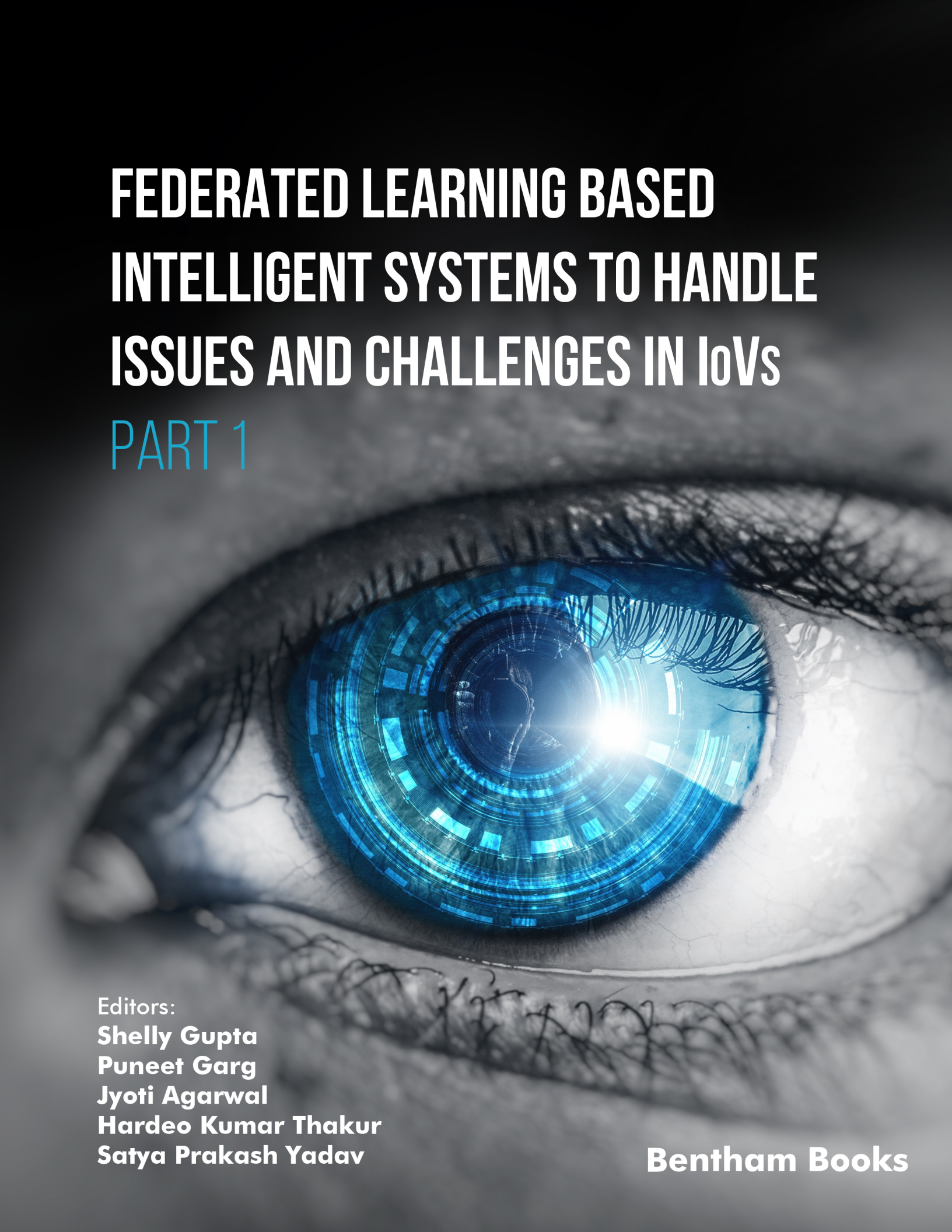
FEDERATED LEARNING BASED INTELLIGENT SYSTEMS TO HANDLE ISSUES AND CHALLENGES IN IoVs

PART 1



Editors:
Shelly Gupta
Puneet Garg
Jyoti Agarwal
Hardeo Kumar Thakur
Satya Prakash Yadav

Bentham Books

Federated Learning for Internet of Vehicles: IoV Image Processing, Vision and Intelligent Systems

(Volume 3)

Federated Learning Based Intelligent Systems to Handle Issues and Challenges in IoVs

(Part 1)

Edited by

Shelly Gupta
CSE (AI) Department
KIET Group of Institutions, U.P.,
Delhi-NCR Ghaziabad, India

Puneet Garg
Department of CSE-AI
KIET Group of Institutions, Ghaziabad, U.P., India

Jyoti Agarwal
CSE Department
Graphics Era University (Deemed to be), India

Hardeo Kumar Thakur
School of Computer Science Engineering and Technology (SCSET)
Bennett University, Greater Noida
U.P., India

&

Satya Prakash Yadav
School of Computer Science Engineering and Technology (SCSET)
Bennett University, Greater Noida
U.P., India

Federated Learning for Internet of Vehicles: IoV Image Processing, Vision and Intelligent Systems

(Volume 3)

Federated Learning Based Intelligent Systems to Handle Issues and Challenges in IoVs

(Part 1)

Editors: Shelly Gupta, Puneet Garg, Jyoti Agarwal, Hardeo Kumar Thakur & Satya Prakash Yadav

ISBN (Online): 978-981-5313-02-4

ISBN (Print): 978-981-5313-03-1

ISBN (Paperback): 978-981-5313-04-8

First published in 2024.

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Ltd.
Executive Suite Y - 2
PO Box 7917, Saif Zone
Sharjah, U.A.E.
Email: subscriptions@benthamscience.net

CONTENTS

PREFACE

In an era where the Internet of Vehicles (IoVs) is altering our transportation environment, the demand for intelligent systems capable of effectively processing and analysing massive volumes of data has never been more. The convergence of IoVs with powerful machine learning algorithms has opened up new opportunities to improve road safety, efficiency, and user experience. However, this rapid evolution presents its own set of obstacles, ranging from data privacy concerns to the intricacies of real-time decision-making.

By examining the cutting-edge federated learning paradigm, this book, Federated Learning Based Intelligent Systems to Handle Issues and Challenges in IoVs, aims to answer these urgent problems. Federated learning, in contrast to conventional centralized methods, permits decentralized data processing, allowing cars to jointly learn from local data while maintaining privacy. This approach not only reduces the hazards connected with data exchange, but it also improves the adaptability of intelligent systems under a variety of driving situations.

We explore the major issues that IoVs are now confronting throughout this work, such as data heterogeneity, network latency, and the requirement for strong security measures. Each chapter mixes theoretical ideas with practical examples, showing how federated learning can be used to develop resilient, intelligent systems that can thrive in the dynamic environment of connected automobiles.

We encourage you to consider the revolutionary possibilities of these technologies as you set out on this journey through the nexus of federated learning and IoVs. Our hope is that this book will not only be a valuable resource for researchers and practitioners, but will also stimulate more innovation in the sector, paving the way for smarter, safer transportation systems.

We are grateful to the authors, scholars, and practitioners who have contributed their skills to this work. We are building the foundation for a time when intelligent technologies prioritize privacy and safety over transportation.

