Journal of Artificial Intelligence, Machine Learning and Neural Network
ISSN:2799-1172
Vol: 02, No. 06, Oct-Nov 2022
http://journal.hmjournals.com/index.php/JAIMLNN
DOI: https://doi.org/10.55529/jaimlnn.26.43.54

Cyber Security Issues and Solution in Vehicular Networks

A. Manikandan*

Assistant Professor, ECE Department, SSM Institute of Engineering and Technology, Dindigul, India

*Corresponding Author: *manikandan.aapece@ssmiet.ac.in*

Received: 10 August 2022 **Accepted:** 26 October 2022 **Published:** 29 November 2022

Abstract: Vehicle Ad-hoc Networks (VANETs), which share traffic-related information between cars and infrastructure and aid to enhance driver safety and road safety, are capable of and viable for implementing Intelligent Transportation Systems (ITS). efficient traffic flow. Nonetheless, the confidentiality and privacy of such information is crucial for VANET due to the open wireless access channel. Attackers can compromise VANET security by capturing, intercepting, altering, replaying, or deleting traffic-related information. Thus, the hottest study field right now is assuring the security and privacy of traffic-related information in VANETs. Vehicle communication has been the subject of extensive effort in this situation. Yet, in terms of security needs, security assaults, and performance effectiveness, these duties fall short of adequately addressing security challenges.This white paper organises various authentication and privacy systems into categories and analyses their workings, advantages and disadvantages, security needs, threats, and performance metrics. Lastly, we chose the research inquiries that would be posted in the VANET security area.

Keywords: Cyber Security, Vehicular Networks, VANET.

1. INTRODUCTION

Road traffic accidents or injuries, which affect almost 1.3 million people annually, are currently the tenth leading causes of death. Road accidents will overtake cancer as the sixth leading cause of mortality by 2030, according to a poll [1]–[3]. The 2007 CARE - European Road Accident Database Study [4], [5] found that each year in EU member states, 43,000 people die and 1.8 million suffer injuries at a cost of €160 billion.About 3% of the global GDP, or $1 trillion US, is spent on the costs of road accidents [6]– [8]. A significant amount of time and fuel are also wasted due to traffic bottlenecks ITS is essential to every aspect of modern life in the digital age we live in. Future traffic management will be improved by ITS's ubiquitous and cutting-edge services, which will help control the aforementioned unpleasant events [9]. Building smart automobiles is now possible because to the rapidly advancing wire-free connectivity technologies [10]– [12]. Automakers and the telecoms sector have now agreed to equip every car with wireless technology, enabling it to connect with other vehicles and roadside infrastructure.

VANET, a subset of MANET (Mobile Ad Hoc Network), is a mobile network that employs moving cars as network nodes to enable communication between the moving vehicle and the surrounding fixed infrastructure [13]. Because it offers a way to gather freely obtained traffic information and sense physical properties linked to exchanging traffic information, VANET is also known as VSN (Vehicle Sensor Network) [14], [15].

The three fundamental elements of a typical VANET system are the dependable TA (TA), roadside unit (RSU), and on-board unit (OBU), as seen in Figure 1. TA is a dependable third party that manages and maintains the whole network infrastructure and serves as a registry for RSUs and OBUs. In order to serve as an intermediary node between the TA and the OBU and to administer numerous authentication procedures, the RSU is a base station (such as WiFi, WiMAX, etc.) installed beside the road.

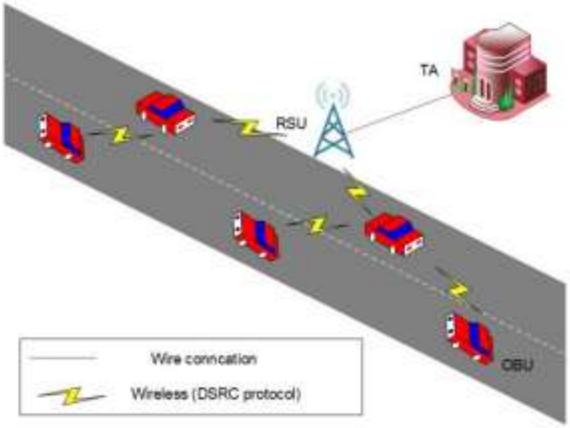

Fig. 1. VANET Components

The on-board OBU's traffic-related data is received, processed, and sent to other cars and RSU via the dedicated short-range communication (DSRC) protocol [16]. With the aid of the IEEE 802.11p wireless communication standard, the DSRC standard has been renamed Wireless

Access for the Vehicular Environment (WAVE). As a result, each vehicle sends alerts about traffic to other cars or RSUs within a set amount of time (100-300 ms).

