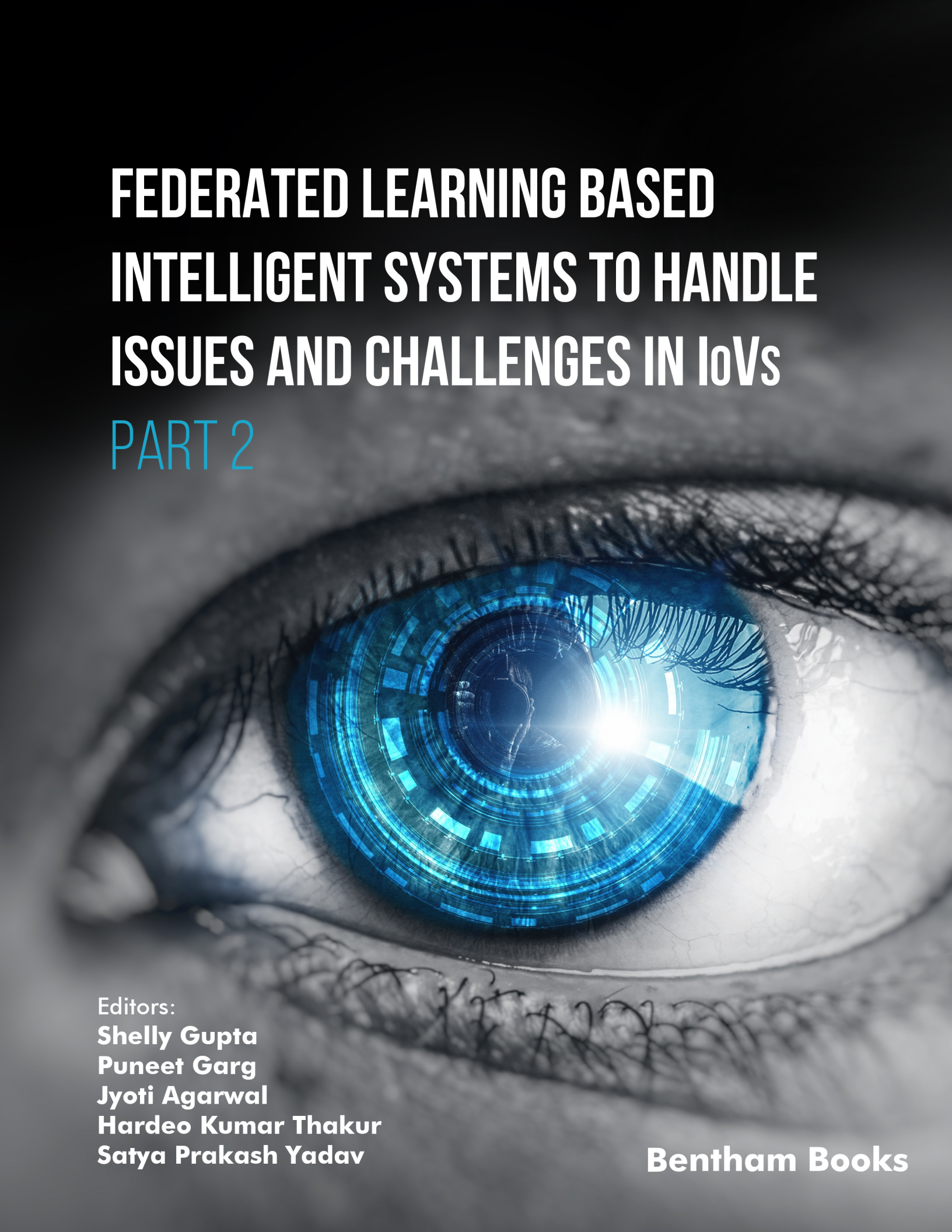
FEDERATED LEARNING BASED INTELLIGENT SYSTEMS TO HANDLE ISSUES AND CHALLENGES IN IoVs

PART 2



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 2)

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 2)

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

ISBN (Online): 978-981-5322-22-4

ISBN (Print): 978-981-5322-23-1

ISBN (Paperback): 978-981-5322-24-8

First published in 2025.

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 analyzing 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 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

Arvind Panwar	School of Computing Science and Engineering, Galgotias University, Greater Noida, India
Disha Mohini Pathak	Department of Computer Science, ABES Engineering College Ghaziabad, U.P., India
Gaurav Singh Negi	Uttaranchal Institute of Technology, Uttaranchal University, Dehradun, India
Gopal Krishna	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
Manish Kumar	School of Computing Science and Engineering, Galgotias University, Greater Noida, India
Navdeep Bohra	Department of CSE, Maharaja Surajmal Institute of Technology, Delhi, India
Neha Sharma	Bharati Vidyapeeth College of Engineering, Paschim Vihar, Delhi, India
Priyanka Gaba	School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India
Ramnarayan	Uttaranchal Institute of Technology, Uttranchal University, Dehradun, India
Somya Srivastava	Department of Computer Science, ABES Engineering College Ghaziabad, U.P., India
Shelly Gupta	CSE AI Department, KIET Group of Institutions, Ghaziabad, UP, India
Urvashi Sugandh	School of Computing Science and Engineering, Galgotias University, Greater Noida, India

CHAPTER 1

Federated Learning on Wheels: A Decentralized Approach to Privacy-Enhanced Data Collection in Internet of Vehicles

Neha Sharma[1,*], Urvashi Sugandh[2], Jyoti Agarwal[3], Arvind Panwar[2] and **Priyanka Gaba[4]**

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

[2] *School of Computing Science & Engineering, Galgotias University, Greater Noida, India*

[3] *Graphic Era Deemed to be University, Dehradun, Uttarakhand, India*

[4] *School of Computing Science & Engineering, Bennett University, Greater Noida, India*

