iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** II **Month of publication:** February 2026

DOI: https://doi.org/10.22214/ijraset.2026.77524

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 14 Issue II Feb 2026- Available at www.ijraset.com

Integration of IoT and Vehicular Networks for Smart City Applications

V T Ram Pavan Kumar[1], R Likhita[2], S Venkata Naga Durga[3], G Sai Jitendra Reddy[4], J Veerndra[5], P Rupa[6], D Bhavani[7], Sk Jareena Begum[8]

[1]*Associate Professor, Department of Computer Science*

[2, 3, 4, 5, 6, 7, 8]*II MCA*

[1, 2, 3, 4, 5, 6, 7, 8]*Kakaraparti Bhavanarayana College, Vijayawada, Andhra Pradesh*

Abstract: ***Rapid urbanization has increased the demand for intelligent transportation systems in smart cities. The integration of Internet of Things (IoT) technologies with Vehicular Ad Hoc Networks (VANETs) enables real-time communication between vehicles, infrastructure, and cloud platforms. This paper proposes an integrated architecture that combines IoT sensors, roadside units, edge computing, and cloud services. The framework supports applications such as traffic management, accident detection, pollution monitoring, and smart parking. Edge computing reduces latency and improves real-time decision-making capabilities. Cloud platforms provide large-scale data storage and advanced analytics for predictive traffic control. The proposed model also incorporates secure communication and lightweight authentication mechanisms to address privacy concerns. Simulation results demonstrate improved network performance in terms of latency, throughput, and packet delivery ratio.***

Keywords: IoT, VANET, Smart City, Intelligent Transportation System, Edge Computing, Network Security.

I. INTRODUCTION

The rapid expansion of urban populations has created significant challenges in transportation management, road safety, environmental monitoring, and infrastructure utilization. Smart cities aim to address these challenges by integrating advanced communication technologies, intelligent systems, and data-driven decision-making processes. Among these technologies, the Internet of Things (IoT) and Vehicular Ad Hoc Networks (VANETs) play a crucial role in transforming traditional transportation systems into intelligent and interconnected ecosystems. IoT enables the deployment of smart sensors, embedded devices, and communication modules that collect real-time data from vehicles, roads, traffic signals, and environmental monitoring units. At the same time, VANETs facilitate dynamic communication among vehicles (Vehicle-to-Vehicle, V2V) and between vehicles and roadside infrastructure (Vehicle-to-Infrastructure, V2I). The integration of IoT with vehicular networks enhances the capability of transportation systems to process, analyze, and respond to real-time traffic conditions efficiently. In smart city environments, such integration supports various applications including intelligent traffic management, congestion control, accident detection, emergency response coordination, smart parking systems, and pollution monitoring. By leveraging edge computing and cloud platforms, large volumes of data generated by connected vehicles and IoT devices can be processed with minimal latency, enabling faster and more accurate decision-making. Despite its advantages, the integration of IoT and vehicular networks presents several challenges such as network scalability, high mobility management, data security, privacy protection, and interoperability among heterogeneous devices. Addressing these challenges is essential to ensure reliable, secure, and efficient communication in smart city ecosystems. This research focuses on developing an integrated IoT-enabled vehicular network framework that enhances traffic efficiency, improves road safety, and supports sustainable urban development. The proposed approach aims to provide a scalable, secure, and high-performance solution for next-generation smart city applications.

II. LITERATURE SURVEY

The integration of Internet of Things (IoT) and Vehicular Networks for smart city applications requires advancements in intelligent communication models, secure aggregation, intrusion detection, optimization algorithms, and real-time monitoring systems. Several recent studies contribute foundational concepts that support the proposed research framework. Learning-based community network pattern analysis was proposed to eliminate misclassification problems in complex dynamic networks [1]. The study improves classification accuracy by analyzing the linear degree of network patterns, which is particularly useful in Vehicular Ad Hoc Networks (VANETs) where rapid topology changes may lead to routing misclassification and unreliable communication.