The rest of this essay is structured as follows. The backdrop of this study is explained in the second section. A few major problems and their solutions for vehicle networks are discussed in Part III. The conclusions of this study are presented in Section IV at the end.

Network Model

Two layers make up VANET. OBU and RSU make up the base layer, whereas TA and the application server make up the top layer (traffic control center).

- OBU: Installed in the car, the OBU gathers, processes, and transmits traffic-related data via the DSRC protocol (IEEE 802.11p) [17]-[19]. A tamper-proof device (TPD), the OBU never divulges the data it has saved. All OBUs have fixed clocks that can be securely resynchronized when they travel through an area with RSU coverage. Every vehicle is equipped with a GPS (Global Positioning System) and the necessary interfaces to find services and contact the driver [20]. RSUs have more computational and storage power than OBUs. Every vehicle transmits a notification about the traffic to the RSU next door.
- RSUs: These roadside base stations provide as the link between the application servers and OBU, TRA, and KGC [21]. RSU's computational and storage resources are more than OBU's but less than those of TA and KGC. When receiving signed flow-related messages, it is the duty of each RSU to check the message signatures.These authenticated messages are subsequently transmitted from the RSUs to the Application Server through a secure channel.
- TAs: These TAs have the power to oversee and keep up with VANETs. RSUs and OBUs must be registered with the TRA. To provide identity anonymity in vehicle communications, it creates pseudo-identities. It maintains secrecy and assumes control of conflict resolution [22]– [24]. It can track down misbehaving entities (RSUs or cars) and uncover their true identities via signed messages, and it revokes them by cancelling their registrations.

Related Work

Mobile Ad Hoc Networks (MANETs) are being utilised more often in a variety of sectors, including energy efficiency, smart agriculture, smart transportation, and Internet of Things (IoT) ecosystems. Wireless technology is anticipated to play a bigger part in the future of the Internet given its recent quick growth [25]. The connection between these nodes can, however, be exploited by MITM (man-in-the-middle) attacks, which are seen to be the fundamental issue with MANETs [25]. This is brought on by malicious nodes intercepting data sent between trustworthy nodes. Consequently, the primary goal of this research is to examine the effects of the attacker's MITM attack approach using message delay and message loss in MANET [25].

The suggested CM-CPPA approach performs communication signing and verification using Chebyshev polynomial mapping operations and chaotic map-based hash algorithms [26]. The suggested CM-CPPA scheme's security study findings utilising the AVISPA simulator are also favourable against typical attacks [26]. Due to the absence of the suggested CM-CPPA scheme, the performance evaluation beats similar state-of-the-art approaches in terms of computational,

communication, etc. overhead for EC and BP operations [26]. The finalised CM-CPPA approach lowers the computational costs of message signing and signature verification by 62.52% and 24.2%, respectively. The format tuple transmission overhead is reduced by 57.69% using the suggested CM-CPPA approach [26].
This paper suggests a Chebyshev polynomial-based defence against side-channel assaults for 5G-enabled vehicle networks [27]. The extraordinary chaotic and anti-military features of Chebyshev polynomials may now be realised thanks to our study. The five phases of our work are system activation, registration, signature, verification, and pseudonym updating [27]. In order to combat side channel assaults, it also continually and routinely refreshes the TPD's vehicle database. Security study demonstrates that our approach records the security (authentication, integrity, and traceability) and privacy (pseudonym identification and unlikability) in 5Genabled vehicle networks [27]. Lastly, neither BPC nor ECC are used in our work. It is superior than previous recent research for in-vehicle networks, but [27].