Shelly Gupta
CSE (AI) Department
KIET Group of Institutions, U.P.,
Delhi-NCR Ghaziabad, India

Puneet Garg
Department of CSE-AI
KIET Group of Institutions, Ghaziabad, U.P., India

Jyoti Agarwal
CSE Department
Graphics Era University(Deemed to be), India

Hardeo Kumar Thakur
School of Computer Science Engineering and Technology (SCSET)
Bennett University, Greater Noida
U.P., India

&

Satya Prakash Yadav
School of Computer Science Engineering and Technology (SCSET)
Bennett University, Greater Noida
U.P., India

List of Contributors

Apurva Jain	Dr. Akhilesh Das Gupta Institute of Technology & Management, New Delhi, India
Achal Kaushik	Bhagwan Parshuram Institute of Technology, GGSIPU, New Delhi, India
Anurag Gupta	CSE AI Department, KIET Group of Institutions, Ghaziabad, India
Anjali Chauhan	CSE AI Department, KIET Group of Institutions, Ghaziabad, India
Arvind Panwar	School of Computing Science and Engineering, Galgotias University, Greater Noida, India
Gopal Krishna	Uttaranchal Institute of Technology, Uttaranchal University, Dehradun, India
Gaurav Singh Negi	Uttaranchal Institute of Technology, Uttaranchal University, Dehradun, India
Jyoti Agarwal	Graphic Era University, Dehradun, India
Jitendra Kumar Gupta	Uttaranchal Institute of Technology, Uttaranchal University, Dehradun, India Department of Computer Science & Engineering, Dr. BR Ambedkar National Institute of Technology, Jalandhar, India
Jyoti Parashar	Dr. Akhilesh Das Gupta Institute of Technology & Management, New Delhi, India
Kapil Kumar Sharma	Department of MCA, IMS Engineering College, Ghaziabad, India School of Computer Science and Application, IIMT University, Meerut, India
Lokesh Meena	Dr. Akhilesh Das Gupta Institute of Technology & Management, New Delhi, India
Manish Kumar	School of Computing Science and Engineering, Galgotias University, Greater Noida, India
Neha Sharma	USICT, GGSIPU, New Delhi, India Bharati Vidyapeeth College of Engineering, Paschim Vihar, New Delhi, India
Nisar Ahmad Malik	Govt Degree College Kulgam, J&K, India
Prachi Dahiya	Department of CSE, Delhi Technological University, Delhi, India
Priyanka Gaba	School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India
Soumya Sharma	Bhagwan Parshuram Institute of Technology, GGSIPU, New Delhi, India
Umang Kant	Department of CSE-AIML, KIET Group of Institutions, Ghaziabad, UP, India
Urvashi Sugandh	School of Computing Science and Engineering, Galgotias University, Greater Noida, India
Vishal Gupta	NSUT East Campus (Formerly AIACT&R), New Delhi, India
Virendra Singh Kushwah	VIT Bhopal University, Sehore, India

CHAPTER 1

Technologies to Solve the Routing Issues in IoVs

Anurag Gupta[1] and **Anjali Chauhan**[1,*]

[1] *CSE AI Department, KIET Group of Institutions, Ghaziabad, India*

Abstract: This book chapter explores the challenges and technologies involved in solving routing issues in the context of the Internet of Vehicles (IoV). The IoV represents a dynamic and complex network environment that connects vehicles, infrastructure, and various other entities. Efficient routing is crucial for timely and reliable information exchange in such networks. The chapter begins by discussing the unique challenges associated with routing in IoV, such as frequent topology changes, limited bandwidth, and high vehicle mobility. It emphasizes the need for robust and efficient routing protocols to ensure seamless data delivery in vehicular networks. Next, the chapter provides a comprehensive review of existing routing techniques and protocols designed specifically for IoV. It covers geographic routing, cluster-based routing, and hybrid routing approaches, examining their strengths, limitations, and applicability to different IoV scenarios. The chapter also discusses the importance of considering quality-of-service (QoS) metrics, such as latency, reliability, and energy efficiency, when designing routing solutions for IoV. Furthermore, the chapter explores advanced technologies that can enhance routing performance in IoV. It delves into the integration of IoV with cloud computing, edge computing, and the Internet of Things (IoT). These technologies offer additional computational resources, data storage capabilities, and real-time data processing at the network edge, leading to improved routing efficiency and reduced latency. The chapter also highlights the role of artificial intelligence (AI) and machine learning (ML) techniques in addressing routing challenges in IoV. It explores how AI and ML algorithms can analyze and predict vehicular mobility patterns, optimize routing decisions, and mitigate network congestion. The chapter emphasizes the potential of AI and ML to adaptively optimize routing strategies based on real-time network conditions. Finally, the chapter concludes by discussing open research challenges and future directions for solving routing issues in IoV. It identifies areas such as intelligent routing protocols, energy-efficient routing schemes, and security mechanisms as critical research domains. The chapter underscores the importance of ongoing research and development to ensure the efficient and secure operation of IoV routing. Overall, this book chapter provides a comprehensive overview of the technologies proposed to address routing issues in the IoV. It serves as a valuable resource for researchers, practitioners, and policymakers working in the field of vehicular networking, offering insights into the challenges, solutions, and future directions for efficient and reliable routing in IoV environments.

[*] **Corresponding author Anjali Chauhan:** CSE AI Department, KIET Group of Institutions, Ghaziabad, India; E-mail: anjisingh.chauhan@gmail.com

Shelly Gupta, Puneet Garg, Jyoti Agarwal, Hardeo Kumar Thakur & Satya Prakash Yadav (Eds.)

Keywords: Machine learning, Anomaly detection, Artificial intelligence, Federated learning, Internet of vehicles, Routing protocols.

INTRODUCTION TO ROUTING ISSUES IN IOV

Routing plays an important role when we implement communication between the Internet of Vehicles. While the network of the Internet of Vehicles provides a real-time information on the road and the information of the vehicles, it becomes necessary to understand IOT, IoV, and Intelligent IoV Systems. Hence, further in this section, we understand these concepts well [1].

Overview of IoV and Related Concepts

The world we live in today is becoming increasingly connected, transforming the way we interact with our surroundings and each other. At the heart of this digital revolution lies the Internet of Things (IoT), a groundbreaking concept that has the potential to revolutionize various aspects of our lives. The IoT refers to a vast network of interconnected devices, objects, and systems, all equipped with sensors, software, and connectivity, enabling them to collect, exchange, and analyze data [2].

One of the most useful applications of IoT is the Internet of Vehicles [2]. The automotive industry is undergoing a profound transformation, fueled by technological advancements and the growing interconnectedness of our world. At the forefront of this revolution is the concept of the Internet of Vehicles (IoV), an innovative paradigm that combines transportation and information technologies to create a smart, efficient, and interconnected vehicular ecosystem [3]. The IoV leverages the power of the Internet of Things (IoT) to connect vehicles, infrastructure, and passengers, enabling seamless communication, data sharing, and intelligent decision-making. In this chapter, we will explore the fascinating realm of the Internet of Vehicles, uncovering its principles, applications, and the transformative impact it holds for transportation systems of the future. In order to maintain an efficient system for IoVs, we needed to build an Intelligent Internet of Vehicles. The concept of the Intelligent Internet of Vehicles (IoV) takes the interconnectedness of vehicles to a whole new level by incorporating advanced technologies and intelligent systems. By leveraging the power of artificial intelligence (AI), machine learning, and data analytics, the IoV transforms vehicles into intelligent entities capable of making autonomous decisions, adapting to changing conditions, and providing personalized services. Intelligent IoV systems can analyze vast amounts of data collected from various sources, such as sensors, cameras, and infrastructure, to make informed decisions about navigation, traffic management, and safety. With AI algorithms continuously learning from real-time data, vehicles become more efficient, responsive, and

capable of communicating and collaborating with each other and the surrounding environment [4]. The Intelligent IoV holds immense potential in revolutionizing transportation, offering optimized routes, predictive maintenance, intelligent parking solutions, and enhanced safety features. By embracing intelligence, the IoV promises to reshape the way we travel, making our journeys more efficient, convenient, and enjoyable.