Abstract: Due to privacy issues and the scattered nature of data produced by vehicles, the Internet of Vehicles (IOV) poses considerable hurdles for data collecting. In this chapter, we examine the idea of "Federated Learning on Wheels" (FLoW), which provides a decentralised method for IOV data collection with a focus on privacy. FLOW makes use of the onboard computer resources of cars to carry out model training locally, making sure that private information stays on the cars and is not shared with a centralised server. This strategy overcomes the shortcomings of conventional centralised data collecting approaches while simultaneously protecting user privacy. We examine the fundamentals of federated learning and how they relate to IOV, highlighting the advantages of maintaining privacy. We also look at secure aggregation procedures and confidentiality safeguards as additional methods for privacy-enhanced data acquisition in FLOW. Additionally, we emphasise the significance of accuracy and performance issues in decentralised contexts and use examples that illustrate FLOW's usefulness. We also explore security and trust issues, talking about possible weaknesses and methods to secure the reliability of participants and model updates. We also consider how blockchain technology may be incorporated for improved security and openness. We conclude by discussing FLOW future directions, difficulties, and ethical issues in order to shed light on its possible significance and legal ramifications. Overall, this chapter clarifies the relevance of Federated Learning to Wheels as a ground-breaking approach to data collecting with increased privacy in the Internet of Vehicles.

Keywords: Blockchain, Federated learning, Internet of vehicles (IOV), Privacy preservation.

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

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

INTRODUCTION

The IOV, a paradigm that facilitates seamless connection and communication among vehicles, infrastructure, and other entities in the transportation ecosystem, has emerged as a result of the fast growth of technology. Vehicles produce enormous volumes of data in the IOV on their location, speed, driving style, and sensor readings. The potential to increase traffic control, road safety, and transit effectiveness is enormous [1, 2]. However, there are several obstacles to the acquisition and use of this data, especially when it comes to privacy issues and the need for efficient data-collecting techniques.

An Overview of the Internet of Vehicles (IOV) and the Difficulties it Faces in Collecting Data

The IOV is made up of a complicated web of linked motor vehicles, roadside equipment, and infrastructure for transit. This network creates a wide variety of data, including sensor data, position data, and vehicle telemetry. However, there are several difficulties in gathering this data for analysis and decision-making. Traditional methods often depend on data gathering that is centralised, meaning that information is acquired and kept on a single server. This centralised strategy, meanwhile, raises questions about data security, privacy, and scalability. Additionally, there is a risk of data breaches when large volumes of sensitive data are sent from cars to a central server due to high connection costs.

Privacy is one of the main problems with collecting IOV data. Sensitive information including location histories, driving habits, and personal identifiers are often found in vehicle-generated data. Maintaining individual privacy is essential to earning the public's confidence and abiding by data protection laws. Concerns regarding unauthorised access, data breaches, and the possibility for abuse of personal information are brought up by the centralization of data collecting. Additionally, the transmission of massive amounts of data from automobiles to a central computer may result in security flaws and privacy issues [3 - 5].

The efficiency and scalability of centralised data collection constitute another difficulty. Massive volumes of data are produced by the IOV, and when they are sent to a central server, they might result in high communication costs and bandwidth use. Data transmission may experience delays, increased latency, and congestion as a consequence. Furthermore, managing the amount, diversity, and velocity of IOV data may provide difficulties for centralised infrastructures [6, 7].

Overview of Federated Learning as a Strategy for Improving Privacy

Federated learning has become a viable privacy-enhancing strategy to overcome the privacy issues connected to centralised data collecting. Federated learning eliminates the need to send raw data to a centralised server and enables model training on local devices, such as vehicles. Models are instead sent to the automobiles, who train themselves using their data. A global model is then created by averaging model updates. Federated learning maintains the privacy and security of the data by keeping it on the devices and only exchanging model updates. This decentralised method of machine learning encourages cooperation while reducing privacy concerns [8, 9]. Fig. (**1**) shows the concept of federated learning *vs* centralized learning.

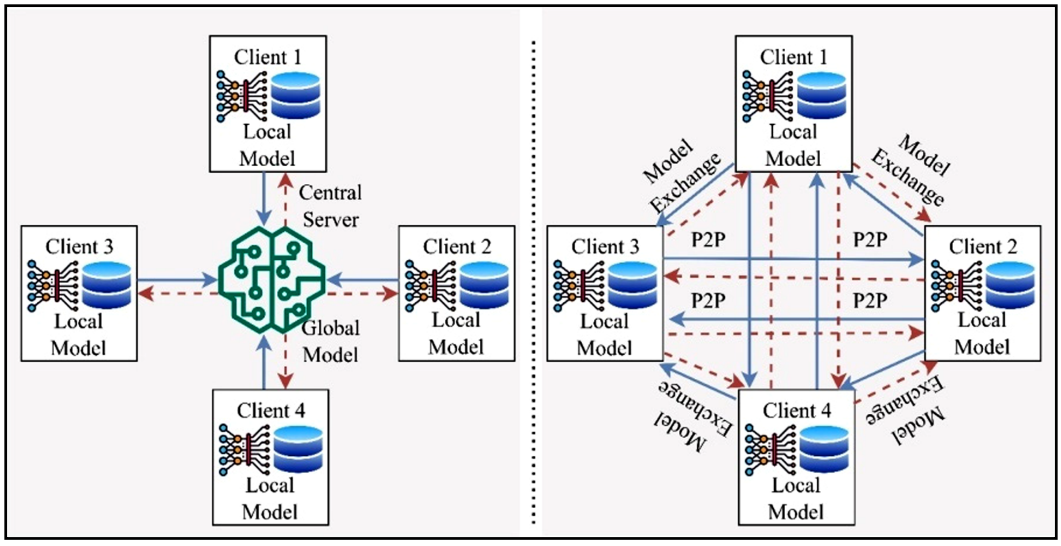


Fig. (1). Federated Learning *vs* centralized learning.

The Significance of Decentralised Data Collection in IOV

Given the sensitivity of vehicle-generated data, decentralised data gathering in IOV is of utmost importance. Vehicles gather information that may contain personally identifying data, driving habits, and past locations. It is essential to secure this sensitive data in order to uphold data protection laws and safeguard individual privacy [10, 11]. Federated learning makes it possible to gather data decentralised, protecting user privacy while keeping control over private data with the vehicle owners. With less dependence on centralised infrastructure and communication capacity, this strategy improves privacy while also enabling IOV to scale more easily and do real-time data analysis.

