [13] and an Autoencoder architecture [14]. The final inference mechanism predicts the possibility of anomalies and the margin of error is computed. If the margin of error is over a fixed threshold, an anomaly is confirmed. This paper explores a novel combinational framework for protecting vehicle to device and CAN network [20] associated with autonomous vehicles.

III. MOTIVATION

The domain of transportation is now undergoing a paradigm transition that will transform the industry forever. Connected autonomous vehicles [21] hold an integral part in the mainstream development of intelligent transportation systems (ITS) [23]. With the rise in connectivity and intercommunication, the number of possible vulnerabilities and loopholes also increase, especially in smart city regions that operate on the simultaneous functioning of multiple heterogenous networks [22]. Vehicle security is of utmost importance in such a scenario where the users are continuously connected to public networks. Intrusion detection helps recognize and record aggressive behavioral patterns, analyze the network traffic to segregate the anomalous candidates and to provide the vehicle with robust protection against other malicious nodes that have breached the network. In the last, in near future electric vehicle, hydrogen vehicle, etc., will be the reality to reduce omission of CO2 gases, to protect the earth, so we choose this area/ topic to work on.

IV. PROPOSED SYSTEM

IMPROVE (Intelligent Machine Learning based Portable, Reliable and Optimal VErification) system consists of an intrusion detection module powered by machine learning that can predict and detect possible intrusion activity into the Controller Area Network. This module offers protection to the Electronic Control Units of the vehicle from being overridden by malware. These software modules are to be added along with the original operational software of the vehicle. The software module monitors the CAN bus line for any possible actions that may indicate malware injection or abnormal behaviour. The proposed CAN protection module consists of a multi-step approach including input, analytics, prediction and final notifications. All the message traffic flowing through the CAN is screened through the protection module and analysed. This analysis is performed by a machine learning algorithm ensemble that evaluates the behaviour as normal or suspicious based on a weighted average voting algorithm. The model informs the passenger or the main control center of the surrounding area network in case of a breach in order to bring awareness towards a possible abnormality. The overall machine learning framework can be strengthened by subjecting it to extensive real-world application in order to constantly update and improve the model accuracy as well as its approach towards evaluating message transmission patterns. Custom updates required at a later date for identifying malicious behaviour can be done by each controller through the vehicle gateway.

A six-model weighted ensemble- Random Forest, Adaptive Boosting, Logistic Regression, Naïve Bayes, Bagging Tree and ANNs have been utilized to take their unique prediction characteristics and approach into consideration a whole unit before deciding on one final estimate. The overall available data for equipping the models with features that might influence their decision is split in a 4:1 ratio for training and testing. The random forest is regarded as a decision tree ensemble which is used in most classification problem for determining the final output through a multiple decision tree vote. Gini Index is set as the learning criterion and a 100-tree structure would be viable for the problem-solving process. The AdaBoost algorithm works based upon a iterative ensemble approach providing a combination of weight settings to provide the best accuracy even with outliers. Logistic Regression employs a sigmoid function to fit the data. It provides a statistical approach to solve prediction problems in a probabilistic manner. The logistic regression algorithm uses logistic function to squeeze the output of a linear equation between 0 and 1 and is modified ideally for classification problems. The Naïve Bayes classifiers, obtaining their name from the fact that they presume that the features of provided data are independent of each other. The likeliness of the prediction belonging to each class is computed based upon probability and the most probable label is assigned as the final prediction. The bagging tree algorithm portrays an ensemble equipped with replacement sampling and finalizes its prediction based on the majority vote. All the aforementioned models are combined to form a complete ensemble for detecting the presence of malicious activity in the CAN bus.

The second module component focuses on the protection of the network data transfer between the passenger's personal device and the vehicle. The type of malware (General Malware, Component specific intrusion or Adware) is also recognized by the system. This overall detection system can be split into three steps of operation- data preprocessing, feature selection and final prediction. The raw data flowing between the device and the vehicle is processed into the system in well sized segments. A tenfold cross validation is implemented with a 3:1 split of the overall data available for training and testing. Hyperparameter tuning is done to adjust the model to the available data and to obtain the maximal accuracy possible. Once the system achieves reliable accuracy on the testing data. The final phase of the system is done upon widespread implementation for real time prediction and monitoring in self driving vehicles. Figure 2 demonstrates the structure of the second component module.

