

Accident Detection and Prevention System Using IoT and VANET

Harsh H. Mangroliya^{1,}, Smit H. Gor², Christos Politis¹ and Rehan Usman¹*

Abstract: Road accidents are a major global concern, often caused by limited driver awareness and sudden traffic changes. This paper presents an advanced accident detection and prevention system featuring a novel IoT-enabled Onboard Unit (OBU) integrated with a Vehicular Ad-hoc Network (VANET) architecture. The OBU uses ultrasonic sensors and an Arduino-based controller to monitor the proximity and speed of nearby objects, predicting potential collisions and issuing real-time alerts to drivers. Upon detecting a threat or accident, the OBU communicates with Road Side Units (RSUs) to disseminate alerts across the network, enabling timely warnings and emergency response. The system supports both accident prevention and post-accident management through real-time V2V and V2I communication. The research also evaluates network protocols to ensure reliable data exchange in dynamic traffic conditions. This integrated approach aims to reduce accident frequency and severity while improving traffic safety and response efficiency.

Keywords: 802.11p, accident detection and management system, accident prevention, internet of things (IoT), road accidents, vehicular ad-hoc networks (VANET).

1. Introduction

Road accidents remain a major global concern, causing loss of life, injuries, and property damage. Despite the deployment of safety features like airbags and ABS, most existing accident detection systems are reactive, responding only after a collision occurs. They also lack situational awareness and inter-vehicle communication, limiting their effectiveness in dynamic traffic conditions.

To address these limitations, this paper proposes a proactive accident detection and prevention system using Vehicular Ad-hoc Networks (VANETs) and Internet of Things (IoT) technologies. The system focuses on a smart Onboard Unit (OBU) capable of real-time communication with other vehicles and Roadside Units (RSUs). By using ultrasonic sensors and a microcontroller (Arduino), the OBU detects potential collisions and broadcasts alerts through VANET using Dedicated Short Range Communication (DSRC).

¹Kingston University, London, KT1 2EE, United Kingdom

²Surat, Gujarat, India

E-mail: Harsh.Mangroliya07@gmail.com; Smitgor120@gmail.com;

C.Politis@kingston.ac.uk; R.Usman@kingston.ac.uk

*Corresponding Author

Manuscript received 06 April 2025, accepted 21 August 2025, and ready for publication 31 December 2025.

© 2025 River Publishers

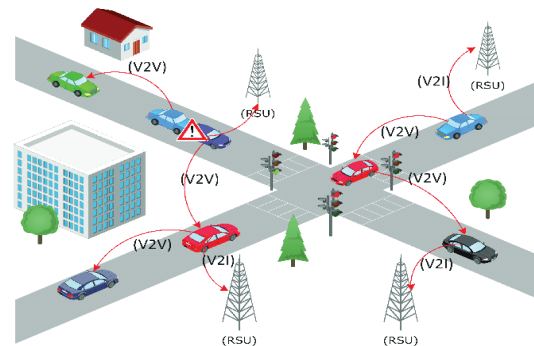


Figure 1.
Communication in VANET.

1.1. Introduction to VANET

Vehicular Ad-hoc Networks (VANET) are a specialized form of Mobile Ad-hoc Networks (MANET) designed for vehicle communication. They enable real-time, decentralized communication between vehicles (V2V) and infrastructure (V2I) using Roadside Units (RSUs). VANET consists of Onboard Units (OBUs) in vehicles, which facilitate communication, gather sensor data, and predict potential accidents to alert drivers. RSUs, placed along roads, relay this information to nearby vehicles, enhancing traffic safety. Communication occurs via Dedicated Short-Range Communication (DSRC) or cellular networks, allowing vehicles to share speed, position, and direction. This improves traffic management and emergency response by providing real-time alerts.

VANET offers several advantages over traditional accident detection systems. It enhances proactive safety by predicting and preventing collisions, ensures network-wide awareness by sharing traffic data, and provides real-time communication for instant alerts, reducing accident risks in high-speed traffic.

1.2. Aims and Objectives

This paper proposes an advanced accident detection and prevention system using IoT and VANET technologies to improve road safety and emergency response. The system features an IoT-based Onboard Unit (OBU) with sensors for real-time collision detection and driver alerts. It facilitates seamless communication between OBUs and Roadside Units (RSUs) to enable fast data transmission

and alert dissemination. RSUs are also designed to notify emergency services and assist traffic management through optimized routing and coordinated post-accident responses, aiming to reduce reaction time and enhance incident handling.