CHAPTER 2

Beyond Cash and Cards: Exploring the Potential of Blockchain for Electronic Payments in the Internet of Vehicles

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

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

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

Abstract: Blockchain technology has emerged as a promising solution for secure and decentralized electronic payments. The emergence of the Internet of Things (IoT) and the Internet of Vehicles (IoV) has opened up new possibilities for the adoption of electronic payment systems based on blockchain technology. This book chapter examines the possibilities of blockchain technology for online transactions. We talk about the difficulties and restrictions faced by blockchain-based payment systems in the IoV, such as scalability, interoperability, and legal compliance. We also discuss likely solutions to address these challenges, such as new consensus mechanisms and off-chain transactions. Additionally, we explore emerging technologies and their potential impact on electronic payments in the IoV, including AI and IoT. Finally, we discuss opportunities for future research and advancement in the sphere of electronic payments in the IoV, and how we can enable a more seamless, secure, and innovative payment ecosystem in the IoV.

Keywords: IoT, IoV, Blockchain, Electronic payments.

INTRODUCTION

Our daily lives have become increasingly dependent on electronic payments, which allow for quick and easy transactions in a variety of industries like banking, e-commerce, and transportation. With the rise of the Internet of Things (IoT) and the Internet of Vehicles (IoV), electronic payments have become even more crucial since they enable secure and speedy transactions in the networked world, which is rapidly increasing [1]. The IoV, which includes linked and autonomous vehicles, is a good illustration of a field that may profit substantially from the adoption of cutting-edge payment methods.

* **Corresponding author Arvind Panwar:** School of Computing Science and Engineering, Galgotias University, Greater Noida, India; E-mail: arvind.nice3@gmail.com

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

While traditional cash and card-based payment systems have been the norm for decades, they may not be sufficient to address the emerging needs of the IoV. Hence, there is a need to explore new payment solutions that can better cater to the unique challenges posed by the IoV. Blockchain technology (BCT) has arisen in recent years as a viable remedy to these issues, enabling safe and effective electronic payments in the IoV [2].

A distributed ledger technology called BCT, which serves as the basis for virtual currencies like Bitcoin and Ethereum, enables transactions to be carried out without the need for middlemen in a secure, transparent, and incorruptible manner. By using its unique characteristics, such as decentralization, transparency, and immutability, as well as by offering new payment channels outside of traditional cash- and card-based systems, BCT has the potential to alter payment systems in the IoV [3].

Introduction to the Topic and the Importance of Electronic Payments in the Internet of Vehicles

How we interact with the transportation sector is changing because of the Internet of Vehicles (IoV), a rapidly growing industry. An efficient and convenient commute is made possible by the Internet of Automobiles (IoV), a network of networked automobiles that communicate with one another and with the infrastructure. The development of advanced payment systems that can satisfy the specific needs of this business has been possible because of the growth of the IoV.

Electronic payments have become an essential component of our daily lives, enabling secure and efficient transactions in various domains. The importance of electronic payments in the IoV cannot be overstated. With the growing number of connected vehicles, the need for fast and secure payment systems is critical to enable seamless and efficient transactions in this domain. Traditional payment systems such as cash and card-based transactions may not be sufficient to meet the demands of the IoV, given the need for secure and fast transactions in a highly dynamic environment.

To address these problems, BCT has emerged as an effective solution for electronic payments in the IoV [4]. Blockchain is a distributed ledger system that makes transactions safe, transparent, and impenetrable without the use of middlemen [5]. By using its unique characteristics, such as decentralization, transparency, and immutability, as well as by offering new payment channels outside of traditional cash- and card-based systems, BCT has the potential to alter payment systems in the IoV [6].

Definition of BCT and its Characteristics

Blockchain is a distributed ledger technology that makes it possible to conduct safe, open, and tamper-proof transactions without the use of middlemen [7]. Transactions are secure and transparent since it is a decentralized system that allows different parties to view the same ledger simultaneously. The term "blockchain" describes how transactions are organized into blocks that are connected by chains in a blockchain network. The steps involved in Blockchain creation are shown in Fig (**1**) below.

One of the main characteristics of BCT is its decentralization. In contrast to traditional payment systems, which rely on a central authority like banks or governments, BCT allows a distributed network of users to maintain the ledger. This decentralized approach has several benefits, including enhanced security, lower transaction costs, and more transparency [8].

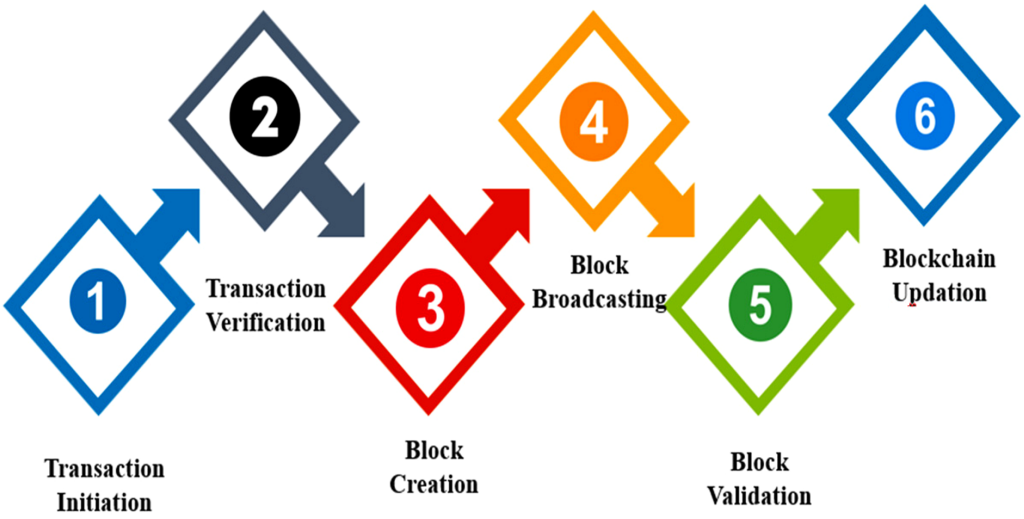


Fig. (1). A Steps of Blockchain Creation.