Importance of Efficient Routing in IoV

Efficient routing is of paramount importance in the Internet of Vehicles (IoVs) as it directly impacts the overall performance, safety, and reliability of vehicular networks. The IoVs ecosystem encompasses a vast network of interconnected vehicles, infrastructure, and various smart devices, all of which rely on effective routing to enable seamless communication and efficient data exchange. This section explores the significance of efficient routing in IoVs, highlighting its various benefits and implications [5].

Enhancing Traffic Management and Congestion Control

Efficient routing algorithms and protocols play a crucial role in managing traffic flow and alleviating congestion in IoVs. By intelligently directing vehicles through optimal routes, traffic congestion can be minimized, leading to improved overall traffic efficiency and reduced travel time. Effective routing enables traffic management systems to dynamically adapt and reroute vehicles based on real-time traffic conditions, ensuring smooth traffic flow and minimizing bottlenecks [6].

Enabling Vehicular Services and Applications

IoVs offer a plethora of services and applications to enhance the driving experience and provide value-added functionalities. Efficient routing is crucial for enabling these services, such as location-based services, navigation systems, infotainment, and vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication. Routing algorithms ensure that the relevant data is efficiently delivered to the intended recipients, enabling a wide range of IoVs applications to function optimally [7].

Optimizing Resource Utilization and Energy Efficiency

Efficient routing algorithms contribute to optimizing resource utilization and energy efficiency in IoVs. By dynamically determining the most energy-efficient routes and minimizing unnecessary vehicle movement, routing protocols can help reduce fuel consumption and minimize carbon emissions. Furthermore, intelligent

CHAPTER 2

Mapping the Intellectual Structure of Internet of Vehicles Research: A Bibliometric Analysis of Emerging Technologies and Applications

Urvashi Sugandh[1], Arvind Panwar[1], Priyanka Gaba[2,*] and **Manish Kumar[3]**

[1] *School of Computing Science and Engineering, Galgotias University, Greater Noida, India*

[2] *School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India*

[3] *School of Computing Science and Engineering, Galgotias University, Greater Noida, India*

Abstract: The Internet of Vehicles (IoV) is an emerging field that has attracted a lot of attention from researchers and practitioners alike. It encompasses a range of technologies and applications that enable communication and data exchange between vehicles, infrastructure, and other connected devices. As the IoV continues to evolve, it is important to understand the intellectual structure of the research that underpins this field. In this paper, we conduct a bibliometric analysis of IoV research to map its intellectual structure and identify emerging technologies and applications. We conducted a systematic review of the literature using bibliometric analysis techniques, including co-citation analysis and network visualization. We analyzed the publication and citation patterns of IoV research, identified the most influential authors, journals, and institutions, and explored the intellectual structure of the field using network analysis techniques. Our results show that IoV research has grown rapidly over the past decade, with a significant increase in publications and citations in recent years. The study also identified several emerging technologies and applications in IoV research, including connected vehicles, vehicular networks, autonomous driving, and smart transportation systems. These emerging technologies and applications have the potential to transform the transportation industry and improve road safety, traffic management, and energy efficiency.

Keywords: Bibliometric analysis, Emerging technologies, Internet of things (IoT), Internet of vehicles (IoV).

INTRODUCTION

The Internet of Vehicles (IoV) is an emerging field that integrates communication and computing technologies with transportation systems to provide innovative

* **Corresponding author Priyanka Gaba:** School of Computing Science and Engineering, Bennett University, Greater Noida, India; E-mail: priyanka.gaba2202@gmail.com

Shelly Gupta, Puneet Garg, Jyoti Agarwal, Hardeo Kumar Thakur & Satya Prakash Yadav (Eds.)

solutions for mobility, safety, and sustainability. The rapid development of IoV has led to an increase in the number of publications on the topic in recent years. However, with such a large volume of research, it can be challenging to gain a comprehensive understanding of the intellectual structure of IoV research, including the most influential authors, journals, and institutions, as well as the emerging technologies and applications within the field [1].

To address this gap, this paper presents a bibliometric analysis of emerging technologies and applications in IoV research. The study aims to provide insights into the intellectual structure of IoV research, which can guide future research and practice in the field. Specifically, the study aims to identify the most influential authors, journals, and institutions in IoV research and to analyze the emerging technologies and applications within the field [2, 3].

The importance of this study lies in its potential to advance the understanding of the intellectual structure of IoV research. By analyzing the bibliographic information, authorship, citation patterns, and keywords of IoV research publications, this study can provide a comprehensive overview of the field. This overview can guide future research directions and priorities and facilitate interdisciplinary collaborations across different domains [4].

The rest of the paper is organized as follows. First, a literature review is presented to provide a background on the concept of IoV and to review previous bibliometric studies on the topic. Second, the methodology of the study is described, including the selection criteria for the literature and data sources and data collection and analysis procedures. Third, the results and findings of the study are presented, including an overview of the publication and citation patterns in IoV research, visualization of the intellectual structure of IoV research, identification of the most influential authors, journals, and institutions, and analysis of the emerging technologies and applications in IoV research. Fourth, the discussion and implications of the findings are presented, including the interpretation of the results in the context of IoV research, implications for future research directions and priorities, and the contribution of the study to the understanding of the intellectual structure of IoV research. Finally, the paper concludes with a summary of the main findings and contributions of the study, limitations and suggestions for future research, and final thoughts on the significance of the study for IoV research and practice.

Background Information on the Internet of Vehicles (IoV) and its Growth

The Internet of Vehicles (IoV) is an emerging field that aims to connect vehicles with each other, as well as with the surrounding infrastructure and network, to provide various services related to transportation, safety, and efficiency. IoV is a

natural extension of the Internet of Things (IoT), where everyday objects are connected to the Internet to enable smarter and more efficient operations. However, in case of IoV, the objects are vehicles, which pose additional challenges and opportunities [5].

The growth of IoV has been remarkable in recent years, driven by advancements in communication and computing technologies, as well as the increasing demand for innovative solutions for transportation and mobility [6, 7]. According to a report by Allied Market Research, the global IoV market is expected to reach $365 billion by 2025, with a compound annual growth rate (CAGR) of 21.1% from 2018 to 2025. The report highlights the increasing adoption of IoV in various applications, such as fleet management, intelligent transportation systems, and connected cars. The growth of IoV is also reflected in the increasing number of publications and research studies on the topic. A bibliometric analysis of IoV research can provide insights into the intellectual structure of the field, including the most influential authors, journals, and institutions, as well as the emerging technologies and applications within the field.

Importance of Studying the Intellectual Structure of IoV Research

Studying the intellectual structure of Internet of Vehicles (IoV) research is important for several reasons. First, it provides insights into the state of the art and the most influential works, authors, and institutions within the field. This information can help researchers and practitioners identify the key trends, gaps, and opportunities in IoV research and guide future research and practice [8, 9].

Second, bibliometric analysis can reveal emerging technologies and applications within IoV research, which can help researchers and practitioners stay up-to-date with the latest developments and contribute to the advancement of the field. For example, the analysis may reveal new applications of IoV, such as smart parking, intelligent charging, or automated driving, which can inspire new research ideas and collaborations [10].

Third, studying the intellectual structure of IoV research can foster interdisciplinary collaborations and partnerships. IoV research involves various disciplines, such as computer science, engineering, transportation, and social sciences. By identifying the most influential authors and institutions, bibliometric analysis can facilitate interdisciplinary collaborations and help bridge the gap between different fields and perspectives.