The vehicle signs the message while it is being transmitted using many pseudo-identities it has acquired from a trusted authority (TA) and an appropriate signing key [28]. As a result, every broadcast message that each vehicle receives must be verified according to the suggested approach [28]. Moreover, the suggested approach enables TA to shield malfunctioning vehicles from insider assaults by preventing them from transmitting signed messages continually [28].The security study demonstrated that the suggested approach complied with the security standards for message integrity and authenticity, message authenticity and integrity, unlinkability, and traceability [28]. The suggested approach also defends against a wide range of typical security threats, such as message interception, impersonation, modification, and replay assaults. Additionally, under the random oracle model, our method is resistant to assaults using adaptively selected messages [28].

A trusted authority (TA) creates a new group key and broadcasts it to CRT-enabled cars according to the suggested manner [29]. Additionally, because the master key for the system does not need to be preloaded, the suggested technique just needs one trusted TPD. The suggested approach shields all 5G-enabled car networks against password guessing attacks and guarantees the maximum level of security [29]. According to a security research [29], the suggested technique is safe against adaptively generated message assaults in a stochastic oracle model and complies with the security criteria of 5G-enabled automobile networks.The suggested technique has been demonstrated to outperform the conventional eight methods in terms of computing and communication costs since the performance study makes use of cryptographic operations based on elliptic curve cryptography [29].

These technologies give hackers the ability to transmit phoney messages and pose as authorised nodes [30]. Additionally, the performance effectiveness of security-related traffic message signing and verification has not been satisfactorily addressed by any of these systems. We create a safe and effective SE-CPPA (Conditional Privacy Preserving Authentication) mechanism in this work to guard against spoofing attacks and boost performance [30].The SE-CPPA approach is based on bilinear pairing cyphers for message signing and verification [30]. By safety analysis and comparison, the suggested SE-CPPA approach may fulfil safety goals in terms of formal and informal analysis [30]. To deter fraudulent assaults, vehicle real-world identity stored in a tamper-resistant device (TPD) is periodically updated and has a finite lifespan [30].

Intelligent transportation technologies like VANET (Vehicle Ad Hoc Network) have grown in popularity in recent years [31]. VANET enables vital and effective vehicle communication.Securing wireless communication channels is one of the key problems of VANETs since existing security techniques still have a large computational and communication overhead and are susceptible to security and privacy issues [31]. To overcome these concerns, our research focuses on enhancing the performance effectiveness of conditional privacy-preserving authentication systems. Currently, this effort examines the system's security flaws [31]. To assure and boost the efficiency of VANET communication, improvements to identity-based conditional privacy authentication procedures are also suggested [31].

Ad-hoc wireless networks have garnered scholarly and general interest recently [32]. In order to complete a large-scale sensing mission, numerous extremely small autonomous networking, connection, and sensing units working together with little energy and processing resources are required [32]. Many sensing devices, numerous computer technologies, and restricted power, connection, and processing capabilities are all collectively provided by wireless sensor systems. Wireless sensor networks with an emphasis on IEEE802.11b may have problems such as battery cleaning with insufficient power sources [32]. As a result, the wireless node's resources are necessary for these devices to operate properly. In this work, two theoretical models are proposed and used to forecast performance-related QoS [32].

Vehicle Ad-Hoc Networks (VANET) have emerged as a result of the quick advancement of wireless communication and the pressing need to lower traffic congestion and mortality [33]. It is essential to defend against cyberattacks on every connection in a VANET. This is due to the fact that transmitting data to a public server might result in numerous cyberattacks. This work suggests an identity-based privacy-preserving authentication mechanism (ID-PPA) to address several security and privacy-related challenges in VANETs [33]. Recently, many identity-based security mechanisms for VANETs were unveiled.However, there could be a lot of issues with these programmes. In fact, these issues with ID-based schemes are resolved by the ID-PPA scheme [33].