The transparency of BCT is another crucial aspect. A blockchain network keeps track of every transaction, and once a block is added to the chain, it cannot be changed or removed [9]. Due to this feature's high level of transparency, which enables all users to monitor network transactions, it is more difficult for fraud to go unreported.

The immutability of BCT is a crucial component. Once a block is included in the chain, it cannot be taken out. As a result, the network offers a high level of security because it is challenging for attackers to alter or delete transactions. The

CHAPTER 3

Federated Learning-Based Data Dissemination Systems for IoVs

Gaurav Singh Negi[1], Gopal Krishna[1,*] and **Jitendra Kumar Gupta[1,2]**

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

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

Abstract: Federated learning-based data dissemination solutions for Internet of Vehicles (IoVs) are gaining interest owing to their capacity to increase data dissemination performance and privacy. This chapter examines the current state of the art in federated learning-based data dissemination systems for IoVs, as well as the obstacles and possibilities associated with their deployment. A literature study, analysis of data dissemination needs in IoVs, and assessment of performance and privacy implications of alternative federated learning techniques are all part of the process for creating and assessing federated learning-based data dissemination systems in IoVs. The findings of a literature analysis and tests evaluating the performance and privacy of federated learning-based data dissemination systems in IoVs reveal that these systems have the potential to increase data dissemination performance and privacy, but various problems must be addressed. This chapter adds to the current literature by offering a thorough examination of the state-of-the-art federated learning-based data distribution systems for IoVs. The chapter discusses important obstacles and possibilities, as well as insights into the approach used to create and evaluate these systems. The chapter explores the consequences for IoVs of federated learning-based data dissemination systems, such as better data dissemination performance and privacy. The chapter focuses on possible applications in smart transportation, urban planning, and public safety. The chapter investigates the implications of federated learning-based data dissemination systems for IoVs, such as improved data dissemination performance and privacy. The chapter focuses on smart transportation, urban planning, and public safety applications.

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

[*] **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

IoVs, also known as the Internet of Vehicles, refers to a network of interconnected vehicles that leverage communication technologies to exchange information with each other and with the surrounding infrastructure [1, 2]. It encompasses the integration of vehicles, communication systems, sensors, and intelligent technologies to create an interconnected and intelligent transportation ecosystem. IoVs aim to enhance road safety, improve traffic efficiency, and enable innovative applications through seamless connectivity and intelligent communication among vehicles. By enabling vehicles to exchange real-time information, IoVs facilitate advanced capabilities such as cooperative collision warning, adaptive traffic signal control, autonomous driving, and efficient route planning [3 - 5]. Vehicle-to-Vehicle (V2V) Communication: IoVs heavily rely on Vehicle-to-Vehicle communication, where vehicles directly exchange information with nearby vehicles [6, 7]. V2V communication enables the sharing of important data, such as speed, position, acceleration, and safety-related messages, contributing to situational awareness and cooperative decision-making among vehicles. Vehicle-to-Infrastructure (V2I) Communication: In addition to V2V communication, IoVs leverage Vehicle-to-Infrastructure communication. This involves the exchange of information between vehicles and various roadside infrastructure components, including traffic lights, road sensors, and smart traffic management systems [8]. V2I communication enables vehicles to obtain real-time traffic information, receive traffic signal optimization, and access services related to parking, charging, and road condition monitoring. Intelligent Transportation Systems (ITS): IoVs are a key component of Intelligent Transportation Systems. ITS integrates information and communication technologies into transportation infrastructure and vehicles to enhance safety, efficiency, and sustainability [9, 10]. IoVs, in conjunction with ITS, enable the development of smart transportation systems, urban planning, and public safety applications. Background on IoVs the Internet of Vehicles (IoVs) refers to a network of interconnected vehicles that communicate with each other and the surrounding infrastructure. IoVs play a vital role in improving road safety, and traffic efficiency, and enabling advanced applications like autonomous driving and intelligent traffic management. One key characteristic of IoVs is their high vehicle mobility, where vehicles are constantly moving and changing their network connections [11]. This dynamic environment requires real-time and reliable communication among vehicles to ensure efficient data dissemination. IoVs generate a vast amount of data, including sensor data from cameras, radars, and GPS systems, as well as data exchanged through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. This data provides valuable insights for various applications in smart transportation and traffic management. However, data dissemination in IoVs faces challenges due to limited bandwidth, high data volumes, varying network conditions, and the

need for efficient and reliable data sharing among vehicles [12]. These challenges require innovative solutions to enable effective data dissemination and utilization in IoVs. Understanding the background of IoVs is crucial for comprehending the unique characteristics and complexities involved in disseminating data within this context. This background information serves as a foundation for the subsequent discussions on federated learning-based data dissemination systems in IoVs. Background on federated learning. The introduction section of the chapter provides an overview and background information on federated learning and its relevance to data dissemination in the context of the Internet of Vehicles (IoVs). Federated learning is a decentralized machine learning approach where models are trained locally on individual devices and the updates are aggregated to create a global model without the need for data sharing [13, 14]. In IoVs, efficient and timely data dissemination among vehicles is crucial for applications like traffic management, collision avoidance, and cooperative perception. Traditional centralized approaches for data dissemination face challenges such as extensive data sharing, privacy concerns, and reliance on a central server. Federated learning offers a promising solution by enabling collaborative learning while preserving data privacy, decentralizing the training process, and leveraging the collective knowledge of the network [15]. The objectives of the chapter include reviewing the state of the art in federated learning-based data dissemination systems for IoVs, analyzing performance and privacy implications, and exploring potential applications in smart transportation, urban planning, and public safety [16]. The overview of federated learning-based data dissemination systems for IoVs is shown in Table **1**.

Table 1. Overview of federated learning-based data dissemination systems for IoVs.