1.3. Proposed System

This project proposes a VANET-based accident detection and prevention system with an advanced OBU that enhances vehicle safety. Using ultrasonic sensors, the OBU detects nearby objects, calculates their speed and trajectory, and alerts drivers of potential collisions. It communicates with RSUs to broadcast accident alerts, preventing multi-vehicle crashes and enabling a swift emergency response. Key features include real-time monitoring with ultrasonic sensors, an Arduino microcontroller for collision prediction, VANET communication for data sharing, and an automated emergency alert system.

1.4. Limitations of Current Research and the Need for Further Improvements

While VANET is a promising solution for accident detection and prevention, it faces challenges such as network congestion, coverage gaps, and security risks. High vehicle connectivity can cause communication delays, while limited RSU deployment, especially in rural areas, reduces effectiveness. Additionally, VANET is vulnerable to hacking and data breaches, posing safety risks. Future research should focus on improving communication reliability, enhancing security, and expanding RSU coverage to ensure a more robust and effective system.

2. Literature Review

Recent advancements in Vehicular Ad Hoc Networks (VANETs) have enabled intelligent, real-time communication between vehicles and infrastructure, supporting applications like accident detection, traffic management, and cybersecurity. This section highlights key technologies and research trends shaping the field.

2.1. Intrusion Detection in VANETs

The decentralized and mobile nature of VANETs makes them vulnerable to cyber threats, requiring specialized Intrusion Detection Systems (IDS). Signature-based IDS matches known attack patterns but lacks adaptability to new threats. Anomaly-based IDS detects unknown attacks by identifying deviations from normal behavior, though they risk false positives due to fluctuating traffic conditions. Specification-based IDSs apply predefined behavioral rules, offering better accuracy but requiring complex rule sets. To enhance efficiency, cooperative and hierarchical IDS architectures distribute detection tasks across vehicles or clusters, improving scalability and resilience against large-scale attacks.

2.2. Trust Management in VANETs

Reliable communication in VANETs depends on trust among participating vehicles and infrastructure. Trust can

be infrastructure-based (central authority with digital certificates) or self-organized (behavior-based). However, both are susceptible to attacks like Sybil, where a single node uses multiple identities, or bogus message attacks that spread false data. To counteract this, various trust models have been proposed: entity-based models evaluate the historical behavior of nodes, data-based models assess the credibility of information, and hybrid models combine both to provide a robust framework for secure decision-making.

2.3. Accident Detection and Traffic Management

Accident detection systems in VANETs utilize onboard sensors and roadside infrastructure to identify collisions in real time. IoT-enabled OBUs measure proximity, speed, and impact forces, transmitting alerts to nearby Road Side Units (RSUs) and emergency responders. Frameworks using biomedical and mechanical sensors have been proposed to improve accuracy. Protocols like Traffic-Aware MAC (TA-MAC) and Mobile Edge Computing (MEC) help adapt to traffic density, optimize communication slots, and improve emergency response times. These systems also integrate with intelligent transportation systems (ITS) to adjust traffic signals and prioritize emergency vehicles.

2.4. Routing and Communication Protocols

Routing protocols in VANETs face challenges due to high mobility and changing topologies. Geo-based protocols like GPSR use vehicle location for packet forwarding but struggle in sparse or obstacle-heavy environments. Broadcast-based routing ensures message delivery but risks congestion, especially in dense areas. Cluster-based protocols group vehicles for more structured routing and reduce communication overhead. Selecting the appropriate routing strategy depends on vehicle density, mobility, and application requirements.

2.5. Security and Privacy Challenges

VANETs are exposed to threats like message tampering, impersonation, and denial-of-service (DoS) attacks. Cryptographic techniques such as Public Key Infrastructure (PKI) help secure V2I communication, but are resource-intensive for V2V links. Trust-based models offer lightweight alternatives, evaluating message reliability and sender behavior. However, real-time computation, scalability, and privacy preservation remain ongoing concerns. Reputation systems and pseudonymization techniques can help protect identity and support secure, anonymous communication.