In order to solve security and privacy problems, VANETs (Vehicle Ad Hoc Networks) often utilise public key infrastructure, group signatures, or identity-based techniques [34]. Nevertheless, none of these approaches can effectively manage the verification of many VANET messages in areas with high traffic densities [34]. Sub-channel attacks can be used by adversaries to obtain private information kept on tamper-resistant devices (TPD) [34]. In this work, we

present a batch verification method for each node's synchronisation message that is based on conditional identity-based privacy authentication [34]. To prevent side-channel assaults, TPD also routinely and consistently refreshes the vehicle information database [34].The suggested technique beats conventional methods since it does not rely on the Map-To-Point hash function or the bilinear pairing process [34].
Intelligent transportation systems (ITS) have recently started to build VANET (Vehicle Ad Hoc Network) [35]. Unfortunately, VANETs are susceptible to security flaws since V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) interactions use open media.Many studies have recently suggested security plans to deal with these problems [35]. However, a lot of these methods have significant computing costs, particularly the batch verification approach, which verifies a number of messages at once [35]. Without utilising the LSWBVM (Batch Verification Method) approach, we provide a minimal security system based on elliptic curve cryptography in this work (ECC). An XOR operation and a global hash function are used in the suggested LSWBVM approach for mutual authentication [35].

For the past several years, intelligent transportation systems have increasingly used vehicle ad hoc networks (VANETs) [36]. Key components of VANET architecture are autonomous, dispersed networks and quickly changing topologies. Significant commercial and academic interest has been generated by VANET's characteristics and applications for improving road safety, notably in studies addressing the improvement of transportation systems that have the potential to save lives [36]. The most significant and challenging issue from the standpoint of VANET security and privacy is message broadcasting in open access networks like VANET [36]. There have been several proposals for investigations on VANET security and privacy [36]. Unobservable, however, was not considered as a general privacy norm. We suggest a VANET-based privacy-preserving communication strategy (VPPCS) to address this problem [36].
Vehicle Ad Hoc Network, a novel wireless communication technology, has the ability to lower the danger of motor vehicle crashes for drivers and offer a variety of entertainment options [37].Because VANET is an open network, messages broadcast by moving objects may face security risks. VANETs are therefore susceptible to security and privacy issues [37]. Recently, several solutions to these VANET issues have been put forth [37]. The most worrying issues, though, are the enormous computational cost and security worries. This paper suggests a method for effective conditional privacy protection using reciprocal authentication [37] to overcome the aforementioned problems with VANETs. The plan depends on various geographical distributions that are the outcome of geographic divides [37].

In order to give drivers a secure and pleasant driving environment, Intelligent Transportation Systems (ITS) relies on the underlying technology of Vehicle Ad Hoc Networks (VANETs) [38]. Security, privacy, and effectiveness must be carefully examined, nevertheless, due to the unusual openness of wireless communication channels. This paper suggests a novel, effective NECPA (Conditional Privacy Preserving Authentication) strategy for secure communication on VANET [38]. The NE-CPPA employs the Elliptic Curve Cryptography (ELC) technique to adhere to

security and privacy requirements [38]. The suggested schema is subjected to a security examination against several attack scenarios.The expenses of computation and communication are then analysed to demonstrate the system's viability and robustness [38].
Use the well-known evolutionary algorithm [39] that concentrates mostly on the RSU area to discover an optimum or almost optimal solution. Utilize SUMO (Software Update Monitor) to simulate road traffic, OpenStreetMap (OSM) to get real map data, Gatcom (Group for Architecture and Computer Technologies) to produce vehicle mobility, and the Veins model framework for simulation. Pedestrian and vehicle networks are used to simulate actual traffic, while Matlab [39] is used to create algorithms for data analysis. The main setting for the simulation is Beirut, Lebanon's Hamraneighbourhood [39]. Our suggested RSU placement model, which is based on the evolutionary algorithm, shows that the ideal RSU position can improve the reception of Basic Safety Messages (BSM) transmitted by the cars [39].

The most crucial elements of the Vehicle Ad Hoc Network (VANET) (RSU) are roadside devices and automobiles with VANET capabilities [40]. Efficiency of the VANET is significantly impacted by the density and placement of these RSUs [40]. It was not feasible to install a significant number of RSUs in the early phases of VANETs due to the limited market penetration of VANET-enabled automobiles or the high deployment cost of RSUs [40]. For optimum performance, a small number of RSUs should be strategically positioned in chosen areas [40]. This paper gives a well-known evolutionary method based on the location of the RSU to identify the optimum or almost optimal solution [40].