Aspect	Description
Definition	A machine learning strategy called federated learning enables training models on distributed data sources while protecting data privacy.
Motivation	Reduce data transfer, use local knowledge, and enable collaborative learning across devices or institutions while addressing privacy issues.
Distribution of Data	Data is dispersed among several servers or devices, frequently between users or organizations.
Training Method	• Local devices are equipped with the first model. • Local devices use their data to train the model. • Only gradients representing model changes are communicated to a central server. • Combining model updates to produce an overall model. • Returned to the local devices is the updated global model.
Protection of Privacy	• Local data is kept on the device, minimizing privacy threats from data transmission. • To further secure sensitive information, aggregated updates frequently include privacy-preserving strategies like differential privacy.

CHAPTER 4

Breaking the Centralization Barrier: Exploring Decentralized Federated Learning for Vehicle Number Plate Recognition in IoV

Arvind Panwar[1], Priyanka Gaba[2], Urvashi Sugandh[1,*] and **Navdeep Bohra[3]**

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

[2] *School of Computing Science & Engineering, Bennett University, Greater Noida, India*

[3] *Department of CSE, Maharaja Surajmal Institute of Technology, Delhi, India*

Abstract: The development of effective and safe machine learning systems for vehicle number plate recognition (VNPR) is now necessary due to the emergence of the Internet of Vehicles (IoV). However, traditional centralised techniques run into issues with data privacy, communication overhead, and centralised data access restrictions. This study explores the possibilities of decentralized federated learning for VNPR in the IoV to solve these constraints. Decentralised federated learning, which overcomes the centralization barrier, allows local model training on the edge devices of participating cars, protecting data privacy and cutting down on communication overhead. The ramifications of this paradigm change are examined in this research, including improved data privacy and security, shared intelligence, and resilience against errors and assaults. It also looks at the trade-off between performance and decentralisation while emphasising the balance attained *via* improved model aggregation and resource use. Additionally covered is the difficulty of consensus algorithms and blockchain-based networks, highlighting the need for further investigation and development. Decentralised federated learning has been identified as a possible strategy for overcoming the centralization barrier in VNPR systems, opening the door to the implementation of efficient, secure, and private machine learning in the IoV.

Keywords: Blockchain technology, Decentralization, Internet of Vehicles (IoV), Vehicle number plate recognition (VNPR).

INTRODUCTION

The concept of the IoV has emerged as an innovative implementation of the Internet of Things (IoT) framework, stemming from the rapid proliferation of IoT

* **Corresponding author Urvashi Sugandh:** School of Computing Science & Engineering, Galgotias University, Greater Noida, India; E-mail: usugandh5@gmail.com

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

technologies. Within the ecosystem of the IoV, automobiles establish connections with both the infrastructure and other vehicles through diverse wireless communication techniques [1, 2]. This connection enables a wide range of applications, such as traffic control, driver assistance, and vehicle monitoring. One of the primary challenges in the IoV ecosystem pertains to the efficient management and analysis of the substantial quantities of data generated by automobiles.

Within the context of the IoV, the process of identifying and acknowledging vehicle number plates is commonly referred to as VNPR. VNPR, also known as Vehicle Number Plate Recognition, plays a critical role in various domains such as toll collection, parking management, and law enforcement. In traditional VNPR systems, the data collected by cameras positioned at different locations is transmitted to a central server for processing. These systems rely on centralised architectures. The centralised design, nevertheless, presents several disadvantages, such as reduced connection speeds, vulnerability to single points of failure, and potential concerns regarding privacy [3, 4].

In recent years, there has been a growing interest in decentralised federated learning (DFL) as a viable alternative to the conventional centralised architecture. The utilisation of DFL, a machine learning technique, enables multiple entities to collaboratively train a model without the need to share data. The utilisation of DFL has the potential to establish a decentralised VNPR system within the IoV environment. This approach enables vehicles to collectively train a VNPR model while ensuring the privacy and confidentiality of their respective data [5, 6].

This book chapter explores the concept of DFL for VNPR within the context of the IoV. The chapter commences with a presentation of the IoV ecosystem and an examination of the challenges associated with establishing a centralised VNPR system. The chapter proceeds to introduce the concept of DFL and its advantages in comparison to centralised architecture. The subsequent subjects discussed in this chapter pertain to the development and execution of a DLF-based VNPR system within the context of the IoV environment. The chapter concludes by examining potential applications of DFL in the IoV context, along with identifying future research directions [7, 8].

The primary objectives of this book chapter are to comprehensively understand the concept of DFL for VNPR in the IoV environment and to explore its potential in overcoming the limitations associated with the centralised design.

Overview of Federated Learning and its Potential in IoV

A viable alternative to centralised machine learning systems has emerged: decentralised federated learning. The issues of vehicle number plate recognition may be overcome in the context of the IoV by using federated learning.

Overview of Federated Learning

A machine learning paradigm called federated learning allows different devices to work together remotely to create a global machine learning model without sharing their raw data with a centralised server. Each device does the training locally, while a central server collects all of the model changes. The modified model is subsequently sent to all devices *via* the central server to continue training. Federated Learning's main benefit is that it protects data privacy while enabling several devices to work together to create a powerful machine-learning model [9].

The Potential of Federated Learning in IoV

Federated Learning may be utilised to create a VNPR system inside the IoV that protects data privacy and minimises the computational burden of centralised systems. Without disclosing their private information to a central server, many cars may work together and develop a reliable number plate recognition model because of the distributed nature of federated learning. Federated Learning may also enhance the number plate recognition model's accuracy by combining the various data produced by various cars [10, 11].

The problems with centralised machine learning systems in the IoV are addressed by federated learning, which is a workable alternative [12]. Federated Learning's decentralised structure makes it possible for several cars to work together and develop a powerful number plate recognition model while safeguarding data privacy. Federated Learning is anticipated to acquire pace and become a crucial technology in the creation of intelligent transportation systems as a result of the growing usage of IoV.

Limitations of Traditional Federated Learning Methods

In order to get beyond the constraints of centralised machine learning systems, federated learning has shown considerable potential. Traditional Federated Learning techniques do, however, have several drawbacks. These constraints may reduce the system's effectiveness and accuracy in the context of VNPR in the IoV. Fig. (**1**) shows the limitations of traditional federated learning methods.