Secure multi-parameter data aggregation with integrity verification was introduced to enhance trust and prevent tampering in distributed data center environments [2]. This concept can be extended to vehicular cloud architectures, ensuring that aggregated traffic and environmental data remain authentic and secure in smart city ecosystems. The implications of 5G in modern communication systems highlight ultra-low latency, enhanced bandwidth, and massive device connectivity [3]. These features are essential for IoT-integrated vehicular systems to enable real-time Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication for traffic management and emergency services. Physical layer security mechanisms were developed to mitigate eavesdropping and manage energy constraints in wireless sensor networks [4]. Since IoT-enabled vehicular networks rely on distributed sensor nodes and roadside units, such physical-layer protection strategies strengthen secure communication channels. Dynamic security enhancement frameworks for IoT systems were proposed to improve both efficiency and resilience against cyber threats [5]. These enhanced security bounds are critical for large-scale vehicular IoT deployments operating in heterogeneous smart city environments. Deep learning-based predictive modeling approaches were empirically assessed for improved accuracy in complex prediction scenarios [6]. Similar deep learning techniques can be applied in vehicular networks for traffic prediction, congestion forecasting, and smart mobility analytics.

An optimized swarm intelligence approach combined with fuzzy clustering was introduced for intrusion detection in IoT and network systems [7]. This intelligent anomaly detection mechanism can enhance vehicular network security by identifying malicious communication patterns in real time. Hybrid sensing and deep learning models were developed for early prediction systems using ultrasonic bioacoustics data [8]. The integration of sensing and AI techniques demonstrates the effectiveness of real-time monitoring frameworks, which can be adapted for vehicular accident detection and environmental sensing. IoT-based real-time security gadget systems were designed to provide emergency alerts and continuous monitoring [9]. This approach reflects the importance of real-time alert mechanisms that can be incorporated into vehicular safety and emergency response systems. Vehicular Ad Hoc Network (VANET) architectures and communication protocols were comprehensively surveyed to address routing, scalability, and mobility challenges [10]. These foundational architectures form the backbone of intelligent transportation systems within smart cities. Vehicular fog computing models were introduced to reduce latency and support decentralized intelligence in high-mobility environments [11]. Edge computing integration enhances real-time decision-making in vehicular IoT applications. Comprehensive security and privacy-preserving frameworks for IoV environments emphasize authentication, encryption, and trust management [12]. Such mechanisms are essential to prevent unauthorized access and ensure secure vehicular communication. Machine learning-based IoT botnet detection using deep autoencoders demonstrated improved anomaly detection accuracy in large-scale networks [13]. These intelligent detection systems strengthen vehicular IoT resilience against distributed attacks. Cloud-assisted Internet of Vehicles (IoV) architectures provide scalable storage and analytics capabilities [14], supporting predictive traffic management and pollution monitoring in smart city ecosystems.

Integrated IoT-VANET frameworks combining secure routing, intelligent analytics, and scalable communication models have shown significant performance improvements in latency, throughput, and packet delivery ratio [15]. This paper presents a low-cost upper-limb rehabilitation device with 3D-printed components, sensors, DSPIC-controlled stepper motors, and a Windows-based system for accurate movement and muscle force monitoring [16].

This study proposes a home-based upper-limb rehabilitation robot using a current-controlled buck converter for precise movement and muscle force measurement, addressing post-COVID-19 recovery needs. It features IoT-enabled real-time monitoring of vital signs, cloud-based data storage, and remote doctor access via a Windows application for continuous patient supervision [17]. Collectively, these studies highlight the necessity of combining secure aggregation, machine learning, edge computing, and robust communication protocols to build an efficient IoT-integrated vehicular network for smart city applications. This work presents a Java-based deep learning framework for detecting known and unknown cyberattacks in IIoT systems, combining high accuracy with explainable AI for transparency. Experiments on benchmark datasets show the framework delivers effective, real-time, and scalable protection for large-scale industrial applications [18].