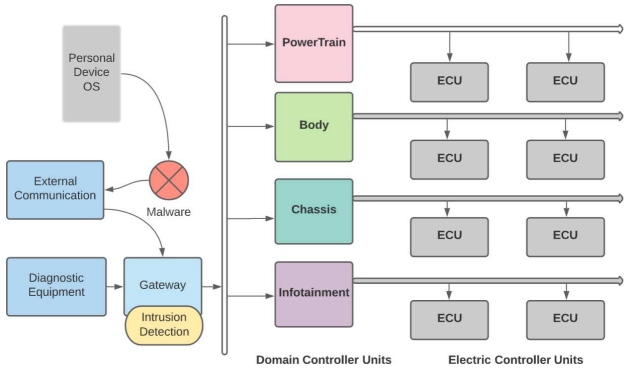

Fig. 2. Internal Architecture of IDS enabled Smart cars

A similar ensemble structure as implemented in the first intrusion detection is utilized here. Decision Trees, Random Forest, K Nearest Neighbours algorithms were employed for formulating the final predictions. The hyper parameters of each model are varied and the best setting are identified for real life application as a malware identification component in autonomous vehicles. The tuning of the parameters boosts up the performance and best optimized cost for the ensemble algorithm. The execution times and F1 scores are taken into consideration while constantly modifying the values for varied experimental conditions.

The overall system, including the two modules is integrated in to the vehicle's default software during production of the inter vehicular settings. Once a malware prediction is made on the CAN Bus or on the V2D network, the passenger in the vehicle is notified along with the control centre of the traffic management system present in the surrounding locality. In last, we request to refer other works to know more about importance of Vehicular Adhoc Network, Future Vehicles of Tomorrow in current era, raised issues in the respective sector and solutions for identified issues using Deep Learning or Machine learning, etc., techniques. Hence, in near future we will see the integration of many emerging technologies like Artificial Intelligence, Blockchain Technology, Cloud Computing, Internet of Things, etc., to improve the comfort or efficient of autonomous/ future vehicles.

V. SIMULATION AND RESULTS

The simulation results were obtained through a combinational use of VANETsim, The Network Simulator – 2 (NS-2) and Python for training the machine learning models models and creating the final ensemble. NS-2 is a discrete event simulator whereas VANETsim is a vehicle network specific simulator to test security solutions. The final ensemble model achieved sig-

nificantly higher performance in terms of accuracy when compared to the individuals' models. As this research progresses, the results of the paper will be provided with the extended version of this work. Further, researchers can find related articles on Adhoc network and their uses in different sectors with modern/ futuristic technologies in [32-53].

VI. CONCLUSION AND FURTHER DISCUSSIONS

With a rapid increase in the digitalization of vehicles, the customer's needs have also evolved towards expecting additional features, connectivity and services. The integration of embedded system devices into the vehicle structure has become popular in the development of future smart vehicles. With increase in complexity of autonomous vehicles, the vulnerabilities and loopholes in the system also increase. Hence the security of the system should be commensurate to the complexity of the overall vehicular network architecture. Network based malware attacks on the vehicle's communications systems are most common. The intervehicle, vehicle to device, vehicle to infrastructure and vehicle to vehicle communication networks are standardly enabled in all autonomous cars. This paper proposes a complete machine-based detection system called IMPROVE for recognizing abnormalities and anomalies in the CAN internal network or in the network established between the vehicle and the passenger's personal device. A multiple model machine learning approach has been employed for the creation of both modules in IMPROVE.

The overall system detects any malicious behaviour based on predictive modelling and notifies the passengers along with the nearby traffic control center if a positive prediction is made. This aims to resolve security issues sue to network malware vulnerabilities in autonomous cars. There is however some ambiguity revolving around the practical application of this framework in real life situation and the degree of mitigation required. The automotive companies directly involved in car production are not the only ones who should be focusing on digital vehicle safety. Third party suppliers and service partners involved in providing component or software services for the autonomous vehicles must also prioritize network security as a breach in their own component could open up a pathway to the main supplier's service network. This will result in unnecessary legal implications for the third-party companies coupled with the loss of trust in consumers. Hence, autonomous vehicle securities are critical for the progress and mainstream application of self-driving cars in the future and IMPROVE aims to provide a positive step towards this motive.

REFERENCES

[1] H. Kwon, S. Lee, J. Choi, and B. Chung, "Mitigation mechanism against in-vehicle network intrusion by reconfiguring ECU and disabling attack packet," in Proceedings of 2018 International Conference on Information Technology (InCIT), pp. 55–59, IEEE, Th¬ailand, 2018.

[2] M. L. Han, B. I. Kwak, and H. K. Kim, "Anomaly intrusion detection method for vehicular networks based on survival analysis," Vehicular Communications, vol. 14, pp. 52–63, 2018.