2. CONCLUSION

With the dissemination of traffic-related information, VANET contributes to increased driver safety and traffic efficiency on the road. VANET, however, might provide some significant challenges and issues for the open wireless access medium. This information's security and privacy might be jeopardised by an attacker. In order for researchers and developers to recognise and discriminate important aspects for VANET security and performance efficiency, we introduce factors linked to VANET security and performance efficiency.Finally, we've talked about some of the unresolved issues that need to be addressed by researchers if VANETs technologies, infrastructures, and services are to be deployed effectively and securely.

3. REFERENCES

1. Ashokkumar, N., Nagarajan, P., Venkatramana, P. (2020). 3D(Dimensional)—Wired and Wireless Network-on-Chip (NoC). In: Ranganathan, G., Chen, J., Rocha, Á. (eds) Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems, vol 89. Springer, Singapore. https://doi.org/10.1007/978-981-15-0146-3_12.

2. N. Ashok Kumar, G. Shyni, Geno Peter, Albert Alexander Stonier, Vivekananda Ganji, "Architecture of Network-on-Chip (NoC) for Secure Data Routing Using 4-H Function of Improved TACIT Security Algorithm", Wireless Communications and Mobile Computing, vol. 2022, Article ID 4737569, 9 pages, 2022. https://doi.org/10.1155/2022/4737569
3. Ashokkumar N, Kavitha A. An Efficient and Novel Design of Loop filter Charge Pump and VCO for PLL using CMOS technology. International Journal of Engineering & Technology. 2018;7(3.1):39-41.
4. Ashokkumar, N., Nagarajan, P., Vithyalakshmi, N., Venkataramana, P. (2019). Quad-Rail Sense-Amplifier Based NoC Router Design. In: Hemanth, J., Fernando, X., Lafata, P., Baig, Z. (eds) International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI) 2018. ICICI 2018. Lecture Notes on Data Engineering and Communications Technologies, vol 26. Springer, Cham. https://doi.org/10.1007/978-3-030-03146-6_170.
5. N. A. Kumar, P. Nagarajan, M. S. L, J. Arockia Dhanraj and T. S. Kumar, "Analysis of Millimeter-Wave based on Multichannel Wireless Networks-on-Chip," 2022 International Conference on Electronics and Renewable Systems (ICEARS), 2022, pp. 405-409, doi: 10.1109/ICEARS53579.2022.9752077.
6. P. Nagarajan, N. A. Kumar, J. Arockia Dhanraj, T. S. Kumar and M. Sundari L, "Delay Flip Flop based Phase Frequency Detector for Power Efficient Phase Locked Loop Architecture," 2022 International Conference on Electronics and Renewable Systems (ICEARS), 2022, pp. 410-414, doi: 10.1109/ICEARS53579.2022.9752249.
7. Neelima, K., Ashok Kumar Nagarajan, and Neeruganti Vikram Teja. "Digital Twin Technology Characteristics Design Implications and Challenges for Healthcare Applications." Advancement, Opportunities, and Practices in Telehealth Technology. IGI Global, 2022. 105-115.
8. Natarajan V, Nagarajan AK, Pandian N, Savithri VG. Low Power Design Methodology. Very-Large-Scale Integration. 2018 Feb 16:47.
9. Kumar, N. Ashok, S. Vishnu Priyan, P. Venkatramana, and Durgesh Nandan. "Routing Strategy: Network-on-Chip Architectures." In VLSI Architecture for Signal, Speech, and Image Processing, pp. 167-197. Apple Academic Press, 2022.
10. Ashokkumar, N., P. Nagarajan, and S. Ravanaraja. "Survey Exploration of Network-on-Chip Architecture." (2009).
11. AshokKumar N, Nagarajan P, Selvaperumal S, Venkatramana P. Design challenges for 3 dimensional network-on-chip (NoC). InInternational Conference on Sustainable Communication Networks and Application 2019 Jul 30 (pp. 773-782). Springer, Cham.
12. Ashokkumar, N., and A. Kavitha. "Transition level energy consumption of NoC (network-on-chip) using data encoding techniques." 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2015.
13. N. Ashokkumar, S. Meera, P. Anandan, Mantripragada Yaswanth Bhanu Murthy, K. S. Kalaivani, Tahani AwadAlahmadi, Sulaiman Ali Alharbi, S. S. Raghavan, S.