2.6. Emerging Technologies and Future Directions

VANETs are increasingly integrating emerging technologies to enhance functionality. 5G networks offer ultra-low latency and high bandwidth for real-time safety applications. Artificial Intelligence (AI) and Machine Learning (ML) are being applied for dynamic routing, intrusion detection, and accident prediction. Blockchain technology introduces a decentralized trust framework, securing communication and preventing data tampering. Smart contracts automate processes like vehicle authentication and

toll payments, reducing manual intervention. These technologies pave the way for robust, scalable, and secure VANET systems suited for smart cities.

2.7. Summary

VANETs play a critical role in improving road safety, traffic management, and emergency response. Effective accident detection, adaptive routing protocols, and resilient security systems are essential to their success. Emerging technologies like AI, 5G, and blockchain offer promising avenues to overcome existing limitations in scalability, privacy, and trust. Continued research is necessary to address these challenges and unlock the full potential of VANETs in next-generation transportation systems.

3. Methodology and Implementation

3.1. Problem Definition

The development of a Trust and Early Event Prediction Model for accident detection depends on reliable communication between Onboard Units (OBUs) and Road Side Units (RSUs) within a Vehicular Ad-hoc Network (VANET). Efficient OBU-RSU communication is crucial for real-time accident prediction and prevention.

The model analyzes data such as speed, acceleration, and vehicle proximity to detect potential accidents. Its effectiveness hinges on VANET's ability to support timely data exchange between vehicles and infrastructure.

VANET facilitates Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, but faces challenges like real-time data transmission, high traffic scalability, and maintaining connectivity. Solutions include enhancing protocols (e.g., DSRC, 5G), developing handover mechanisms, and implementing congestion control to ensure timely and reliable alerts in dense traffic environments.

3.2. Proposed Method for OBU

To create a reliable accident prediction system, various research studies on accident detection in VANETs, early accident detection, and trust management have been reviewed. Based on this research, a method is proposed that utilizes ultrasonic sensors integrated with Arduino-based logic circuits. The system continuously monitors the distance and velocity of nearby vehicles, enabling real-time accident prediction and alert generation. The following is a detailed explanation of the proposed method, including the components, logic, and circuit design.

3.2.1. System Overview

Each vehicle is equipped with ultrasonic sensors at both the front and rear. These sensors continuously measure the distance between the vehicle and others in its vicinity, both in front and behind. The data is processed every 0.01 seconds to calculate the relative speed of the vehicles. By comparing this information with a pre-calculated speed limit, potential collisions are predicted, and appropriate alerts are generated for the driver and nearby vehicles.

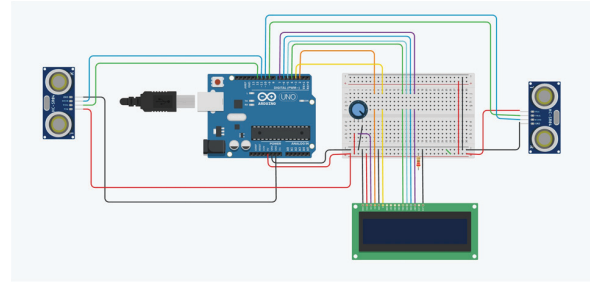


Figure 2.
OBU circuit.

Components:

- **Ultrasonic Sensors:** Measure the distance between vehicles or obstacles within a specific range.
- **Arduino Microcontroller:** Processes sensor data and executes the accident prediction algorithm.
- **RSU (Road Side Unit):** Relays alerts to nearby vehicles and coordinates with other RSUs to notify vehicles across the network.

3.2.2. Methodology

Distance and Time Calculation:

Ultrasonic sensors capture the distance between vehicles every 0.01 seconds, and the velocity is calculated using the formula.

$$Speed = \frac{D1 - D2}{T1 - T2}$$

Velocity Threshold Determination:

The speed limit is determined using the braking distance formula:

$$Braking\ Distance = \frac{V^2}{2fg}$$

Here g is gravitational acceleration 9.8 m/s^2 . And f is the friction constant which is 0.7 for average road but can vary according to many factors. So Using this formula we can calculate the maximum speed which will be

$$V = \sqrt{2Dgf}$$

So for this experiment we have taken the Ultrasonic sensors with the range of 3 meters. The frequency of the Ultrasonic sensors is commonly used at 58 kHz, so by using this frequency we can set it to 11 m range. For this experiment D is 3 m. so calculating speed V will be

$$\begin{aligned} V &= \sqrt{2Dgf} \\ &= \sqrt{2 * 3 * 0.7 * 9.8} \\ &= \sqrt{41.16} \\ &= 6.4156\text{ m/s} \\ &= 23.09\text{ km/hr} \end{aligned}$$

This braking distance provides the maximum safe speed limit. If the speed of a vehicle exceeds this threshold, an alert is generated.