[3] S. Olariu, I. Khalil, and M. Abuelela, "Taking vanet to the clouds," International Journal of Pervasive Computing and Communications, vol. 7, no. 1, pp. 7–21, 2011.

[4] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," Journal of Network and Computer Applications, vol. 40, no. 1, pp. 325–344, 2014.

[5] J. Wang, Y. Liu, and Y. Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length," Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1138–1149, 2011.

[6] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: challenges and a solution framework," IEEE Internet of things Journal, vol. 1, no. 1, pp. 10–21, 2014.

[7] E. Seo, H. M. Song and H. K. Kim, "GIDS: GAN based Intrusion Detection System for In-Vehicle Network," 2018 16th Annual Conference on Privacy, Security and Trust (PST), Belfast, 2018, pp. 1-6.

[8] J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. 2014. Generative adversarial nets. In Proceedings of the 27th International Conference on Neural Information Processing Systems - Volume 2 (NIPS'14). MIT Press, Cambridge, MA, USA, 2672–2680.

[9] H. M. Song, Jiyoung Woo, Huy Kang Kim, In-vehicle network intrusion detection using deep convolutional neural network, Vehicular Communications, Volume 21, 2020, 100198

[10] Alshammari, M. Zohdy, D. Debnath and G. Corser, "Classification Approach for Intrusion Detection in Vehicle Systems. Wireless Engineering and Technology" pp: 79-94. 10.4236/wet.2018.94007, 2018.

[11] G. Marchetti, Mirco Stabili, Dario. (2017). Anomaly detection of CAN bus messages through analysis of ID sequences. 1577-1583. 10.1109/IVS.2017.7995934.

[12] M. Hanselmann, T. Strauss, K. Dormann and H. Ulmer, "CANet: An Unsupervised Intrusion Detection System for High Dimensional CAN Bus Data", IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.2982544, 2020.

[13] S. Hochreiter and J. Schmidhuber, "Long Short-term Memory". Neural computation. 9. 1735-80. 10.1162/neco.1997.9.8.1735, 1997.

[14] P. Baldi. 2011. Autoencoders, unsupervised learning and deep architectures. In Proceedings of the 2011 International Conference on Unsupervised and Transfer Learning workshop - Volume 27 (UTLW'11). JMLR.org, 37–50.

[15] Tyagi A.K., Kumari S., Fernandez T.F., Aravindan C. (2020) P3 Block: Privacy Preserved, Trusted Smart Parking Allotment for Future Vehicles of Tomorrow. In: Gervasi O. et al. (eds) Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science, vol 12254. Springer, Cham. https://doi.org/10.1007/978-3-030-58817-5_56

[16] Sravanthi, K. & Burugari, Vijay Kumar & Tyagi, Amit. (2020). Preserving Privacy Techniques for Autonomous Vehicles. 8. 5180-5190. 10.30534/ijeter/2020/48892020.

[17] Shasvi Mishra, Amit Kumar Tyagi, "The Role of Machine Learning Techniques in Internet of Things Based Cloud Applications", AI-IoT book, Springer, 2021.

[18] A.Mohan Krishna, Amit Kumar Tyagi, S.V.A.V.Prasad "Preserving Privacy in Future Vehicles of Tomorrow", JCR. 2020; 7(19): 6675-6684. doi: 10.31838/jcr.07.19.768.

[19] Amit Kumar Tyagi, N. Sreenath, "Preserving Location Privacy in Location Based Services against Sybil Attacks", International Journal of Security and Its Applications (ISSN: 1738-9976 (Print), ISSN: 2207-9629 (Online)), Volume 9, No.12, pp.189-210, December 2015.

[20] Amit Kumar Tyagi, N. Sreenath, "A Comparative Study on Privacy Preserving Techniques for Location Based Services", British Journal of Mathematics and Computer Science (ISSN: 2231-0851), Volume 10, No.4, pp. 1-25, July 2015.

[21] Tyagi A.K., Fernandez T.F., Mishra S., Kumari S. (2021) Intelligent Automation Systems at the Core of Industry 4.0. In: Abraham A., Piuri V., Gandhi N., Siarry P., Kaklauskas A., Madureira A. (eds) Intelligent Sys-

tems Design and Applications. ISDA 2020. Advances in Intelligent Systems and Computing, vol 1351. Springer, Cham. https://doi.org/10.1007/978-3-030-71187-0_1

[22] Tyagi, Amit Kumar; Nair, Meghna Manoj; Niladhuri, Sreenath; Abraham, Ajith, "Security, Privacy Research issues in Various Computing Platforms: A Survey and the Road Ahead", Journal of Information Assurance & Security. 2020, Vol. 15 Issue 1, p1-16. 16p.