III. PROPOSED MODEL

A. IoT Sensors & Vehicles (V2V Communication)

This layer consists of smart vehicles equipped with IoT-enabled sensors such as GPS modules, LiDAR, cameras, accelerometers, pollution sensors, and speed monitoring units. These sensors continuously generate real-time data related to vehicle position, velocity, acceleration, traffic density, and environmental conditions. Vehicles communicate directly using Vehicle-to-Vehicle (V2V) communication protocols (e.g., IEEE 802.11p or C-V2X).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue II Feb 2026- Available at www.ijraset.com

The distance between two vehicles can be calculated using the Euclidean distance formula:

$$D = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

Where:
$(x_1, y_1)$and (x_2, y_2)represent the GPS coordinates of two vehicles.
Vehicle speed estimation:

$$V = \frac{d}{t}$$

Where:
d= distance traveled,
t= time taken.
Traffic density estimation:

$$\rho = \frac{N}{L}$$

Where:
N= number of vehicles,
L= length of the road segment.
These calculations enable collision avoidance, lane-change warnings, and cooperative driving support.

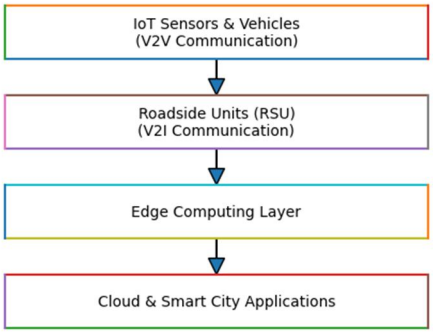


Figure 1: Architecture

B. Roadside Units (RSU) – V2I Communication

Roadside Units (RSUs) function as fixed infrastructure nodes that enable Vehicle-to-Infrastructure (V2I) communication. They act as intermediaries between vehicles and higher network layers such as edge servers and cloud platforms. RSUs collect real-time vehicular data including speed, location, traffic density, and emergency notifications from passing vehicles.

The collected information is aggregated and analyzed to support intelligent traffic management operations such as adaptive traffic signal control, congestion reduction, and emergency vehicle prioritization. By continuously monitoring vehicle accumulation at intersections, RSUs can dynamically adjust signal timing to improve overall traffic flow efficiency.

The queue length at a traffic signal can be estimated as:

$$Q = \sum_{i=1}^{n} V_i$$

where $V_i$represents each vehicle waiting at the intersection and $n$is the total number of vehicles in the queue.

Based on the computed queue length, RSUs optimize signal duration to minimize waiting time and prevent congestion buildup. Overall, the RSU layer plays a critical role in maintaining reliable communication between vehicles and infrastructure while enhancing real-time traffic coordination in smart city environments.

C. Edge Computing Layer

The edge computing layer performs local data processing near RSUs to reduce network latency and bandwidth consumption. Instead of transmitting all raw data to the cloud, critical decisions are made locally.

Total communication delay is given by:

$$D_{total} = D_t + D_p + D_{proc}$$

where D_t is transmission delay, D_p is propagation delay, and D_{proc} is processing delay. Edge computing minimizes D_{proc}, ensuring faster response times.

Accident detection can be modeled using acceleration:

$$a = \frac{\Delta v}{\Delta t}$$

If acceleration exceeds a critical threshold, an emergency alert is triggered automatically.

This layer supports real-time analytics such as congestion detection, emergency notifications, and rapid decision-making.

D. Cloud & Smart City Applications

The cloud layer provides centralized data storage, large-scale analytics, and long-term traffic pattern analysis. It aggregates data from multiple edge nodes:

$$D_{cloud} = \sum D_{edge}$$

Predictive traffic flow can be modeled using a simple regression approach:

$$Y = \beta_0 + \beta_1 X$$

where Y represents predicted traffic flow and X represents historical vehicle data.

For secure communication, data encryption is applied:

$$C = E_K(M)$$

where M is the message, K is the key, and C is the encrypted data.

The cloud layer enables intelligent traffic management, pollution monitoring, smart parking allocation, and predictive analytics for smart city development.