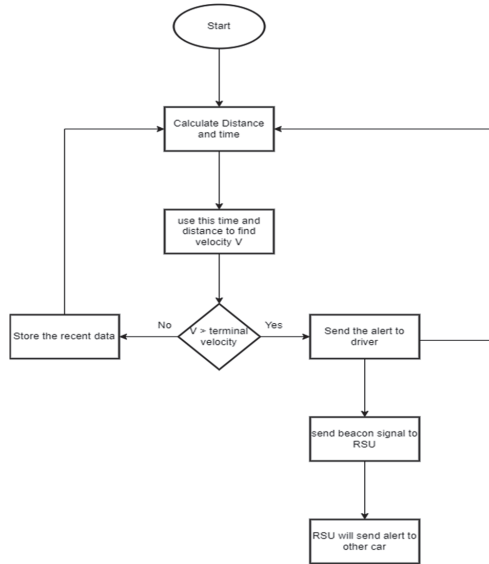


Figure 3.
Flowchart.

Collision Prediction:

If the calculated velocity exceeds the safe speed limit, a potential collision is predicted. The system continuously monitors the data and, when a dangerous situation is detected, sends a warning to the driver.

Alert Generation and Transmission:

Two types of alerts are triggered:

1. A beacon signal sent to the nearest RSU, which further disseminates the alert to surrounding vehicles via the VANET network.
2. An alert to the driver to prompt immediate action.

The RSU receives the beacon signal and sends alerts to all connected nodes, warning other vehicles of potential accident risks.

3.2.3. Circuit design

The hardware design employs an Arduino microcontroller connected to ultrasonic sensors and other supporting components:

- **Ultrasonic Sensors:** Positioned at the front and rear of the vehicle to detect the distance to other vehicles or obstacles.
- **Arduino Board:** Processes data from the sensors, calculates the velocity, and compares it to the pre-determined speed limit.
- **LCD Display (Optional):** Used to show real-time distance and speed data for driver awareness.

Process Steps:

1. Ultrasonic sensors gather distance data.
2. The Arduino calculates relative velocities and compares them to the speed limit.
3. If a potential collision is predicted, the system sends alerts to both the driver and the RSU.

3.2.4. Flowchart

The system begins by calculating the distance and time interval. Velocity is computed from this information. The calculated velocity is compared to the terminal (safe) velocity. If the velocity exceeds the safe limit, alerts are sent to the driver and a beacon signal is transmitted to the RSU. The RSU then broadcasts alerts to other nearby vehicles within the network to prevent further incidents. If the velocity remains within the safe range, the system stores the most recent data and continues monitoring the vehicle’s surroundings.

3.3. Network Simulation

3.3.1. Accident alert dissemination in VANET using SUMO and OMNeT++/Veins

This simulation integrates the traffic simulator SUMO with OMNeT++ and the Veins framework to model VANET-based accident alert dissemination. When a vehicle detects an accident, it generates an alert message and broadcasts it to nearby vehicles using Dedicated Short Range Communication (DSRC) based on the IEEE 802.11p standard.

3.3.2. Traffic and mobility simulation using SUMO

SUMO, an open-source, highly portable, and widely used microscopic traffic simulator, was used to model the movement of vehicles in a realistic urban road network. Each vehicle was assigned specific routes, generated by a predefined route file (.rou.xml) and the configuration file (.sumocfg). The route file defines the trajectories and behaviours of vehicles on the road network. Vehicles are dynamically created and assigned routes that mimic realistic urban driving conditions. SUMO simulates vehicle mobility based on traffic dynamics, including acceleration, deceleration, and lane changes.