Fourth, bibliometric analysis can help identify the research networks and communities within IoV research, which can provide valuable resources, support, and feedback for researchers and practitioners. By understanding the connections

CHAPTER 3

Influence of Wireless Sensor Network in Internet of Vehicles

Neha Sharma[1,2,*], **Vishal Gupta**[3] and **Jyoti Agarwal**[4]

[1] *USICT, GGSIPU, New Delhi, India*

[2] *Bharati Vidyapeeth College of Engineering, Paschim Vihar, New Delhi, India*

[3] *NSUT East Campus (Formerly AIACT&R), New Delhi, India*

[4] *Graphic Era University, Dehradun, India*

Abstract: The integration of Wireless Sensor Networks (WSNs) and the Internet of Vehicles (IoV) has emerged as an area of growing interest in recent years. WSNs provide an efficient means of gathering data from the environment, while the Internet of Vehicles empowers communication between vehicles, infrastructure, and among vehicles. However, the integration of WSNs and the Internet of Vehicles is challenging due to the high mobility of vehicles and the limited bandwidth of wireless communication. This bibliometric analysis examines the research trends and patterns in the area of Wireless Sensor Networks and metaheuristics for the Internet of Vehicles (IoV). Through a systematic analysis of publications in the Web of Science database, the study found that research on Wireless Sensor Networks for the Internet of Vehicles has been steadily increasing since 2010, with a peak in 2019. China was identified as the leading country in terms of research output, followed by the United States and India. The most common keywords associated with wireless sensor networks for IoV include "Internet of Things," "routing," "security," "energy efficiency," and "vehicle-to-vehicle communication." The analysis also revealed that the most popular research areas include routing protocols, energy efficiency, security, and vehicle-to-vehicle communication. This study provides valuable insights into the current state of research on WSNs for IoV and highlights the gaps between these two. Also, it shows the future research works done in this field discussing routing issues. Lens.org is used for data collection, and VoSviewer is used for data analysis.

Keywords: Mobility management, Data dissemination, Energy efficiency, Internet of vehicles, Metaheuristic, Quality of service, Security and privacy, Wireless sensor networks.

[*] **Corresponding author Neha Sharma:** USICT, GGSIPU, New Delhi, India and Bharati Vidyapeeth College of Engineering, Paschim Vihar, New Delhi, India; E-mail: neha.sh.2689@gmail.com

Shelly Gupta, Puneet Garg, Jyoti Agarwal, Hardeo Kumar Thakur & Satya Prakash Yadav (Eds.)

INTRODUCTION

The rapid progress in science and technology has prompted us to choose increasingly complex and unconventional techniques. In these cutting-edge technologies, the Internet of Things (IoT) is a standard bearer [1, 2]. We can sense and operate the required things remotely thanks to the Internet of Things [3]. A WSN is made up of several tiny, low-power sensor nodes that are limited in their bandwidth, computational capability, and energy supply but are nonetheless able to detect physical occurrences. WSNs are vulnerable to numerous assaults since they are typically installed in open, unprotected regions [4-6]. WSNs are vulnerable to several security vulnerabilities because of their self-organizing nature, constrained bandwidth, dispersed wireless operations, multi-hop traffic forwarding, and reliance on additional sensor nodes. A large number of intermediary nodes are used by wireless sensor nodes to transport data to the sink after processing it for improved performance [7-9]. These nodes work together to create a wire-free sensor network that can gather data and communicate it to the user upon request (sink). WSN may be used to gather data on the state of the environment, a target's location, a real-time event, *etc*. [10-14].

A wireless sensor network, or WSN, uses inexpensive, small sensor nodes to keep an eye on the outside world. In the field to be felt, hundreds to thousands of sensor nodes are randomly planted. Applications like environmental monitoring, weather forecasting, precision agriculture, natural catastrophe prevention, disaster management, border surveillance, smart cities, *etc.* all heavily rely on WSN [15, 16]. It is used to observe numerous physical characteristics in the actual world, including temperature, pressure, moisture content, gas, acoustics, vibrations, *etc*. [17-21]. In a WSN, the sensor node is composed of sensors, a microcontroller, a communication module, and a power source. The sensor unit keeps track of its surroundings, gathers data, analyses it, and sends it to other sensor nodes *via* a communication unit [22-29].

To create an energy-efficient WSN, many clustering and routing protocols with various elements have been established in the literature [30-35]. The clustering approach divides the network into clusters and organizes neighboring nodes into them. The remaining nodes are referred to as cluster members, and a leader named CH will be chosen from the group of nodes [36-38]. Equal clustering is the process of creating clusters in a network with the same number of nodes, whereas unequal clustering is the process of creating clusters with an uneven number of nodes [39-41]. A Cluster Head (CH) will be chosen from each cluster based on a set of requirements. Three tasks fall within the purview of the CH: collecting data from cluster members, aggregating it, and sending it to the BS. The CH also serves as a relay node for data transmission to BS from other CHs. Fig. (**1**) depicts

the general system model of clustering. Only when the distribution of nodes is uniform can equal clustering be effective and yield superior outcomes. Uniform distribution is quite unlikely due to the nodes' haphazard placement. This causes the nodes to use energy inequitably, particularly CHs that are closest to the BS. When using multi-hop transmission, CHs closer to the base station (BS) serve as relays for remote CHs [42-49]. Therefore, CHs closer to BS exhaust their energy and pass away before their distance from BS.

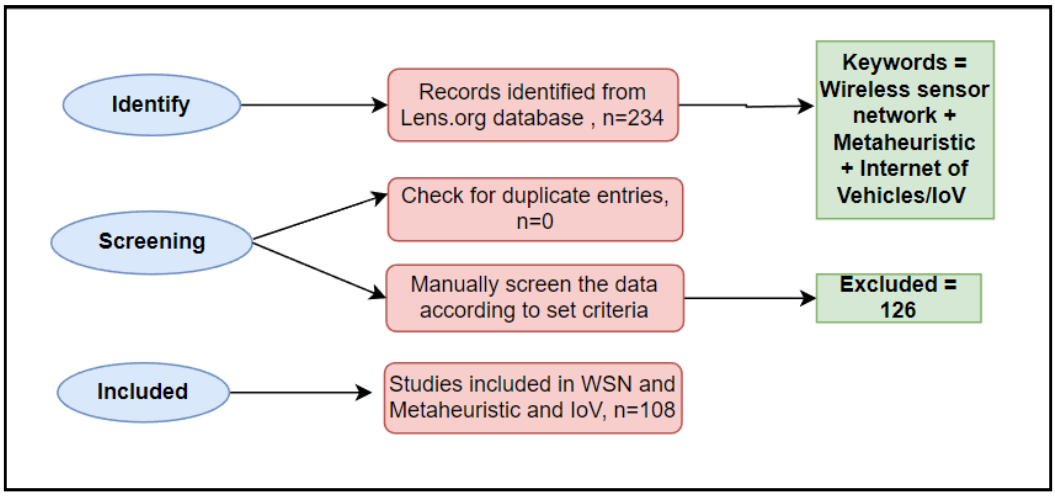


Fig. (1). Steps of publications retrieval.