[23] R, Varsha, Amit Kumar Tyagi 'Deep Learning Based Blockchain Solution for Preserving Privacy in Future Vehicles'. 1 Jan. 2020: 223 – 236.

[24] Bozdal, Mehmet, Mohammad Samie, Sohaib Aslam, and Ian Jennions. "Evaluation of can bus security challenges." Sensors 20, no. 8 (2020): 2364.

[25] Demba, Albert, and Dietmar PF Möller. "Vehicle-to-vehicle communication technology." In 2018 IEEE International Conference on Electro/Information Technology (EIT), pp. 0459-0464. IEEE, 2018.

[26] Sangaiah, Arun Kumar, Jaya Subalakshmi Ramamoorthi, Joel JPC Rodrigues, Md Abdur Rahman, Ghulam Muhammad, and Mubarak Alrashoud. "LACCVoV: linear adaptive congestion control with optimization of data dissemination model in vehicle-to-vehicle communication." IEEE Transactions on Intelligent Transportation Systems (2020).

[27] Ndashimye, Emmanuel, Sayan K. Ray, Nurul I. Sarkar, and Jairo A. Gutiérrez. "Vehicle-to-infrastructure communication over multi-tier heterogeneous networks: A survey." Computer networks 112 (2017): 144-166.

[28] Menouar, Hamid, Ismail Guvenc, Kemal Akkaya, A. Selcuk Uluagac, Abdullah Kadri, and Adem Tuncer. "UAV-enabled intelligent transportation systems for the smart city: Applications and challenges." IEEE Communications Magazine 55, no. 3 (2017): 22-28.

[29] Shladover, Steven E. "Connected and automated vehicle systems: Introduction and overview." Journal of Intelligent Transportation Systems 22, no. 3 (2018): 190-200.

[30] Wang, Haoxin, Tingting Liu, BaekGyu Kim, Chung-Wei Lin, Shinichi Shiraishi, Jiang Xie, and Zhu Han. "Architectural design alternatives based on cloud/edge/fog computing for connected vehicles." IEEE Communications Surveys & Tutorials 22, no. 4 (2020): 2349-2377.

[31] Amit Kumar Tyagi, S U Aswathy, Autonomous Intelligent Vehicles (AIV): Research statements, open issues, challenges and road for future, International Journal of Intelligent Networks, Volume 2, 2021, Pages 83-102, ISSN 2666-6030. https://doi.org/10.1016/j.ijin.2021.07.002.

[32] Amit Kumar Tyagi (2022), Handbook of Research on Technical, Privacy, and Security Challenges in a Modern World. IGI Global. DOI: 10.4018/978-1-6684-5250-9

[33] Khushboo Tripathi, Manjusha Pandey, and Shekhar Verma. 2011. Comparison of reactive and proactive routing protocols for different mobility conditions in WSN. In Proceedings of the 2011 International Conference on Communication, Computing & Security (ICCCS '11). Association for Computing Machinery, New York, NY, USA, 156–161. https://doi.org/10.1145/1947940.1947974

[34] Jajula, S.K., Tripathi, K., Bajaj, S.B. (2023). Review of Detection of Packets Inspection and Attacks in Network Security. In: Dutta, P., Chakrabarti, S., Bhattacharya, A., Dutta, S., Piuri, V. (eds) Emerging Technologies in Data Mining and Information Security. Lecture Notes in Networks and Systems, vol 491. Springer, Singapore. https://doi.org/10.1007/978-981-19-4193-1_58

[35] Ranchhodbhai P.N, Tripathi K., "Identifying and Improving the Malicious Behavior of Rushing and Blackhole Attacks using Proposed IDSAODV Protocol", International Journal of Recent Technology and Engineering, vlo. 8(3), pp.6554-6562, 2019

[36] Midha S, Tripathi K, Sharma MK. Practical Implications of Using Dockers on Virtualized SDN. Webology. 2021 Apr; 18, pp.312-30.

[37] D. Agarwal and K. Tripathi, "A Framework for Structural Damage detection system in automobiles for flexible Insurance claim using IOT and Machine Learning," 2022 International Mobile and Embedded Technology Conference (MECON), 2022, pp. 5-8, doi: 10.1109/MECON53876.2022.9751889.