CHAPTER 5

Federated Learning-Based Vehicle Number Plate Recogntion in IoVs

Disha Mohini Pathak[1,*], Somya Srivastava[1] and **Shelly Gupta[2]**

[1] *Department of Computer Science, ABES Engineering College Ghaziabad, U.P., India*

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

Abstract: Artificial intelligence is widely used in a variety of industries. AI technology drives much of what we do. In a similar vein, as AI-based technologies advance, smart automobiles and the Smart Transport system will likewise experience revolutionary transformation. Different techniques are applied to create a system that is used to manage traffic and increase security inside the transportation network, different techniques are used. The automatic number recognition system (ANPR) described in this research can extract an image of a vehicle license plate by employing image processing methods. To make things easier, the proposed system may be operated without the installation of any extra GPS-like devices. The suggested system consists of image processing techniques, such as filters to eliminate blur and noise when distantly acquired photographs of moving vehicles are taken. To obtain the region of interest, its edges are detected, and an image is cropped. The procedure for better outcomes includes normalization, localization, image enhancement, restoration, and character retention approaches. Its effectiveness may be negatively impacted by the state of the license plate, unconventional formats, complex vision, camera quality, camera position, tolerance for distortion, motion blur, contrast-related issues, reflections, limitations in a processing unit, environmental factors, indoor/outdoor or time-independent shots, software tools, or other hardware-based restrictions.

Even with the greatest algorithms, a successful ANPR system implementation might need extra computer hardware to boost the proposed System's accuracy.

Keywords: ANPR, Computer vision, Edge detection, Gaussian blur, OCR, Segmentation.

INTRODUCTION

This is the era of smart societies; an intelligent infrastructure that incorporates cutting-edge technologies and data-driven solutions to improve the effectiveness,

* **Corresponding author Disha Mohini Pathak:** Department of Computer Science, ABES Engineering College Ghaziabad, U.P., India; E-mail: disha.itengineer@gmail.com

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

safety, and sustainability of each field. Transportation plays an important role in upgrading our society. To maximize the flow of people and commodities, technology plays a very important role in automating the complete system. It uses several different elements, including sensors, communication networks, and data analytics that lead towards a Smart Transportation System [1].

An automatic number recognition system, also known as an automatic license plate recognition (ALPR) system or an automatic number plate recognition (ANPR) system, is a technology that employs optical character recognition (OCR) to automatically read and detect the characters on vehicle license plates [2, 3]. It is frequently employed in applications such as toll collecting, traffic control, parking enforcement, and law enforcement [1]. Compared to human-operated systems, the system's automated nature lowers the need for manual intervention and increases the speed and accuracy of license plate readings. Automobiles involved in crimes, those that have expired or invalid registrations, and stolen automobiles can all be found using ANPR technology. Law enforcement authorities can use it to easily recognize and track questionable or wanted vehicles. Traffic flow monitoring, traffic infraction detection, such as speeding or running red signals, and parking rule enforcement can all be aided by ANPR devices. Toll booths and gated areas can use ANPR technology to automate toll collection and regulate access to restricted areas.

The major steps used in this process are shown in Fig. (**1**),

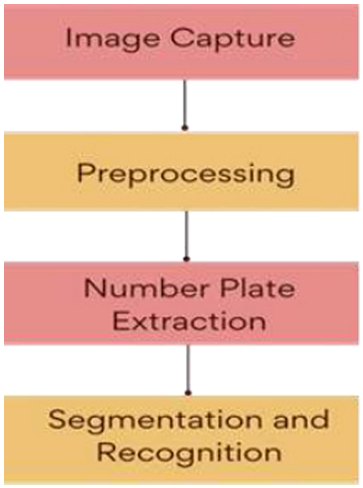


Fig. (1). Basic Steps in an ANPR.

Image capture: The system takes pictures of cars and their license plates using specialized cameras or sensors [4]. These cameras can be installed on moving

objects like police cars or toll booths as well as immovable objects like poles or gantries.

Image preprocessing: To increase the visibility and clarity of the license plate area, the collected photos are enhanced and altered throughout the preprocessing phases [5, 6]. This aids in getting better outcomes while recognizing characters.

Number Plate Extraction: The system identifies the region of interest within the image that contains the license plate using image processing methods [6]. The license plate area can now be separated from the rest of the vehicle.

Character Segmentation and Recognition: After locating the license plate region, the algorithm divides the characters on the plate into groups [7]. Due to differences in license plate style, font, and size, this requires isolating each character or digit from the license plate image, which can be a difficult operation.

An optical character recognition algorithm then processes the segmented characters, analyzing and deciphering the individual characters. To identify the captured characters, the OCR system compares them to a database of recognized characters.

The identified characters are translated into text format and then further processed to draw out pertinent data. Depending on the needs of the system, this could also include the license plate number, the state or nation code, and other information.

Normally, the information from the retrieved license plate is saved in a database for further study, retrieval, or comparison with other records. This makes it possible for law enforcement authorities to locate and swiftly identify potential suspects' automobiles.

Depending on the type of camera used, its setup, lighting fixtures, mounting area, area coverage, complicated scenes, shutter speed, and other environmental impediments, the image shot at the scene could have some trouble. Pre-processing involves applying several filters and functions to the image to improve the system's accuracy and the ability to extract the number plate from it. The two most prevalent applications are in traffic control systems and parking lots. In addition, it can be applied to the identification of stolen vehicles and vehicle entry-exit monitoring systems.

ANPR is a hot research topic these days. Several research works have already been performed in this area [8 - 12]. Different image pre-processing techniques have been applied to make the quality input image that in turn gives efficient output.