Nodes in the WSN often communicate data to BS on a regular basis, making it ideal for applications that need periodic data monitoring [50-65]. Time-sensitive circumstances cause the physical environment to change suddenly and quickly, which results in multiple data transmissions and a considerable impact on energy usage. A reactive protocol, which transmits data when the threshold value is crossed [66-81], is introduced to solve this problem. Data will only be transmitted *via* the reactive protocol when the detected value is greater than the threshold value. Both hard and soft threshold values are included in the threshold value [82-85]. Following the selection of the CHs, it broadcasts to the other members of the cluster two threshold values (hard threshold and soft threshold values). The cluster members will broadcast the data to the CH when the detected value exceeds the hard threshold value [86-89]. By limiting the nodes' ability to broadcast to times when the detected value is within the range of interest, the hard threshold attempts to decrease the number of transmissions. By excluding any transmissions with a minimal or no change in the perceived value from the hard threshold value, the soft threshold significantly minimizes the number of transmissions [90-92]. The soft threshold can be changed depending on the

CHAPTER 4

Federated Learning in Secure and Reliable Systems for IoVs

Umang Kant[1,*] and **Prachi Dahiya**[2]

[1] *Department of CSE-AIML, KIET Group of Institutions, Ghaziabad, UP, India*

[2] *Department of CSE, Delhi Technological University, Delhi, India*

Abstract: The Internet of Vehicles (IoV) is an emerging technology that allows vehicles to communicate with each other and with the infrastructure around them. This technology has the potential to revolutionize the transportation industry, but it also raises concerns about the security of the data that is shared among vehicles, with their base stations and infrastructure.

In this context, secure data-sharing methodologies are essential to protect sensitive information, such as location, driving patterns, data of the people travelling in the vehicle, and protection of shared data from malicious factors. This chapter explores some of the methods that can be used for secure data sharing in the IoV. One approach is to use encryption and decryption techniques to protect data in transit and at rest. This method involves encoding the data in a way that only authorized parties can access it, and decoding it when it reaches its destination. Another approach is to use blockchain technology, which provides a decentralized and immutable ledger that can be used to store and verify data. Additionally, access control mechanisms, such as role-based access control, can be used to limit the access of different users to specific data sets. This method ensures that only authorized parties can access sensitive data.

In conclusion, secure data-sharing methodologies are crucial for the successful implementation of the IoV. Encryption and decryption, blockchain technology, and access control mechanisms are some of the methods that can be used to protect sensitive information and maintain the privacy and security of the data.

Keywords: Blockchain, Heterogeneity, Internet of things, Machine learning, Scalability.

INTRODUCTION

Federated learning is a machine learning technique that enables multiple devices to collaboratively train a shared model while keeping their data decentralized and

[*] **Corresponding author Umang Kant:** Department of CSE-AIML, KIET Group of Institutions, Ghaziabad, UP, India; E-mail: umang.kant@gmail.com

Shelly Gupta, Puneet Garg, Jyoti Agarwal, Hardeo Kumar Thakur & Satya Prakash Yadav (Eds.)

private. In this approach, the data remains on individual devices, and only model updates are shared with a central server as shown in Fig. (**1**). Federated learning has gained a lot of attention in recent years as it offers several benefits, including privacy-preserving machine learning, reduced data transfer, and increased scalability. In the context of the Internet of Vehicles (IoVs), federated learning can be used to build intelligent systems that enable vehicles to learn from the data collected from various sources, including sensors, cameras, and other IoT devices. IoVs can generate vast amounts of data, and the ability to learn from this data can significantly improve the performance of vehicles, such as better routing, energy efficiency, and driver assistance [1, 2].

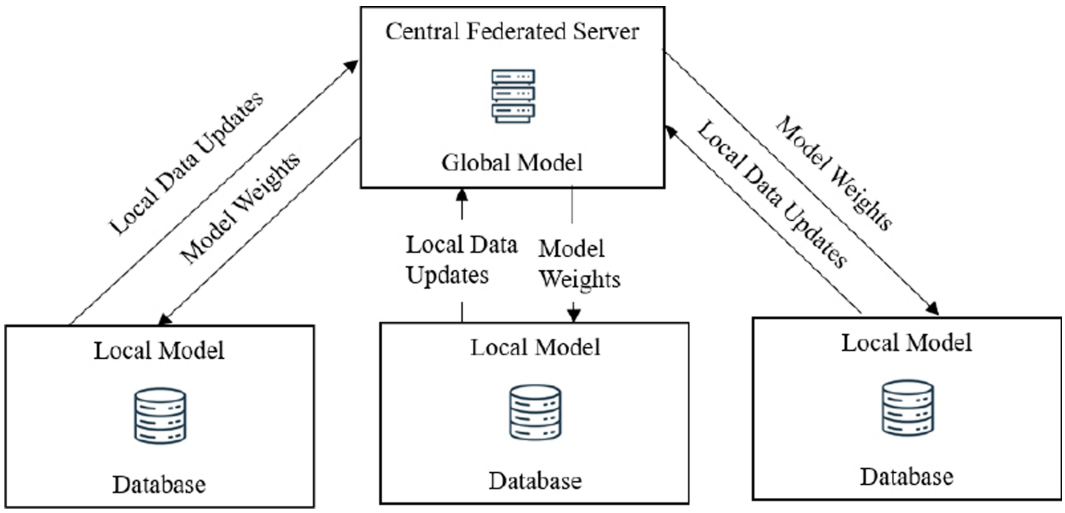


Fig. (1). Collaborated model training using federated learning.

One of the key benefits of federated learning in the context of IoVs is that it allows multiple vehicles to train a shared model while preserving the privacy of their data. This can be especially useful in scenarios where data privacy is critical, such as location tracking, driving behavior analysis, and accident prediction. By enabling vehicles to learn from each other's data without sharing it directly, federated learning can help create more intelligent and efficient systems while ensuring the privacy of individuals' data. The Internet of Vehicles (IoV), as shown in Fig. (**2**), refers to the interconnectedness of vehicles, road infrastructure, and other entities in the transportation system [3]. With the growing number of connected vehicles, the need for secure and reliable systems is becoming increasingly important. The reason is that insecure and unreliable systems in IoV can lead to accidents, loss of life, and financial losses. For example, hackers could compromise the system and gain control of a vehicle, resulting in an accident [4, 5].