[38] S. Midha, G. Kaur and K. Tripathi, "Cloud deep down — SWOT analysis," *2017 2nd International Conference on Telecommunication and Networks (TEL-NET)*, 2017, pp. 1-5, doi: 10.1109/TEL-NET.2017.8343560.

[39] K. Somisetti, K. Tripathi and J. K. Verma, "Design, Implementation, and Controlling of a Humanoid Robot," *2020 International Conference on Computational Performance Evaluation (ComPE)*, 2020, pp. 831-836, doi: 10.1109/ComPE49325.2020.9200020.

[40] Sai, G.H., Tripathi, K., Tyagi, A.K. (2023). Internet of Things-Based e-Health Care: Key Challenges and Recommended Solutions for Future. In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P.C., Ganzha, M. (eds) Proceedings of Third International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems, vol 421. Springer, Singapore. https://doi.org/10.1007/978-981-19-1142-2_37

[41] S. Subasree, N.K. Sakthivel, Khushboo Tripathi, Deepshikha Agarwal, Amit Kumar Tyagi, Combining the advantages of radiomic features based feature extraction and hyper parameters tuned RERNN using LOA for breast cancer classification, Biomedical Signal Processing and Control, Volume 72, Part A, 2022, 103354, ISSN 1746-8094, https://doi.org/10.1016/j.bspc.2021.103354.

[42] Kumari, S. & Muthulakshmi, P. (2022). Transformative Effects of Big Data on Advanced Data Analytics: Open Issues and Critical Challenges. Journal of Computer Science, 18(6), 463-479.

[43] S. Midha and K. Triptahi, "Extended TLS security and Defensive Algorithm in OpenFlow SDN," *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2019, pp. 141-146, doi: 10.1109/CONFLUENCE.2019.8776607.

[44] Midha, S., Tripathi, K. (2021). Extended Security in Heterogeneous Distributed SDN Architecture. In: Hura, G., Singh, A., Siong Hoe, L. (eds) Advances in Communication and Computational Technology. Lecture Notes in Electrical Engineering, vol 668. Springer, Singapore. https://doi.org/10.1007/978-981-15-5341-7_75

[45] Midha, S., Tripathi, K. (2020). Remotely Triggered Blackhole Routing in SDN for Handling DoS. In: Dutta, M., Krishna, C., Kumar, R., Kalra, M. (eds) Proceedings of International Conference on IoT Inclusive Life (ICIIL 2019), NITTTR Chandigarh, India. Lecture Notes in Networks and Systems, vol 116. Springer, Singapore. https://doi.org/10.1007/978-981-15-3020-3_1

[46] Mapanga, V. Kumar, W. Makondo, T. Kushboo, P. Kadebu and W. Chanda, "Design and implementation of an intrusion detection system using MLP-NN for MANET," *2017 IST-Africa Week Conference (IST-Africa)*, 2017, pp. 1-12, doi: 10.23919/ISTAFRICA.2017.8102374.

[47] Tyagi, A.K. (Ed.). (2021). Data Science and Data Analytics: Opportunities and Challenges (1st ed.). Chapman and Hall/CRC.

[48] Tyagi, A.K., & Abraham, A. (Eds.). (2022). Recurrent Neural Networks (1st ed.). CRC Press. https://doi.org/10.1201/9781003307822

[49] Tyagi, A.K., & Abraham, A. (Eds.). (2021). Recent Trends in Blockchain for Information Systems Security and Privacy (1st ed.). CRC Press. https://doi.org/10.1201/9781003139737

[50] Kumar Tyagi, A., Abraham, A., Kaklauskas, A., Sreenath, N., Rekha, G., & Malik, S. (Eds.). (2022). Security and Privacy-Preserving Techniques in Wireless Robotics (1st ed.). CRC Press. https://doi.org/10.1201/9781003156406

[51] Tyagi, A. K., Rekha, G., & Sreenath, N. (Eds.). (2021). Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles. IGI Global. http://doi:10.4018/978-1-7998-3295-9

[52] Tyagi, A. K. (Ed.). (2021). Multimedia and Sensory Input for Augmented, Mixed, and Virtual Reality. IGI Global. http://doi:10.4018/978-1-7998-4703-8

[53] Akshita Tyagi, Swetta Kukreja, Meghna Manoj Nair, Amit Kumar Tyagi, Machine Learning: Past, Present and Future, Neuroquantology, Volume 20, No 8 (2022), DOI: 10.14704/nq.2022.20.8. NQ44468

2023 International Conference on Computer Communication and Informatics (ICCCI), Jan. 23– 25, 2023, Coimbatore, INDIA