CHAPTER 6

Smart Transportation Systems for Vehicle Geographical Tracking

Jitendra Kumar Gupta[1,2], Gaurav Singh Negi[1], Gopal Krishna[1,*] and **Ramnarayan[1]**

[1] *Uttaranchal Institute of Technology, Uttranchal University, Dehradun, India*

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

Abstract: Smart transportation networks are essential components of modern cities, and vehicle spatial monitoring plays a significant role in improving their efficiency and safety. This book chapter covers the purpose, approach, findings, contribution, repercussions, restrictions, and usefulness of smart transportation systems for vehicle geographical tracking. The goal of the chapter is to assess current research on smart transportation systems and vehicle location monitoring, as well as to examine real-world examples and case studies. The results suggest that smart transportation systems with vehicle location tracking may greatly boost transportation system efficiency, reduce traffic congestion, and improve safety by monitoring vehicle movements in real-time and identifying possible problems. Moreover, intelligent transportation systems may give essential data to city planners and lawmakers in order to improve transportation infrastructure and develop more sustainable and equitable transportation networks. While these systems have significant potential benefits for cities, such as reducing traffic congestion, increasing transportation efficiency, and increasing safety, there are some drawbacks to consider, such as privacy concerns about the collection and use of personal data, as well as the possibility of technological failures and cybersecurity risks. The importance of this chapter originates from its thorough examination of smart transportation systems for vehicle location tracking, study of real-world examples and case studies, and focus on the possible advantages and limits of these systems for modern cities. It is a fantastic resource for legislators, city planners, transportation engineers, and academics who want to learn more about the potential of smart transportation systems to improve the efficiency and safety of modern metropolitan transportation systems.

Keywords: IoVs, Intelligent transportation systems, Smart transportation networks, Vehicle location tracking.

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

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

INTRODUCTION

Smart transportation refers to the integration of advanced technologies and data-driven systems to improve the efficiency, safety, and sustainability of transportation networks [1]. It involves the use of intelligent infrastructure, real-time data collection and analysis, and communication technologies to optimize various aspects of transportation, including vehicle operations, traffic management, and traveler information. Smart transportation systems leverage emerging technologies such as the Internet of Things (IoT), artificial intelligence (AI), big data analytics, and connectivity to enhance mobility, reduce congestion, minimize environmental impact, and enhance the overall transportation experience.

Geographical Tracking in Smart Transportation: Geographical tracking in the context of smart transportation involves monitoring and recording the real-time or historical locations of vehicles within a transportation network [2]. It utilizes technologies such as Global Positioning System (GPS), satellite navigation systems, and wireless communication to track the geographical coordinates of vehicles accurately. Geographical tracking systems enable the continuous monitoring of vehicle movements, allowing transportation authorities, fleet operators, and other stakeholders to have a comprehensive understanding of the transportation network's dynamics. The primary purpose of geographical tracking in smart transportation is to gather data on vehicle locations, routes, and speeds [3]. This data can be used to improve the efficiency of transportation systems in several ways which can be shown in Fig. (**1**).

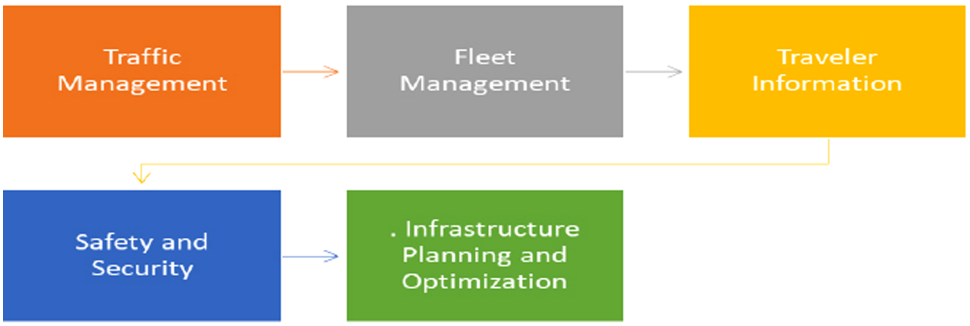


Fig. (1). Geographical tracking in smart transportation.

Traffic Management: Geographical tracking enables real-time monitoring of vehicle flow and congestion patterns, allowing transportation authorities to make informed decisions in managing traffic. By analyzing the collected data, traffic signals can be dynamically adjusted, and traffic flow can be optimized to alleviate congestion and reduce travel times.

Fleet Management: Geographical tracking is crucial for fleet operators to monitor their vehicles' locations and statuses. It enables efficient dispatching, route planning, and resource allocation, leading to improved operational efficiency, reduced fuel consumption, and better customer service.

Traveler Information: Geographical tracking data can be utilized to provide accurate and up-to-date information to travelers. Real-time information about traffic conditions, estimated arrival times, and alternative routes can be delivered through various channels such as mobile applications, dynamic road signs, and online platforms, enabling travelers to make informed decisions and plan their journeys more efficiently.

Safety and Security: Geographical tracking plays a vital role in enhancing the safety and security of transportation systems. It allows for the detection of abnormal vehicle behaviors, such as deviations from predefined routes or excessive speeds, enabling timely intervention in case of emergencies or potential security threats. Geographical tracking data can also be used for accident reconstruction and investigation purposes.

Infrastructure Planning and Optimization: The data collected from geographical tracking systems provides valuable insights for infrastructure planning and optimization. It helps transportation authorities identify areas with high traffic volumes or recurring congestion, guiding the development of new roads, public transit routes, or intelligent transportation systems. By analyzing historical tracking data, transportation planners can make data-driven decisions to improve the overall efficiency and sustainability of the transportation network.

While geographical tracking in smart transportation offers numerous benefits, it also raises concerns regarding privacy, data security, and ethical use of personal information. These issues need to be carefully addressed through appropriate policies, regulations, and technological safeguards to ensure the responsible and transparent implementation of smart transportation systems [4].

This study explores the potential of geographical tracking in improving smart transportation systems by improving efficiency, safety, and sustainability. It covers applications like real-time traffic management and environmental monitoring and addresses challenges like privacy, regulatory compliance, and infrastructure requirements. The content also explores applications in emergency response, urban planning, and personalized mobility services. It advocates for a balanced approach that preserves privacy while promoting innovation and proposes federated learning for decentralized data management in IoVs.