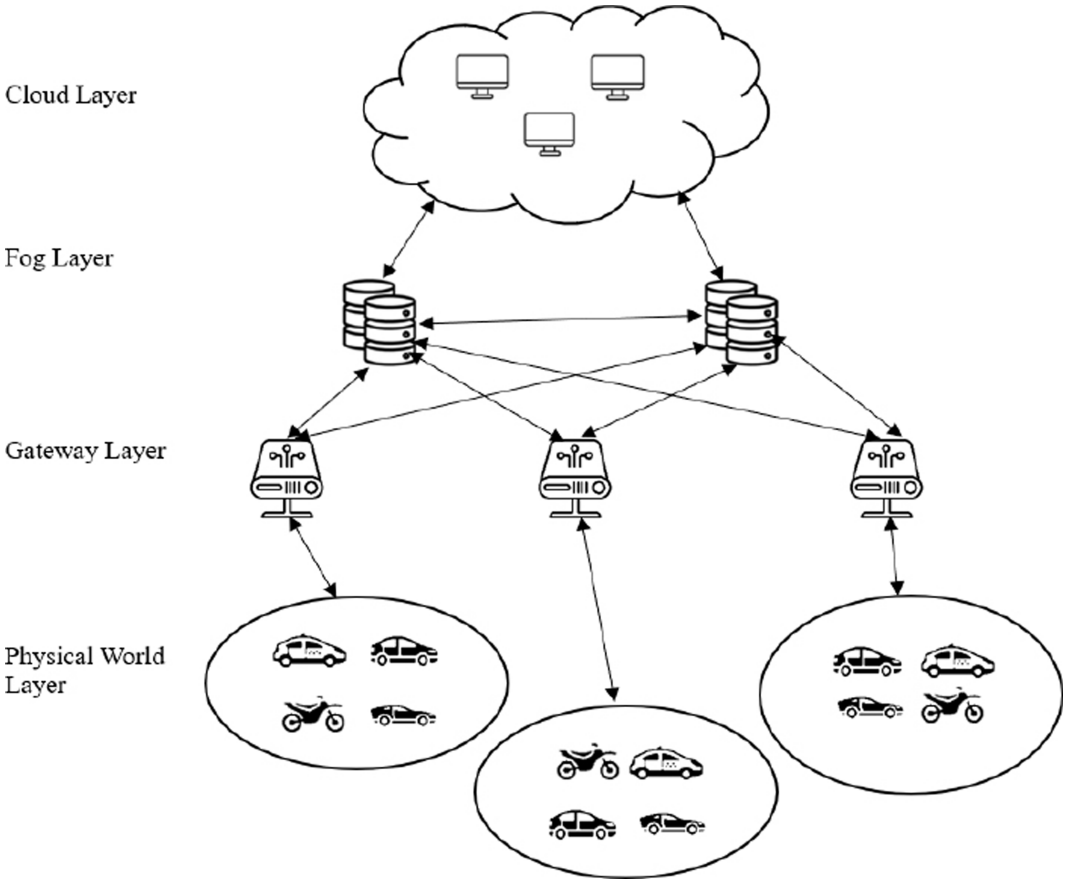


Fig. (2). IoV architecture.

Federated learning is a technique used in machine learning that allows multiple parties to train a shared model without sharing their data. Instead of sending data to a central server for processing, data remains on local devices and is only used to update the shared model. This approach can help address the security and privacy concerns in IoV systems. By using federated learning, the data remains on local devices, reducing the risk of data breaches. Additionally, since data is not being sent to a central server, there is less risk of a single point of failure that could compromise the entire system. Furthermore, federated learning allows the system to learn from multiple sources, resulting in a more accurate and robust model [6, 7].

Federated Learning has emerged as a viable solution to address the privacy concerns associated with traditional machine learning techniques, such as Automated Machine Learning. While these advanced technologies offer numerous

CHAPTER 5

Adaptive Solutions for Data Sharing in IoVs

Virendra Singh Kushwah[1], Apurva Jain[2], Jyoti Parashar[2,*], Lokesh Meena[2] and **Nisar Ahmad Malik[3]**

[1] *VIT Bhopal University, Sehore, India*

[2] *Dr. Akhilesh Das Gupta Institute of Technology & Management, New Delhi, India*

[3] *Govt Degree College Kulgam, J&K, India*

Abstract: With the rapid growth of the Internet of Vehicles (IoV), there is an increasing need for effective and secure data sharing among vehicles, infrastructure, and other entities within the IoV ecosystem. However, traditional data-sharing mechanisms face numerous challenges, such as heterogeneity of data formats, privacy concerns, and scalability issues. In this study, we propose adaptive solutions for data sharing in IoVs, which aim to address these challenges and facilitate efficient and secure data exchange. Our approach leverages adaptive techniques to dynamically adjust data-sharing mechanisms based on the context and requirements of the IoV environment. We present a comprehensive overview of the proposed solutions, including data format transformation, privacy-preserving techniques, and scalable data-sharing protocols. We also discuss the potential benefits and limitations of our approach and provide insights into future research directions in the field of data sharing in IoVs

Keywords: Adaptive, Accessibility, Centralized, IoV, Security.

INTRODUCTION

Because it permits real-time communication between diverse entities such as automobiles, handheld devices carried by pedestrians, and roadside units, the Internet of Vehicles (IoVs) makes it feasible to control traffic in a manner that is both safer and more effective. Because IoV is superior to other technologies, academic research into the Internet of Vehicles applications such as autonomous driving, vehicle management, high-definition (HD) maps, and big data awareness has proven to be fruitful. It stands to reason that the protection of this information as it is shared among IoV participants should be considered an essential compo-

* **Corresponding author Jyoti Parashar:** Dr. Akhilesh Das Gupta Institute of Technology & Management, New Delhi, India; E-mail: jyoti.parashar123@gmail.com

Shelly Gupta, Puneet Garg, Jyoti Agarwal, Hardeo Kumar Thakur & Satya Prakash Yadav (Eds.)

nent of IoV infrastructure given that the Internet of Vehicles applications rely heavily on vast amounts of data collected from vehicles [1, 2].

Existing IoV systems, on the other hand, have shortcomings that could put the safety of the data-sharing paradigm in automobiles at risk.

- The security of all information and systems. The Client-Server (CS) paradigm, on which the great majority of IoV systems are built, introduces a potential single point of failure and invites malevolent attacks such as Distributed Denial of Service (DDoS) attacks and Sybil attacks, both of which have the potential to render the entire IoV system unusable [3]. This is due to the fact that the CS model includes a client that acts as both a server and a client. The information pertaining to vehicles and RSUs that are stored in the centralized database is susceptible to being manipulated by adversaries, who might use this information to create havoc on the streets.
- Keeping one's identity a secret from others. Analyzing patterns in data acquired from vehicles, such as driving track data, which is exchanged wirelessly, allows attackers to discover the identities of automobiles. This type of data includes driving track data. People's enthusiasm for sharing vehicle data is dampened as a result of the possibility of disclosure of their identity, which in turn slows down the real implementation of IoV systems [4, 5].

In order to solve these problems, Horng and colleagues came up with a method for secure data sharing in car networks that is based on the identification of the user. However, because their architecture is dependent on dependable cloud computing nodes, it contains a single point of failure, which is a significant weakness. It is possible that frequent modifications to the group members could place a large computational load on the group manager. This is because the group manager serves as a trusted arbiter in the BBS04 group signature-based privacy-preserving vehicular communication technique that was developed by Wei *et al.* In the linkable location-based services system proposed by Yadav *et al.*, which is based on a modified Linkable Spontaneous Anonymous Group (LSAG) [6] ring signature approach, the trusted parties, also known as RSUs, are required to serve as signature proxies. This is the case even if the LSAG ring signature technique was modified. Constructing decentralized and zero-trust vehicular networks ought to be seen as a fashionable security alternative in future IoV systems, as such centralized approaches are no longer sufficient to deal with the sophistication of today’s cyberattacks. This is because the Internet of Vehicles (IoV) is a network of vehicles [7, 8].

The development of blockchain technology has captured a significant amount of people's interest in recent years. There is a reason to believe that blockchain

technology, which possesses beneficial characteristics such as decentralization, trustworthy execution, and tamper resistance, may be able to assist with the aforementioned problems. One such concept for assuring the trustworthy exchange of data in IoV networks comes from the research conducted by Chen *et al.*, who propose for a quality-driven incentive system based on consortium blockchains. This particular proposal can be found in the work of Chen *et al.* To make the exchange of confidential information easier, Zhou and his colleagues developed LVBS, a condensed blockchain optimized for automobiles [9, 10]. These solutions do not take into account the fact that disclosing cars' identity could potentially compromise their privacy, despite the fact that a decentralized fabric makes the system more secure. In addition, the capabilities of the currently available blockchains are unable to satisfy the demand for high throughput as well as the mobility of IoV systems. As a consequence of this, new challenges have arisen as a direct consequence of the incorporation of IoV into blockchain-based infrastructures:

The first challenge is to maintain the confidentiality of identifiers under specific circumstances. When it comes to the protection of drivers' personal information, the blockchain presents a potential security issue because it is a publicly distributed ledger. This means that anybody who has access to the internet can view its data. Even if pseudonym accounts on a blockchain can “anonymize” the identification of a vehicle, an attacker could still discover the car's true identity by monitoring and analyzing the transactions linked with it. Due to the ineffective anonymity method implemented by the blockchain, consumers are unlikely to provide information about their vehicles to the IoV systems. Despite the anonymity protections they provide, Trusted Authorities (TAs) should nevertheless be held responsible for revealing the identities of malicious nodes and penalizing them. This is the case even while TAs protect users' privacy. Therefore, IoV systems that are based on blockchain technology require a strategy that protects users' privacy when it comes to conditional identifiers [11].