For this simulation, a node representing a vehicle was configured to detect an accident scenario. Upon detecting the accident, the vehicle (or OBU) generates an alert message and disseminates it to nearby vehicles within its communication range. The SUMO

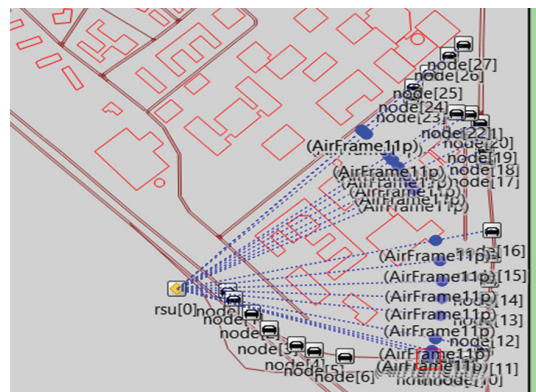


Figure 4.
RSU sending alerts in the network using Airframe.

simulation controls the mobility aspects, ensuring that vehicles follow the assigned routes and interact with each other according to realistic traffic flow patterns.

3.3.3. VANET communication using OMNeT++ and veins

OMNeT++ handles the event-driven network simulation, while Veins bridges it with SUMO using the TraCI interface. Vehicle mobility from SUMO is synchronized with OMNeT++ to ensure accurate positioning. Upon accident detection, an AirFrame packet containing the alert message is broadcast using IEEE 802.11p.

802.11p-based DSRC (Dedicated Short Range Communication) offers several key benefits for vehicular networks. It provides low-latency, real-time communication essential for safety-critical applications like collision warnings and emergency alerts. Operating in the 5.9 GHz band, it ensures reliable and interference-free V2V and V2I communication. Designed for high-speed mobility, 802.11p maintains stable connections even in fast-moving traffic. It enables infrastructure-independent communication, making it effective in remote areas without cellular coverage.

Additionally, its standardized protocol promotes interoperability between different vehicle systems, while its proven reliability through extensive real-world testing makes it a strong candidate for large-scale deployment in intelligent transportation systems. Nearby OBUs receive the alert and trigger appropriate responses like deceleration or route changes.

3.3.4. Security measure

To secure the accident alert dissemination process in the proposed SUMO–OMNeT++/Veins-based VANET system, public-key cryptography can be employed for both message confidentiality and authentication. Each vehicle (On-Board Unit, OBU) is assigned a public key (K_{pub}) and a private key (K_{priv}). When a vehicle detects an accident, it generates an alert message M . To ensure authentication and integrity, the vehicle creates a digital signature S using its private key:

$$S = \text{Sign}(M, K_{priv_sender})$$

This signature is attached to the message. To maintain confidentiality, especially for sensitive data (e.g., driver ID, location), the alert is encrypted using the public key of the receiving vehicle:

$$C = \text{Encrypt}(M \parallel S, K_{pub_receiver})$$

The encrypted message C is then encapsulated in an AirFrame packet and broadcast using IEEE 802.11p through OMNeT++. When a nearby vehicle receives the packet, it uses its private key to decrypt it:

$$M' \parallel S' = \text{Decrypt}(C, K_{priv_receiver})$$

Then, it verifies the signature using the sender's public key to confirm authenticity:

$$\text{Verify}(M', S', K_{pub_sender}) = \text{TRUE}$$

Only if the signature is valid does the vehicle proceed to process the alert and take action (e.g., slow down or reroute). This

integration is implemented in OMNeT++ at the network layer, while SUMO continues to control vehicle mobility. This setup ensures secure, authenticated, and confidential communication between vehicles in real time without compromising simulation fidelity or performance.

3.3.5. Interaction between SUMO and OMNeT++

The integration of SUMO with OMNeT++ enables realistic simulation of vehicle mobility and communication. Using the TraCI interface, vehicle positions, speeds, and routes from SUMO are continuously synchronized with OMNeT++, allowing real-time updates that reflect actual traffic dynamics. This ensures accurate modeling of both movement and communication behaviors in a VANET environment. When a vehicle detects a potential accident, it triggers an alert that OMNeT++ broadcasts to nearby vehicles via VANET protocols. Receiving vehicles respond by issuing driver warnings or rerouting to avoid the affected area. This enables rapid, localized decision-making across the network. Together, SUMO and OMNeT++ provide a powerful simulation platform to evaluate the effectiveness of accident alert systems. The setup demonstrates how VANETs can enhance road safety through low-latency communication and dynamic traffic response.