CHAPTER 7

Identity-Based Message Authentication Systems in IoVs

Gopal Krishna[1,*], Jitendra Kumar Gupta[1,2], Gaurav Singh Negi[1] and Ramnarayan[1]

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

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

Abstract: IBMAS (Identity-based message authentication systems) is a viable option for safeguarding data transfers in Internet of Vehicles (IoV) settings. We cover the state-of-the-art in IBMAS for IoVs in this book chapter, including their goal, techniques, results, contributions, implications, limits, and relevance. The goal of this chapter is to give academics and practitioners an overview of IBMAS for IoVs, including their design and implementation, to assist them in understanding the potential benefits and limits of these systems. We provide a study of existing IBMAS for IoVs in the literature, assessing their features, performance, and security aspects. We also propose a technique for assessing the efficacy of IBMAS for IoVs, concentrating on essential parameters such as message authentication performance, scalability, and attack resistance. The results of our test show that IBMAS can offer excellent message authentication with little overhead in IoV situations. Our addition to the literature is a thorough examination of IBMAS for IoVs, including their benefits and drawbacks, as well as a practical approach for assessing their performance and security qualities. We also talk about the consequences of IBMAS for IoVs, such as how they could affect data security and privacy in smart transportation systems. However, IBMAS has significant disadvantages, such as its reliance on a trusted third party and the risk of key exposure. Notwithstanding these limitations, IBMAS is important for IoVs because of its capacity to offer efficient and secure message authentication, which is crucial for the safe and dependable functioning of IoV systems. Finally, this chapter is an excellent resource for academics and practitioners interested in IBMAS for IoVs, covering their design, implementation, and assessment, as well as their implications for data security and privacy in intelligent transportation systems.

Keywords: Authentication, IBMAS, IoVs, IoVs, V2X.

[*] **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

Authentication systems are now more powerful than ever due to the sharp growth in cyber security threats. Even if there are more creative ways to authenticate users, password-based authentication remains one of the most often used techniques. Different authentication techniques have been increasingly implemented throughout time in the form of biological and graphical passwords. The latest innovations in authentication systems combine two or more techniques. The combination is used by these systems to distinguish between actual users and pretend users. Systems for authenticating users come into one of three categories: what you know, what you have, and what you are. By authenticating keys, messages, and entities, authentication guarantees secure communication inside a network. Identity authentication, sometimes referred to as the process of validating the authenticity of each user in communication, is a useful technique to stop Eve from claiming to be a genuine user in a conversation. To guarantee that only the authenticated user may receive sent messages, a communication protocol must be developed [1 - 5]. Vehicle-to-everything (V2X) technology is used by vehicle ad hoc networks (VANETs) for autonomous networking and communication between cars, which is a crucial building block for the implementation of an intelligent transportation system (ITS).

Dedicated short-range communications (DSRC) was the first standard used in the development of VANETs. Vehicular Ad hoc Network (VANET), a development of mobile ad hoc network (MANET), has been more important in wireless communication systems over the past few decades. The importance and relevance of Identity-Based Message Authentication (IBMA) systems in Internet of Vehicles (IoVs) can be attributed to several key factors [6 - 8].

Security: IoVs rely on secure and trusted communication between vehicles, infrastructure components, and other stakeholders. IBMA systems play a crucial role in ensuring the authenticity and integrity of messages exchanged within the IoV ecosystem. By verifying the identity of senders and detecting message tampering, IBMA enhances the overall security posture of IoVs, protecting against unauthorized access, data breaches, and malicious activities [8 - 10, 57].

Simplified Key Management: Traditional public key infrastructure (PKI) used in many authentication systems can be complex and resource-intensive to manage, especially in large-scale IoVs. IBMA simplifies the key management process by leveraging users' public identities instead of certificates, reducing the overhead associated with key distribution, revocation, and certificate management. This simplification makes IBMA systems more scalable and efficient, enabling their practical implementation in IoVs.

Efficiency and Performance: IBMA systems offer efficient and lightweight authentication mechanisms for IoVs. By eliminating the need for extensive cryptographic operations and certificate exchanges, IBMA reduces computational overhead, communication latency, and processing power requirements. This efficiency contributes to faster authentication processes, improved communication performance, and better resource utilization in IoVs.

User-Friendly Approach: The use of public identities (*e.g.*, email addresses, usernames) in IBMA systems offers a more user-friendly approach to authentication in IoVs. It eliminates the need for users to manage and exchange complex public keys or certificates, making it easier for individuals to adopt and participate in the IoV ecosystem [11 - 13]. This user-friendliness can contribute to a smoother user experience, widespread acceptance, and broader adoption of IoV technologies. Compatibility and Interoperability: IBMA systems can be designed to be compatible with existing communication protocols and infrastructure in IoVs. By leveraging standard communication protocols such as Dedicated Short-Range Communications (DSRC) or Cellular Vehicle-to-Everything (C-V2X), IBMA can be integrated seamlessly into the existing IoV infrastructure, ensuring interoperability with other systems and devices.

Identity-Based Message Authentication (IBMA) is a method used in the Internet of Vehicles (IoVs) to improve communication security by utilizing identity-based cryptography. It simplifies key management and offers efficient authentication mechanisms for dynamic and scalable environments. Future research aims to enhance security, privacy, scalability, and interoperability to support widespread adoption and integration in IoVs, fostering a safer and more reliable transportation ecosystem.

Future-Proofing: As IoVs continue to evolve and incorporate emerging technologies such as autonomous vehicles, connected infrastructure, and smart city initiatives, the need for robust and scalable authentication mechanisms becomes increasingly essential. IBMA systems provide a flexible and adaptable approach to authentication that can accommodate the evolving requirements and complexities of future IoV environments. IBMA systems play a vital role in enhancing the security, efficiency, and user-friendliness of authentication in IoVs. By providing simplified key management, efficient authentication mechanisms, and compatibility with existing infrastructure, IBMA contributes to the secure and reliable operation of IoVs, fostering trust, privacy, and the widespread adoption of connected vehicle technologies [14, 15, 59]. To elaborate the above the general structure of chapter flow is shown in Fig. (**1**).

SUBJECT INDEX

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

V

W