ArockiaJayadhas, "Deep Learning Mechanism for Predicting the Axillary Lymph Node Metastasis in Patients with Primary Breast Cancer", BioMed Research International, vol. 2022, Article ID 8616535, 14 pages, 2022. https://doi.org/10.1155/2022/8616535

14. Ashokkumar, N Ashokkumar and P, Krishnagandhi and Kannan, B and Raju, Y David Solomon, Smart Farming Field Observation Using Embedded Systems (2020). International Journal of Electrical Engineering and Technology, 11(4), 2020, pp. 241-245, Available at SSRN: https://ssrn.com/abstract=3658019
15. Kavitha, A., N. Ashok Kumar, and M. Revathy. "Automatic Identification of Maritime Boundary Alert System using GPS." International Journal of Engineering & Technology 7.3.1 (2018): 20-22.
16. Ashokkumar, N., B. Kannan, and Y. Raju. "Smart Farming Field Observation Using Embedded Systems." International Journal of Electrical Engineering and Technology 11.4 (2020).
17. NAGARAJAN, Ashokkumar, A. Kavıtha, and S. Devı. "Wireless Sensor Data Fusion Techniques in Estimating Temporal Resource Attributes in Scenarios of Intermittent Connectivity." El-Cezeri 9.2: 413-423.
18. I. Chandra, M. S. L, N. Ashok Kumar, N. P. Singh and J. Arockia Dhanraj, "A Logical Data Security Establishment over Wireless Communications using Media based Steganographic Scheme," 2022 International Conference on Electronics and Renewable Systems (ICEARS), 2022, pp. 823-828, doi: 10.1109/ICEARS53579.2022.9752183.
19. Ashokkumar, N., and A. Kavitha. "A novel 3D NoC scheme for high throughput unicast and multicast routing protocols." Technical Gazette 23.1 (2016): 215-219.
20. Ashokkumar, N., and A. Kavitha. "Network on Chip: A Framework for Routing in System on Chip." Journal of Computational and Theoretical Nanoscience 12.12 (2015): 6077-6083.
21. Kumar, N. A., Kavitha, A., Venkatramana, P., & Nandan, D. (2022). Architecture Design: Network-on-Chip. In VLSI Architecture for Signal, Speech, and Image Processing (pp. 147-165). Apple Academic Press.
22. A. Balasubramani, K. Kalaivanan, R. C. Karpagalakshmi and R. Monikandan, "Automatic facial expression recognition system," 2008 International Conference on Computing, Communication and Networking, Karur, India, 2008, pp. 1-5, doi: 10.1109/ICCCNET.2008.4787749.
23. Karpagalakshmi, R.C.Rajesh.D “Hierarchical Clustering of Music towards Human Mood “, International Journal of Advanced Research in Computer science,Volume 1, NO.4, Nov-Dec 2010.ISSN:0976-5697 pp.93-96.
24. R. C. Karpagalakshmi and D. Tensing, "Vehicle object observation using position based local gradient model," 2012 International Conference on Radar, Communication and Computing (ICRCC), Tiruvannamalai, India, 2012, pp. 293-298, doi: 10.1109/ICRCC.2012.6450598.
25. Karpagalakshmi, R.C. Karthigachandrasekakaran “A Survey on Search-As-You-Type Using Ranking Queries “, International Journal of Advanced Research in Computer

science and Software Engineering, Volume 3, Issue 10, Oct-2013, ISSN:2277-128X pp.1040-1043.