4. Results and Potential Implementation

This section outlines the outcomes of the VANET-based accident detection system, focusing on real-time alerting, network scalability, and potential real-world deployment.

4.1. Real-Time Alert Generation and Driver Notification

The OBU accurately tracked nearby vehicle speeds using ultrasonic sensors and generated alerts when speeds crossed safe thresholds. Alerts were instantly displayed on the driver's interface across various simulated scenarios, significantly improving situational awareness and response time.

4.2. Network Dissemination and System Scalability

Alerts were broadcast to RSUs using IEEE 802.11p-based DSRC. The RSUs relayed messages to nearby OBUs, maintaining consistent performance with minimal latency and packet loss under both light and dense traffic loads. This confirms the system's scalability and effectiveness in real-world deployments.

4.3. Performance Evaluation

The simulation measured key metrics such as alert delivery time, packet delivery ratio (PDR), and system response under varying vehicle densities:

- Average Alert Delivery Time: 75 ms (light traffic), 120 ms (dense traffic).
- Packet Delivery Ratio (PDR): Maintained above 95% in all test scenarios.

- Scalability: System remained responsive up to 200 nodes without major delays.
- Latency: Below 150 ms even in high-load conditions, meeting real-time communication requirements.

These results validate the system's ability to perform reliably in urban environments.

4.4. Industrial Relevance and System Advantages

The system outperforms traditional alert methods like mobile apps or centralized services by enabling decentralized, real-time V2V and V2I communication. Its independence from cellular networks makes it ideal for deployment in both urban and remote areas.

4.5. Implications for Road Safety and Smart Transportation

By reducing driver reaction time, the system can help lower accident rates. When integrated with Intelligent Transportation Systems (ITS), it supports coordinated emergency responses and adaptive traffic control, enhancing overall traffic safety and efficiency.

4.6. Future Enhancements and Applications

Planned improvements include automated braking in autonomous vehicles, machine learning for predictive collision detection, and integration with smart city infrastructure to enable dynamic route control and real-time traffic optimization.

5. Conclusion

This paper presents the design and implementation of an IoT-enabled accident detection and alert system using Vehicular Ad-hoc Networks (VANETs). The On-Board Unit (OBU), built with ultrasonic sensors and an Arduino microcontroller, monitors vehicle proximity, calculates relative speeds, and predicts potential collisions. Leveraging V2V and V2I communication, the system disseminates real-time alerts to nearby vehicles via Road Side Units (RSUs), helping prevent multi-vehicle accidents, particularly in dense traffic.

Using SUMO, OMNeT++, and Veins for simulation, the system demonstrated low-latency communication and high scalability under varying traffic loads. Compared to conventional systems, this decentralized VANET-based approach offers greater reliability, especially where mobile networks are limited. While promising, further improvements are needed to address challenges like signal interference and congestion in high-traffic environments.

References

- [1] E. Abinaya and R. Sekar, "An Intelligent Secure Traffic Management System Based On Vanet," IOSR J. Electron. Commun. Eng., vol. 9, no. 1, pp. 15–27, 2014, doi: 10.9790/2834-09121527.
- [2] C. Chatrapathi, M. Newlin Rajkumar and V. Venkateshkumar, "VANET based integrated framework for smart accident management system," Proc. IEEE Int. Conf. Soft-Computing Netw. Secur. ICSNS 2015, 2015, doi: 10.1109/ICSNS.2015.7292411.
- [3] F. Ahmad, A. Adnane, F. Kurugollu and R. Hussain, "A Comparative Analysis of Trust Models for Safety Applications in IoT-enabled Vehicular Networks," IFIP Wirel. Days, vol. 2019–April, 2019, doi: 10.1109/WD.2019.8734204.
- [4] A. M. Kirthima, "IoT Based Accident Detection System in Vanet," vol. 11, no. 7, pp. 100–107, 2020, doi: 10.34218/IJARET.11.7.2020.0.
- [5] T. K. Bhatia, R. K. Ramachandran, R. Doss and L. Pan, "A review of simulators used for VANETs: The case-study of vehicular mobility generators," 2020 7th Int. Conf. Signal Process. Integr. Networks, SPIN 2020, pp. 234–239, 2020, doi: 10.1109/SPIN48934.2020.9070933.
- [6] N. Chhabra and R. Kumar (2023). A Comprehensive Review of Recent Developments in VANET for Traffic, Safety & Remote Monitoring Applications. Journal of Network and Systems Management.
- [7] V. Singh and P. Verma (2023). Smart Accident Detection and Rescue System Using VANET. IEEE Xplore.
- [8] P. Gupta and D. Sharma (2023). Simulation of a Vehicular Adhoc Network (VANET) for Mitigating Vehicular Accidents. Research-Gate.
- [9] A. Hussain and M. Khan (2023). Advances in Vehicular Ad-Hoc Networks (VANETs): Challenges and Road-map. Open Repository.