Another challenging area is the capacity for rapid expansion in response to changing conditions. Due to the fact that it utilizes a large number of cutting-edge technologies, the blockchain suffers from scalability problems and speed constraints [12]. The number of consensus nodes can have a direct impact on the convergence speed of the blockchain, which in turn has an effect on the performance of the blockchain. As a result, the vast amounts of data and transactions involved in IoV systems are currently beyond the capability of the blockchain as it is.

In this study, we present a multi-sharding blockchain-based system that may be used to exchange data pertaining to vehicles in a manner that is confidential to the

CHAPTER 6

Using Natural Language Processing to Improve Safety in the Internet of Vehicles

Neha Sharma[1,*], **Soumya Sharma**[2] and **Achal Kaushik**[2]

[1] *Bharati Vidyapeeth College of Engineering, Paschim Vihar, New Delhi, India*

[2] *Bhagwan Parshuram Institute of Technology, GGSIPU, New Delhi, India*

Abstract: This chapter focuses on the applications and challenges of the Internet of Vehicles (IoV) and how Natural language processing is used in safety applications in IoV. The Internet of Things (IoT) is used to identify the internet of vehicles. The tremendous growth in the smart automotive sectors has recently led to a huge rise in interest in Internet of Vehicles (IoV) technology. IoV is used to connect objects, vehicles, and surroundings so that data and information may be transferred between networks. It also lets cars transmit and gather information about other vehicles and roadways. By easing traffic congestion, enhancing traffic management, and assuring road safety, IoV is introduced to improve the experience of road users. The challenges and problems that the contemporary IoV system faces are covered in this study. How to manage the privacy of huge groups of data and cars in IoV systems is one of the critical issues that researchers need to deal with. IoV networks may benefit from the numerous clever solutions provided by artificial intelligence (AI) technology to handle all the queries and problems. There is a deep connection between IoT and AI. Similarly, IoV being a subset of IoT and natural language processing (NLP) being a subset of AI are also deeply connected. Without NLP, it is difficult to run the voice control systems in IoV. The hands-free interface, which is provided by NLP, benefits the IoV in many ways.

NLP techniques can be used to improve safety concerns in IoV. For instance, using sensory data from the surrounding area, NLP may be used to analyze driving behavior and the surroundings in order to prevent traffic accidents. This chapter consists of a detailed survey on IoV, with its applications and challenges, and NLP technologies that can be used for safety applications.

Keywords: IoV, IoT, NLP, Safety.

[*] **Corresponding author Neha Sharma:** Bharati Vidyapeeth College of Engineering, Paschim Vihar, New Delhi, India; E-mail: neha.sh.2689@gmail.com

Shelly Gupta, Puneet Garg, Jyoti Agarwal, Hardeo Kumar Thakur & Satya Prakash Yadav (Eds.)

INTRODUCTION

The Internet of Vehicles (IoV) is a rapidly growing area of research, with the potential to significantly improve transportation safety. The Internet of Vehicles (IoV) refers to the integration of vehicles with various sensors, communication networks, and data analysis technologies. Natural Language Processing (NLP) is a branch of artificial intelligence that focuses on enabling computers to understand, interpret, and respond to human language [40, 41].

Background and Motivation

This chapter provides an overview of IoV and NLP and explores the potential benefits of combining these two technologies. However, the vast amounts of data generated by IoV systems can be difficult to analyze and make sense of. This paper explores the use of natural language processing (NLP) techniques to improve the safety of the IoV. Specifically, we propose a system that uses NLP to analyze and classify driver behavior based on data from IoV sensors. The system uses machine learning algorithms to automatically identify potentially dangerous behaviors, such as aggressive driving or distracted driving and provides real-time alerts to the driver or other relevant parties [42].

The IoV is a network of connected vehicles and infrastructure that enables real-time communication and data exchange between vehicles, drivers, and the environment [1]. This technology has the potential to significantly improve transportation safety, but it also poses new challenges in terms of managing and analyzing the vast amounts of data generated by IoV systems. One way to address these challenges is to use NLP techniques to extract insights from the data and identify potentially dangerous driving behaviors [43, 44].

IoV needs software to keep track of its location and defend against harmful assaults on its network. Self-driving, safe driving, social driving, mobile apps, and electric cars are displayed by the IoV. The whole network, which consists of vehicles, roads, roadside devices, sensors, and people, coordinates and maintains communication [2, 3]. IoV connects two futuristic dreams: 1) vehicle networking and 2) vehicle intelligence [4] and focuses on the integration of objects, such as people, vehicles, things, systems, and situations to create an intelligent system dependent on computing and communication abilities that aid administrations, (for example, worldwide traffic productivity and the executive's administration dependent on contamination levels, street conditions, clog traffic level, or vehicular security administrations) for enlightenment [5, 45].

One of the most significant benefits of combining IoV and NLP is the improved communication between drivers and their vehicles. NLP systems can enable

drivers to interact with their vehicles using natural languages, such as spoken commands or text messages [46].

For example, a driver could ask their car for directions to a specific location, and the car could respond with a spoken response or a visual map. This would make driving easier by navigating in unfamiliar areas, thereby, reducing the likelihood of accidents.

The Internet of Vehicles (IoV)

The IoV is a concept that is rapidly gaining momentum in the automotive industry. The idea is to create a connected network of vehicles that can communicate with each other and with other systems. The goal is to improve safety, efficiency, and convenience for drivers [6]. IoV systems typically include sensors and communication technologies that allow vehicles to collect and exchange data amongst themselves and with other systems [7]. For example, vehicles can share information about road conditions, traffic congestion, and weather. This data can then be used to optimize driving routes, reduce accidents, and enhance the driving experience [47, 48].

The Internet of Vehicles refers to the integration of vehicles with the Internet and other communication technologies, allowing vehicles to communicate with each other and with other devices and systems in order to improve safety, efficiency, and overall driving experience [8, 9].

According to a survey (shown in CISION PR Newswire) conducted by Markets in 2021, the IoV market is expected to grow significantly in the coming years, with a projected compound annual growth rate of 13.8% between 2021 and 2026 [10]. The survey also found that the increasing demand for connected vehicles and the development of advanced communication technologies are among the key drivers of this growth [11].

Another survey conducted by Gartner in 2021 found that the most important use cases for IoV technology are related to safety and security, such as advanced driver assistance systems, collision avoidance, and vehicle tracking [12, 13]. Other important use cases include traffic management, environmental sustainability, and convenience features such as in-vehicle entertainment and personalized recommendations [14, 15].