26. Karpagalakshmi R C and Dr.D.Tensing " Surveillance of vehicle objects with aerial Images using localization and posture based Local gradient model " Journal of Theoretical and Applied Information Technology. Vol. 64 No.1, ISSN: 1992-8645, pp-199 – 204.
27. Karpagalakshmi R C and Dr.D.Tensing" Event Detection at Vehicle Location Points using Spatial Time Invariant Model "International Journal of Engineering and Technology, Vol 6 No 2.pp – 1188 – 1193.
28. Karpagalakshmi R C and Dr.D.Tensing "Orientation Model for Effective Event Detection in Vehicle Location "International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 9, Number 23 (2014) pp. 18889-18898.
29. Malliga C, Karpagalakshmi RC. "Evaluating the Learning Objects in Domain Module generation from Plain text book". The International Daily journal ,ISSN 2278 – 5469 EISSN 2278 – 5450, Discovery, 2015, 32(142),22-27.
30. Malliga C, Karpagalakshmi RC. "Automated formation of domain module from plain textbooks Usingdom-sortze system". EJERM ,Volume - 2, Issue – 2.
31. Prabhakaran K, Karpagalakshmi RC. "Sketch and execution of productive virtue security for android smart phone". The International Daily journal ,ISSN 2278 – 5469 EISSN 2278 – 5450,Discovery,2015, 30(122), 116-121.
32. Anandhi.T, Karapagalakshmi.R.C, Efficient Cryptosystem for Scalable Data Sharing in Cloud Storage,International Journal of Advanced Research Trends in Engineering and Technology ,Vol. 3, Special Issue 22, April 2016.
33. Karpagalakshmi, R.C, Tensing. D &Kalpana,A.M 'VPEDA: A Robust Vantage Point based Event Detection Architecture for Efficient Object Detection and Localization', Asian Journal of Information Technology,15(24) : 4970 -4978, 2016.
34. K. Namrata, R. C. Karpagalakshmi, Dr. D. Tensing, "Survey on 2D-DCT Based Image Watermarking with High Implanting Limit and Robustness", Volume 4 Issue 10 , International Journal on Recent and Innovation Trends in Computing and Communication. pp: 161 – 164.
35. Karpagalakshmi, RC, Tensing, D &Kalpana, AM , "MULTI-POINT CO-ORDINATION SCHEME FOR TRAFFIC CONTROL SYSTEMS " Asian Journal of Research in Social Sciences and Humanities, Vol. 6, No. 10, pp. 911-919.
36. Karpagalakshmi, RC, Tensing, D &Kalpana, AM 'Image Localization using Deformable Model and its Application in Health Informatics, Journal of Medical Imaging and Health Informatics,Vol. 6, No. 8, Dec 2016, pp. 1972 -1976.
37. Kalpana, AM ,Karpagalakshmi, RC, Tensing, D , "IMPLEMENTATION OF RTT-GM FOR VEHICULAR RECOGNITION AND LOCALIZATION , " Asian Journalof Research in Social Sciences and Humanities, Vol. 7, No. 1, pp.941-949.