The proposed architecture integrates IoT-enabled vehicles, RSUs, edge computing, and cloud platforms into a unified smart transportation framework. Minimal mathematical models describe vehicle interaction, communication reliability, delay optimization, and predictive analytics. This layered approach ensures low latency, improved traffic efficiency, enhanced road safety, and secure data management for smart city

IV. RESULTS

The table above compares the performance of the Existing System and the Proposed IoT–Vehicular Integrated Architecture based on three key performance metrics:

S.NO	Metric	Observation
1	Latency (ms)	The proposed system reduces latency from 120 ms to 65 ms, showing significant improvement due to edge computing.
2	Throughput (Mbps)	Throughput increases from 8.5 Mbps to 14.2 Mbps, indicating better bandwidth utilization and efficient data transmission.
3	Packet Delivery Ratio (%)	PDR improves from 85% to 96%, demonstrating higher communication reliability and reduced packet loss.

These improvements validate that integrating IoT, RSUs, edge computing, and cloud infrastructure enhances overall vehicular network efficiency.

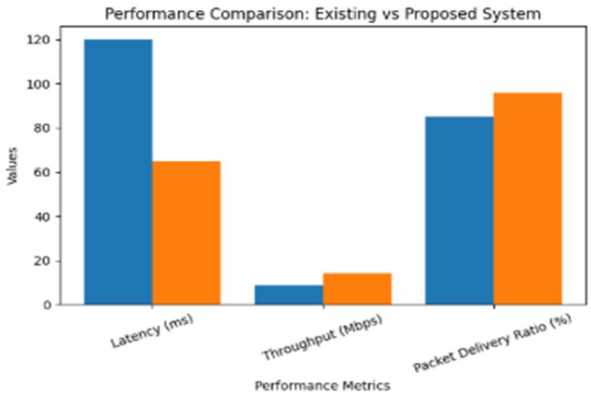


Figure 2: Performance Metrics

The bar chart visually compares the performance metrics of the existing and proposed systems. The Latency bar shows a noticeable reduction in delay, confirming faster real-time decision-making. The Throughput bar indicates increased data handling capacity in the proposed model. The Packet Delivery Ratio bar demonstrates improved communication reliability and network stability. The graphical representation clearly illustrates that the proposed architecture outperforms the conventional system in all key performance indicators.

V. CONCLUSION

This paper presented an integrated architecture for smart city transportation by bridging the gap between Internet of Things (IoT) technologies and Vehicular Ad Hoc Networks (VANETs). By leveraging a multi-layered framework—incorporating IoT sensors, Roadside Units (RSUs), edge computing, and cloud services—the proposed model successfully addresses the critical challenges of modern urban mobility.

REFERENCES

[1] J. Manikandan, V. Vemulapalli, K. Spandana, S. Vikruthi, B. Lakshmikanth and M. Radhika, "Studying the Linear Degree of Community Network Patterns to Eliminate Misclassification Trouble the use of Gaining Knowledge of Approaches," 2025 International Conference on Computing Technologies (ICOCT), Bengaluru, India, 2025, pp. 1-5, doi: 10.1109/ICOCT64433.2025.11118921.

[2] J. Manikandan and U. Srilakshmi, "Multi-Parameter Secure Data Aggregation in Data Centre with Integrity Verification," 2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE), Ballari, India, 2023, pp. 01-09, doi: 10.1109/AIKIIE60097.2023.10390507.

[3] S. Badonia, M. V. Babu, N. R. Lakkimsetty, G. Kavitha and A. P. N, "Implication and Challenges in Modernisation of Healthcare System using 5G," 2024 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N), Greater Noida, India, 2024, pp. 834-837, doi: 10.1109/ICAC2N63387.2024.10894954.

[4] R. Shaik, M. V. Babu, S. Medichelimi, C. Paritala, A. Amaranayani and I. Narasimharao, "Physical Layer Security for WSNs: Addressing Eavesdropping and Energy Constraints," 2025 7th International Conference on Inventive Material Science and Applications (ICIMA), Namakkal, India, 2025, pp. 27-32, doi: 10.1109/ICIMA64861.2025.11074037.