Overall, the Internet of Vehicles has the potential to transform the way we think about transportation and to provide a wide range of benefits for drivers, passengers, and society as a whole [16]. However, much like any emerging technology, there are also challenges with IoV that should be addressed, including

CHAPTER 7

Federated Learning-Based Frameworks for Trusted and Secure Communication in IoVs

Kapil Kumar Sharma[1,2], Gopal Krishna[3,*], Gaurav Singh Negi[3] and **Jitendra Kumar Gupta[3,4]**

[1] *Department of MCA, IMS Engineering College, Ghaziabad, India*

[2] *School of Computer Science and Application, IIMT University, Meerut, India*

[3] *Uttaranchal Institute of Technology, Uttaranchal University, Dehradun, India*

[4] *Department of Computer Science & Engineering, Dr. BR Ambedkar National Institute of Technology, Jalandhar, India*

Abstract: Federated learning is a machine learning approach that allows many parties to collaborate on training a model without disclosing their raw data. Federated learning is critical in the context of the Internet of Vehicles (IoVs) because it allows cars to exchange sensitive data while maintaining privacy and security. This chapter of the book delves into federated learning-based frameworks for trustworthy and secure communication in IoVs. The chapter investigates the difficulties associated with training machine learning models in IoVs and evaluates the various federated learning frameworks offered for this context. The chapter examines the significance of secure communication and privacy protection in federated learning and the many strategies and procedures utilized to achieve these objectives. It investigates federated learning's possible applications in IoVs, such as traffic prediction and management, intelligent routing optimization, and vehicle safety and security enhancement. Finally, the chapter discusses future research areas for federated learning in IoVs and their implications for the discipline. While numerous federated learning frameworks have been developed for IoVs, privacy and security issues must be solved before federated learning can realize its full potential in IoVs. The chapter suggests several potential future research areas, including developing new federated learning frameworks that better address the challenges of IoVs, exploring additional federated learning applications in this context, and evaluating the performance and efficiency of different federated learning approaches in IoVs.

Graphical Abstract: Graphical abstract of this paper is as shown in Fig. (**1**) below.

Keywords: Federated learning, IoVs, Machine learning, Privacy preservation, Secure communications.

[*] **Corresponding author Gopal Krishna:** Uttaranchal Institute of Technology, Uttaranchal University, Dehradun, India; E-mail: gopalkrishna@gmail.com

Shelly Gupta, Puneet Garg, Jyoti Agarwal, Hardeo Kumar Thakur & Satya Prakash Yadav (Eds.)

INTRODUCTION

In machine learning, federated learning, colloquially referred to as collaborative learning, is a method of training an algorithm by combining multiple training sessions, each with a dataset of its own. This differs from conventional centralized techniques that combine local datasets into one training session, as well as approaches that assume that local data samples are evenly distributed. Federated learning tackles critical challenges such as data privacy and security, rights of access, and different data by allowing a large number of people to collaborate on constructing a single, effective machine-learning model with no sharing of data. Defense, communications, the Internet of Things (IoT), and the pharmaceutical business all employ federated learning. Is federated learning more effective than pooled data learning? is one of the most important unanswered questions. Additional unsolved concerns include the device's reliability and the impact of the malicious actor on the learned model [1 - 4]. As in the case of a team presentation or a report, several individuals share their data remotely to train a single, collaborative deep learning model, regularly improving on it. Each participant receives the model from the cloud data center, often a pre-trained basis model. The model is trained on the participant's data before the summation and encryption of the new model configuration. Model enhancements are uploaded to the cloud for encryption, averaging, and integration into a centralized model. Team-based training is iterative until a model is fully trained [5 - 7]. Like a team presentation or a report, many people remotely share their data to train a single model, always learning from it. Each participant receives the model from the cloud data center, usually a pre-trained basis model. They train the model with their data, then summarise and encrypt the model’s new configuration. Model updates are uploaded to the cloud, encrypted, averaged, and integrated with the centralized model. Team-based training takes iteration after iteration until the model is fully trained [8, 9]. An overview of IoVs is shown in Fig. (**2**). The intelligent linked car system transforms your automobile from a simple and direct mobile tool to the one that offers entertainment and travel information to drivers, such as real-time insights into driving data and helpful parking advice while you’re on the go. You do not need to park your car during your trip; you can connect it to your smartphone and keep an eye on your car’s attributes all the time. You and your passengers can enjoy the best of your driving life with rich AV content and a human-friendly operation interface [10].

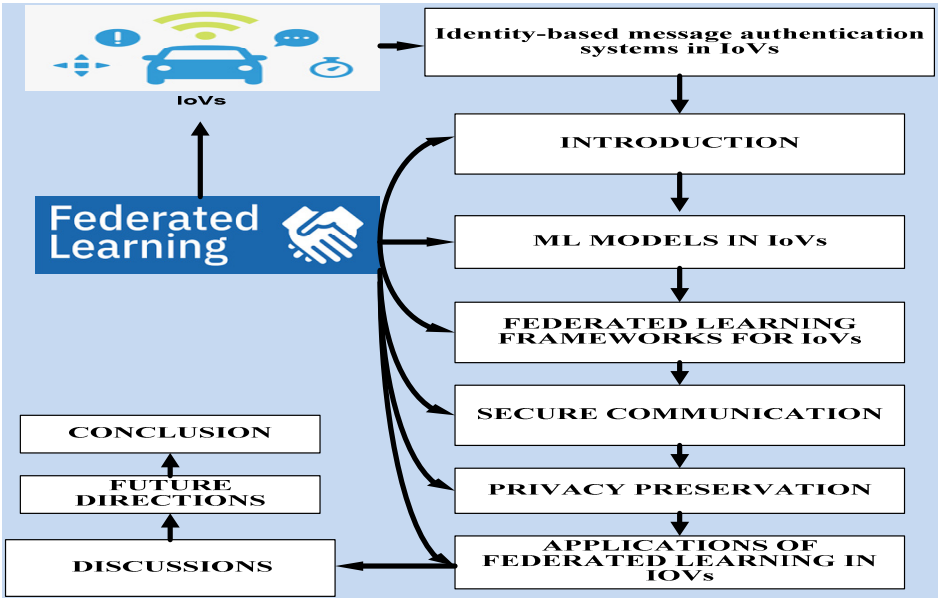


Fig. (1). Graphical abstract.

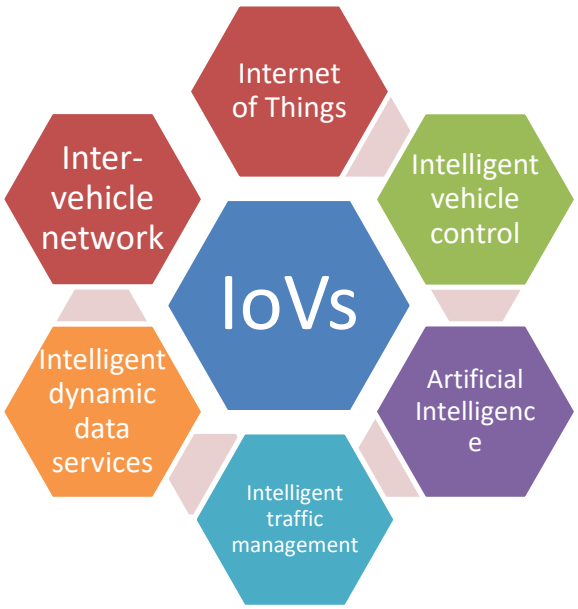


Fig. (2). Overview of IoVs.

You and your passengers can enjoy your time behind the wheel to the fullest with comprehensive AV information and an easy-to-use interface. The IoT is the foundation of the IoT. According to the IoT Internet of Vehicles (IoV) Strategic

SUBJECT INDEX

A

B

C

D

E

F

G

H

I

L

M

N

P

R

S

T

V

W