38. K.Namrata,R.C.Karpagalakshmi,S.S.Manikandasaran,"IMPLEMENTATION OF NOVEL TECHNIQUE FOR IMAGE WATERMARKING USING 2D-DCT" International Journal of Pure and Applied Mathematics, Volume 117, No. 16 pp.221-226.
39. Dr. R. C. Karpagalakshmi, Dr.R.Rajasekar, and Dr.A. M. Kalpana, "STUDY ON EFFECTIVE TRAFFIC ORGANIZATION WITH FUZZY USING NEIGHBOR JUNCTION POINTS", International Journal of Pure and Applied Mathematics. volume 118 no. 14.
40. Dr. R. C. Karpagalakshmi,Dr.R.Umamaheswari,Dr.R.Rajasekar, "Analysis of Time Discrepancy in Multi Proxy Synchronization for Transportation" TAGA JOURNAL OF GRAPHIC TECHNOLOGY for the publication in Volume 14-2018. pp.195-200.
41. Dr. R. C. Karpagalakshmi, A.Kanimozhi, International journal of Computer Science Engineering Techniques on FACIAL EXPRESSION AND RECOGNITION USING LOCAL DIRECTIONAL NUMBER PATTERN, Volumn 3, Issue 5.
42. Ms. A.Kanimozhi, Dr.R.C.Karpagalakshmi, Ph.D, Dr.P.VijayalakshmiPh.D, International Journal of Research and Analytical Reviews on MULTIMODAL FACIAL EMOTION RECOGNITION SYSTEM, Volume 6, Issue 2 ,pp. 527-532.
43. Ms. Arularasi, Dr.R.C.Karpagalakshmi, Ph.D, Dr.P.Vijayalakshmi, International Journal of Research and Analytical Reviews on Protection and Privacy of Smart home Automation Syatem Using IOT, Volume 6, Issue 2 , pp.167-171.
44. S. Boopalan, Dr. Puneet Goswami, Dr.K. Ramkumar, Dr.R.C. Karpagalakshmi, . Jour of Adv Research in Dynamical & Control Systems on Heterogeneous Distort-Prevention Manifold Resource Distribution Mechanism for Cloud Management, Vol. 12, No. 3.
45. Meghala Murgesh, Karpagalakshmi, R. Umamaheswari, Journal of Data Mining and Management, Iot Based Real Time Video Data Monitoring, e-ISSN: 2456-9437, Volume-5, Issue-1 (2020), http ://doi.org /10.5281 /zenodo .3691039.
46. Dr R C Karpagalakshmi, Mr.Bharathkumar, Mr.Vignesh, Mr.Yogaraj, Mr.Naveenkumar," Implementation of automated low cost Data warehouse for Preserving and Monitoring Vegetables and Fruits" ,Journal of Engineering Sciences ,Vol 11, Issue 11.
47. Dr R Umamaheswari,Dr R C Karpagalakshmi and Mr.Kavinkumar ," AN ANDROID APPLICATION FOR SMART ATTENDANCE MANAGEMENT SYSTEM BY USING FACE RECOGNITION" , Journal of Engineering Sciences ,Vol 11, Issue 11.
48. Dr K Chandramohan, Dr R C Karpagalakshmi ,Ms.Sumaiya, Ms.Subhashini and Ms.Sowmiya ," Design and Implementation Of Weeding Robot For Organic Farming" , Journal of Engineering Sciences ,Vol 11, Issue 11.
49. Dr R C Karpagalakshmi, Mr.Gobinathan, Dr R Umamaheswari, A SIVA, "REVIEWING AND MODELLING OF SEED SOWING MULTIPURPOSE ROBOT TOWARDS SMART FARMING", Journal of Engineering Sciences ,Vol 11, Issue 11.
50. R. C. Karpagalakshmi, P. Vijayalakshmi, K. Gowsic · R. Rathi, "An EfectiveTrafc Management System Using Connected Dominating Set Forwarding (CDSF) Framework for Reducing Traffic Congestion in High Density VANETs ", Wireless Personal

Communications (2021) 119:2725–2754, https://doi.org/10.1007/s11277-021-08361-y, 11-march-2021.

51. S. Suvitha, R. C. Karpagalakshmi, R. Umamaheswari, K. Chandramohan, M. S. Sabari, “An Estimation and Evaluation of Network Availability in Link State Routing Networks ”, Journal of Network Security Computer Networks, e-ISSN: 2581-639X, Vol-7, Issue-3 (Sep-Dec, 2021), https://doi.org/10.46610/JONSCN.2021.v07i03.003.
52. P. Nirmala Devi, K. Chandramohan , R. C. Karpagalakshmi , R. Umamaheswari , Gayathri J, “Blockchain and Reliable Mapping Scheme Utilizing Decentralized Computing Sources”,”Journal of Information Technology and Sciences ”,e-ISSN: 2581-849X Volume-7, Issue-2 (2021).
53. T.Ramalingam, R. Umamaheswari , R. C. Karpagalakshmi , K. Chandramohan , M.S.Sabari, “ Location of plant Leaf maladies utilizing picture division”,” Journal of Image processing and Artificial Intelligence ”, e-ISSN: 2581-3803 Volume-7, Issue-3
54. Vijayprabakaran.K , Dr.R.C.Karpakalakshmi , Dr.R.Umamaheswari, “Tracking nearby ambulance using GPS single point positioning algorithm “, “Journal of Android and IOS Applications and Testing “,Volume 7 Issue 1.