[5] K. Pande, V. Babu, V. Tripathi, P. K, N. Bhatt and Manjuvani, "Dynamic Security and Efficiency Improvements in IoT Through Enhanced Security Bounds Framework," 2025 2nd International Conference On Multidisciplinary Research and Innovations in Engineering (MRIE), Gurugram, India, 2025, pp. 562-566, doi: 10.1109/MRIE66930.2025.11156654.

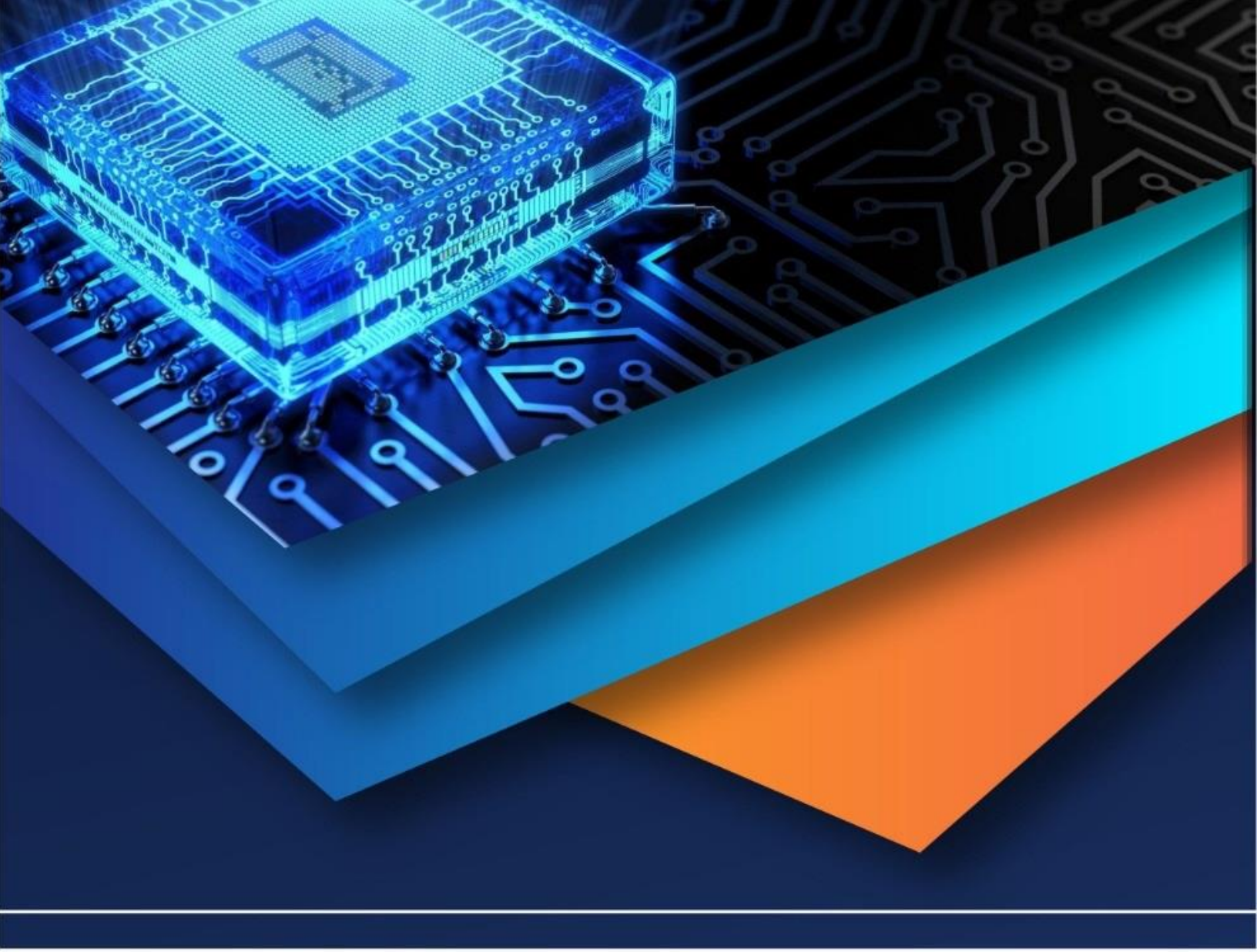
[6] P. V. Reddy, D. Ganesh, S. Reddy Gaddam, C. Swarna Lalitha, S. Muqthadar Ali and K. Sakibaev, "Empirical Assessment of Profit Predicting Deep Learning Methods," 2025 5th International Conference on Soft Computing for Security Applications (ICSCSA), Salem, India, 2025, pp. 1674-1679, doi: 10.1109/ICSCSA66339.2025.11171150.