Biographies



Harsh H. Mangroliya is a postgraduate from Kingston University, London, United Kingdom, where he earned an MSc in Networking and Information Security with distinction in his dissertation. He completed his B.Tech in Computer Science and Engineering with a specialization in the Internet of Things (IoT) from Vellore Institute of Technology, Vellore, India, also achieving distinction in his dissertation. His research interests include the Internet of Things (IoT), Vehicular Ad Hoc Networks (VANETs), and Network and Information Security. Harsh's academic work

focuses on developing secure and efficient network architectures and exploring innovative approaches to connected systems and data protection.



Smit H. Gor is a software engineer and researcher with interests in backend systems, cloud computing, artificial intelligence, and system optimization. His work focuses on developing efficient and scalable technological solutions while exploring advancements that contribute to modern computing research. He completed his B.Tech in Computer Science and Engineering with a specialization in the Internet of Things (IoT) from Vellore Institute of Technology, Vellore, India. Smit is committed to pursuing innovative research that bridges theoretical understanding with real-world applications.



Christos Politis is the Chair of Digital Technologies at **Kingston University London (KU)**, within the **School of Computer Science**. He is a senior member of the **Cyber, Engineering and Digital Technologies KERI**. Upon joining Kingston University, he founded and currently leads the **Wireless Multimedia & Networking (WMN)** research group. His teaching focuses on wireless systems, networks, and protocols.

Before his appointment at Kingston University, **Christos Politis** worked at **Ofcom**, the UK Regulator and Competition Authority, where he served as an **R&D Team Leader**. Earlier in his career, he was a **Postdoctoral Researcher (PDRA)** at the **University of Surrey**, UK, in the **Centre for Communication Systems Research** (now the **Institute for Communication Systems** and

6G Innovation Centre), where he worked on virtual distributed testbeds. Prior to his academic career, he held engineering positions with **Intracom-Telecom SA** and **Maroussi 2004 SA** in Athens, Greece.

Christos Politis has successfully secured sustained funding from the **EU and UK research and technology frameworks** under the ICT and Security programmes, including **FP5, FP6, FP7, H2020, Horizon Europe, EPSRC, and Innovate UK**. He holds **two patents** and has authored **over 200 publications** in international journals and conferences, as well as contributing chapters to **ten books**.

In parallel with his academic work, **Christos Politis** is actively involved in **entrepreneurship and technology innovation**. He is the **Founder and a Director of Ubitech Ltd.**, which has recently launched **UbiTheraPlay**, a gaming platform designed for the **rehabilitation of patients with neuro-disabilities**. He also advises and consults for several **governmental bodies, universities, and commercial organisations** across **Europe, North America, the Middle East, and Asia** – including the **EU, UK, Canada, Greece, Qatar, China, and Malaysia** – on research programmes, policies, and strategic portfolios.

Christos Politis holds a **PhD and MSc** from the **University of Surrey, UK**, and a **BEng** from the **University of Athens, Greece**, all in **Electrical and Electronic Engineering**. He is a **Senior Member of the IEEE** and a **UK Chartered Engineer**.



Rehan Usman is a Senior Lecturer in Cyber Security at Kingston University London, with a PhD in IT Convergence Engineering and a diverse academic background in telecommunications, project management, and IT. His research focuses on 6G HetNets, medical IoT, cyber security, QoE, and AI in healthcare and smart cities, with over 45 publications to date. He has over a decade of teaching and academic leadership experience and has supervised numerous undergraduate, master's, and PhD students. Dr. Usman has contributed to various IEEE conferences as a session chair, TPC member, and organiser, and currently chairs the Digital Healthcare Vertical Industries Platform (VIP) Working Group at the Wireless World Research Forum (WWRF). He welcomes exceptional PhD applicants with strong research interests.