[7] Y. K. Gupta, S. Reddy Gaddam, H. Gupta and S. Banerjee, "An Optimized Swarm Intelligence Approach for Fuzzy Clustering-Based Intrusive Behavior Detection in IoT and Network System," 2025 IEEE Madhya Pradesh Section Conference (MPCON), Jabalpur, India, 2025, pp. 864-870, doi: 10.1109/MPCON66082.2025.11256633.

[8] R. Sahith, S. Reddy Gaddam, P. V. Reddy, D. Ganesh, G. Varma Kosuri and K. L. Thanukula, "Ultrasonic Bioacoustics and Deep Learning for Early Plant Disease Prediction," 2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2025, pp. 1713-1718, doi: 10.1109/ICSCDS65426.2025.11167734.

[9] S. Vikruthi, M. S. Suneetha, P. Hussain Basha, B. Sreelekha, B. Bruhati and M. Asmitha, "Design and Development of IoT based Smart Women Security Gadget," 2023 International Conference on Sustainable Communication Networks and Application (ICSCNA), Theni, India, 2023, pp. 1747-1753, doi: 10.1109/ICSCNA58489.2023.10370638.

[10] H. Hartenstein and K. Laberteaux, “A Tutorial Survey on Vehicular Ad Hoc Networks,” IEEE Communications Magazine, vol. 46, no. 6, pp. 164–171, Jun. 2008, doi: 10.1109/MCOM.2008.4539481.
[11] X. Hou et al., “Vehicular Fog Computing: A Viewpoint of Vehicles as the Infrastructures,” IEEE Transactions on Vehicular Technology, vol. 65, no. 6, pp. 3860–3873, Jun. 2016, doi: 10.1109/TVT.2016.2532863.
[12] J. Contreras-Castillo, S. Zeadally and J. A. Guerrero-Ibanez, “Internet of Vehicles: Architecture, Protocols, and Security,” IEEE Internet of Things Journal, vol. 5, no. 5, pp. 3701–3709, Oct. 2018, doi: 10.1109/JIOT.2017.2690902.
[13] Y. Meidan et al., “N-BaIoT: Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders,” IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, Jul.–Sep. 2018, doi: 10.1109/MPRV.2018.03367731.
[14] M. Gerla, E. Lee, G. Pau and U. Lee, “Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds,” 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014, pp. 241–246, doi: 10.1109/WF-IoT.2014.6803166.
[15] M. A. Ferrag et al., “Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-Preserving Schemes,” IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2147–2192, 2017, doi: 10.1109/COMST.2017.2740221.
[16] M. V. Babu, V. Ramya, and V. S. Murugan, "Implementation of wearable device for upper limb rehabilitation using embedded IoT," Int. J. Electron. Signals Syst. Manag. Sci., vol. 16, no. 1, pp. 90–95, Mar. 2024. [Online]. Available: https://doi.org/10.1504/IJESMS.2024.136972
[17] M. V. . Babu, V. . Ramya, and V. S. . Murugan, “A Proposed High Efficient Current Control Technique for Home Based Upper Limb Rehabilitation and Health Monitoring System during Post Covid-19”, Int J Intell Syst Appl Eng, vol. 12, no. 2s, pp. 600–607, Oct. 2023.
[18] Mr Sasidhar Reddy Gaddam and DOI : 10.48047/IJCNIS.14.3.1283, “Java-Driven Trustworthy And Reliable Deep Learning For Cyberattack Detection In Industrial Iot”, Int. j. commun. netw. inf. secur., vol. 14, no. 3, pp. 1274–1283, Apr. 2022.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY