WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Integrating Trust Management with Blockchain and Fog Computing: A Survey on Securing and Optimizing Smart Traffic Systems

Dr. M. Rudra Kumar[1*], N. Karthik Narayan[2†] and A Deepika[3†]

[1*]Department of Information Technology, Organization, Gandipet, Hyderabad, 500075, Telangana, India.
[2]Department of Information Technology, Organization, Gandipet, Hyderabad, 500075, Telangana, India.
[3]Department of Information Technology, Organization, Gandipet, Hyderabad, 500075, Telangana, India.
E-mail(s): mrudrkumar it@mgit.ac.in; karthiknarayan0611@gmail.com; deepikareddy1203@gmail.com;
DOI : https://doi.org/10.55248/gengpi.6.0425.15189

ABSTRACT

The rapid growth of vehicular networks and the increasing integration of smart transportation systems have raised concerns regarding trust and security in vehicle-to-everything (V2X) communication. As these systems rely heavily on data exchange among vehicles, road-side units (RSUs), and centralized enti- ties, ensuring the authenticity and reliability of transmitted information becomes crucial for safety and efficiency. This paper surveys the current state of trust management systems in vehicular networks, with a particular focus on leverag- ing blockchain technology to enhance data integrity and security. We explore various trust evaluation models, the role of RSUs in maintaining trust, and the application of synthetic data through simulations for system testing. Addition- ally, the paper discusses the challenges in maintaining scalability, privacy, and robustness in trust management systems, along with future research directions. By examining existing solutions and frameworks, this survey aims to provide a comprehensive overview of the methods, tools, and techniques that contribute to the development of a reliable and secure trust management system in vehicular networks.

Keywords: Trust Management, RSUs, Blockchain Technology, Trust Evaluation Models, Trust Metrics.

1. Introduction

A smart city is an urban region that employs modern digital technology and data- driven systems to increase urban service efficiency, residents' quality of life, and sustainability. Cities are facing rising issues as urbanization grows, including over- crowding, pollution, limited resources, and outdated infrastructure. To address these concerns, smart cities use Information and Communication Technologies (ICT), the Internet of Things (IoT), and Artificial Intelligence (AI) to build an interconnected ecosystem in which systems such as transportation, electricity, healthcare, and public safety operate seamlessly. Smart cities use real-time data and automation to optimize resources, lower operating costs, and provide high-quality services to inhabitants [8]. The primary notion of a smart city is to make urban life more efficient, sus- tainable, and citizen-centric. Traditional cities frequently have poor infrastructure, wasteful energy utilization, traffic congestion, and insufficient public services. Smart cities address these inefficiencies by implementing technology-driven solutions that deliver actionable insights and automate procedures. For example, IoT-enabled sen- sors may detect water leaks in pipelines, decreasing waste and improving distribution. Similarly, smart grids enable cities to dynamically balance energy supply and demand, hence decreasing power interruptions and carbon footprint. Such innovations assist cities in transitioning to more sustainable urban living while improving governance, communication, and decision-making processes [22].

One of the distinguishing characteristics of smart cities is their capacity to incor- porate digital technology into the physical environment. For example, smart sensors and networks are embedded in urban infrastructure to monitor and manage utilities, traffic, and the environment. This interface enables city administrators to collect and analyze massive amounts of data, discover inefficiencies, and implement data-driven solutions in real time. Citizens may use digital platforms and mobile applications to actively participate in governance, quickly access services, and provide feedback, making cities more inclusive and responsive. Smart cities can accomplish economic growth, increase public involvement, and provide higher living standards by cultivat- ing a connectivity environment.

This image 1 represents the core components of a smart city, highlighting how technology enhances various urban domains to improve efficiency, sustainability, and quality of life. It includes Smart Transportation for optimized mobility, Smart Agriculture for sustainable farming practices, and Smart City Services for efficient management of utilities like water and waste. Smart Health integrates digital health- care systems, while Smart Homes focus on energy-efficient and secure living spaces. Smart Energy promotes renewable energy and optimized power distribution, and Smart Infrastructure ensures intelligent urban planning and connectivity. Lastly,

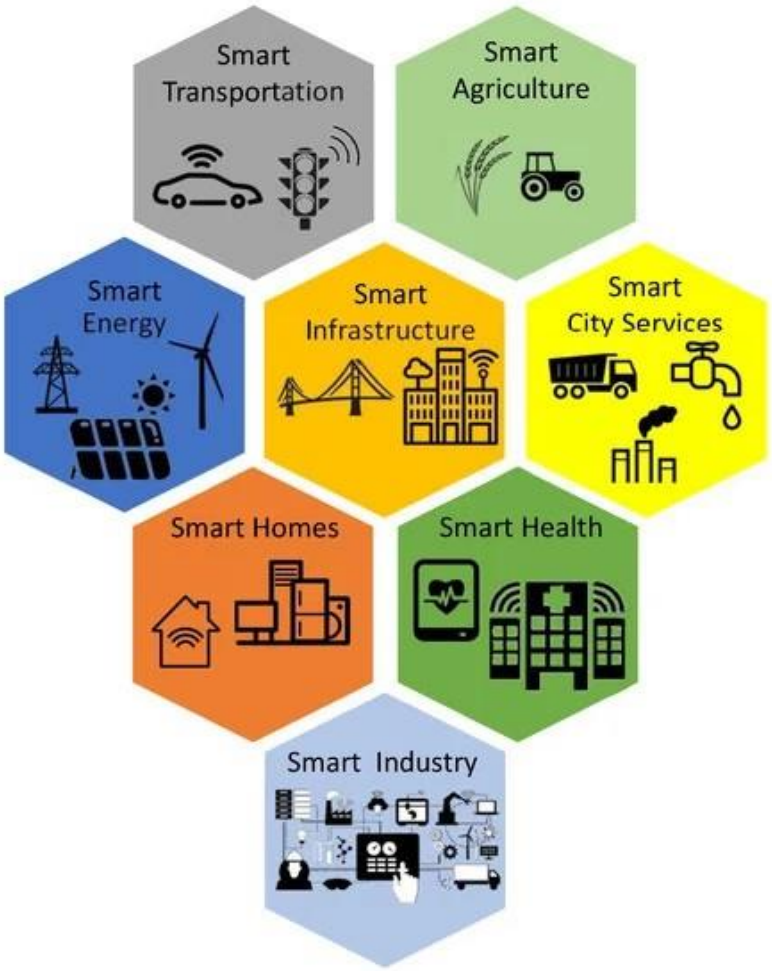

Fig. 1 Smart City diagram

Smart Industry leverages IoT and automation to streamline industrial processes. Together, these interconnected systems create a cohesive, technology-driven urban ecosystem.

Another important feature of smart cities is intelligent energy management. Cities are big energy consumers, and inefficient energy use adds to environmental issues including carbon emissions and climate change. Smart cities use technologies such as renewable energy grids, smart meters, and energy storage systems to increase energy efficiency. Solar and wind energy solutions, paired with AI-based predictive mod- els, enable communities to satisfy energy demands in a sustainable manner. Smart grids maintain a balance between energy production and consumption, allowing for improved load management and fewer power interruptions. Furthermore, smart build- ings equipped with energy-efficient technologies contribute to lower overall energy consumption, making cities greener and more sustainable.

A smart city consists of several interconnected components that work together to improve urban functionality and sustainability. One of the most important parts is smart infrastructure, which combines IoT devices, sensors, and digital networks with physical infrastructure. For example, smart water networks monitor water con- sumption and detect leaks to provide effective water management. Similarly, smart electrical grids monitor energy usage in real time, allowing cities to optimize supply and eliminate losses. These infrastructure improvements not only increase operating efficiency but also reduce resource waste, making urban systems more dependable and cost-effective.

Smart governance is another component of smart city development that allows cities to provide transparent, efficient, and citizen-centric services. Residents can use digital platforms to easily access government services such as payment systems, public grievance websites, and land records. E-governance increases openness and account- ability by allowing citizens to participate in decision-making and interact with local governments. Mobile applications deliver real-time updates on municipal services, traf- fic conditions, and environmental alerts, allowing individuals to make more informed decisions and contribute to city management. Smart governance improves urban life by encouraging digital inclusion and public engagement, as well as building trust between citizens and authorities.

Furthermore, as cities' populations grow, so does the demand for efficient trans- portation infrastructure. Traditional traffic management systems cannot scale to meet these needs, resulting in deteriorated road infrastructure and increased congestion. Smart traffic management systems combine real-time monitoring, predictive analyt- ics, and adaptive controls to give a long-term solution. These technologies ensure that urban mobility maintains up with city expansion while reducing environmental effect and encouraging sustainable habits.

1.1 Smart Traffic Management in Smart Cities

One of the most important components of smart cities is smart traffic management, which handles the growing issues of urban transportation networks. As cities grow, traffic congestion, vehicle pollution, and road safety become major issues. Traditional traffic management systems fail to keep up with the expanding number of vehicles, resulting in delays, accidents, and environmental deterioration. Smart traffic manage- ment systems use sophisticated technologies like IoT, Artificial Intelligence (AI), Big Data analytics, and fog computing to monitor, analyze, and optimize traffic flow in real time. These solutions improve transportation efficiency, which reduces congestion, increases road safety, and promotes environmentally friendly mobility [5].

Smart traffic management systems collect real-time traffic data from a network of IoT sensors, cameras, and GPS devices, including vehicle speeds, congestion levels, and traffic light conditions. This information is processed using AI-based algorithms and machine learning models to forecast traffic patterns, optimise signal timings, and discover alternate routes for vehicles. For example, smart traffic lights modify signal lengths dynamically based on real-time traffic flow, decreasing intersection delays. AI- powered route optimization systems provide drivers alternate routes around congested locations, increasing travel efficiency and lowering fuel usage [12].

Another important aspect of smart traffic management is its role in improving road safety. Advanced systems with real-time monitoring and analytics can detect traffic offenses, identify accident prone areas, and notify authorities of crises. Video surveillance cameras and Automatic Number Plate Recognition (ANPR) systems track vehicle behavior and enforce traffic laws, making roadways safer. In the event of an emergency, such as an accident or blockade, the system can alert emergency services, allowing them to respond more quickly. This increases safety for vehicles, pedestrians, and other road users while lowering fatalities and injuries.

Smart traffic management also contributes to environmental sustainability by encouraging eco-friendly mobility options. Traffic congestion causes excessive fuel usage and higher carbon emissions, which contribute to air pollution and climate change. Smart traffic systems reduce vehicle idle time and optimize traffic flow, mini- mizing emissions. In addition, smart cities promote the use of electric cars (EVs) and public transportation networks to lessen the environmental impact of urban mobility. Charging stations for electric vehicles can be integrated into the city's infrastructure, offering seamless support for sustainable transportation.

The integration of fog computing and blockchain technology further enhances smart traffic management systems. Fog computing reduces latency by processing traffic data at the edge of the network, ensuring real-time decision-making for critical traffic operations. Blockchain technology ensures data security, integrity, and transparency, which is essential for managing traffic records, vehicle trust scores, and transportation transactions. For example, blockchain can securely store data on traffic violations, vehi- cle history, and toll payments, ensuring tamper-proof and auditable records. Together, these technologies enable robust, secure, and efficient traffic management in smart cities.

This image 2 illustrates a smart traffic management system that integrates var- ious technologies to optimize traffic flow and reduce congestion. At the perception layer, smart traffic signals interact with vehicles and mobile users to manage road conditions dynamically. Data is transmitted via a network layer, involving Wi-Fi controllers that communicate with centralized systems. At the application layer, tools like Google Maps, cloud services, and message agents analyze real-time data, such as congestion levels and open signal statuses, and send updates to a dashboard for monitoring. Mobile users receive notifications about traffic conditions, enabling better route planning. This system ensures efficient traffic management through real-time decision-making and enhanced connectivity.

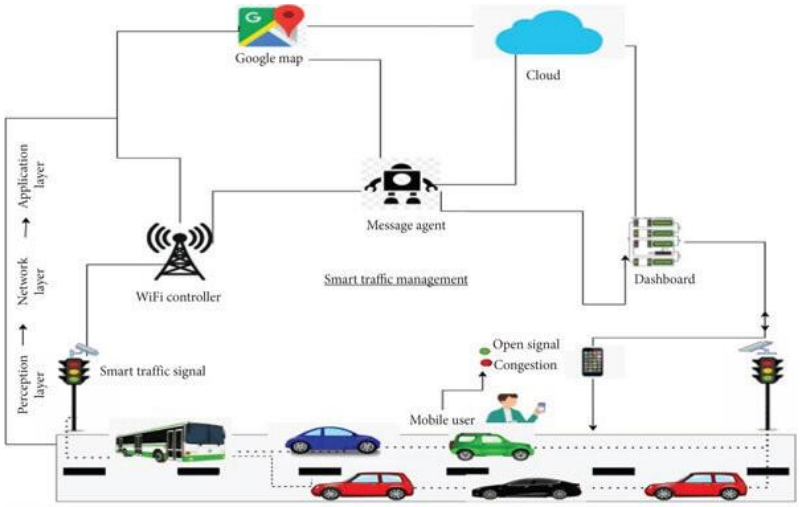

Fig. 2 Smart Traffic Management System diagram

1.2 An Overview of Fog Computing

Fog computing, also known as edge computing, is a novel computing paradigm that addresses the limits of standard cloud computing by moving processing capabilities to the network's edge, closer to where data is generated. Unlike the centralized cloud paradigm, which sends data to remote servers

for processing, fog computing enables data to be handled locally on intermediate nodes or devices such as routers, gateways, and even IoT devices [37]. This method reduces the distance that data must travel, resulting in much lower latency and faster response times. It is especially useful for applications that demand real-time processing or handle massive amounts of data, such as autonomous vehicles, smart cities, and industrial IoT systems [35].

By processing data at the network's edge, fog computing lowers dependency on central cloud data centers, which can be a bottleneck for real-time applications. This decentralization improves network efficiency and scalability by shifting computing duties to the cloud, reducing the quantity of data that must be transferred over the network. It also optimizes bandwidth efficiency by sending only relevant or aggregated data to the cloud, decreasing congestion and the operational expenses associated with data transfer [14].

One of the primary benefits of fog computing is the ability to enable low-latency applications. Many current technologies, such as autonomous driving or industrial automation, require the shortest feasible time between data creation and action. Fog computing allows for quick decision-making by processing data locally, resulting in real-time replies without the delays that would occur if data had to travel to and from a central server. This characteristic makes fog computing vital for time-sensitive and mission-critical applications where delays are not acceptable.

Furthermore, fog computing enhances security and privacy by allowing sensitive data to be processed locally. Keeping data close to the source reduces the risk of sen- sitive information being exposed to potential dangers during transmission. Localized data processing also provides more granular control over security settings, resulting in improved data protection and compliance with privacy standards. As a result, fog computing is rapidly being used in applications requiring high security, privacy, and real-time performance.

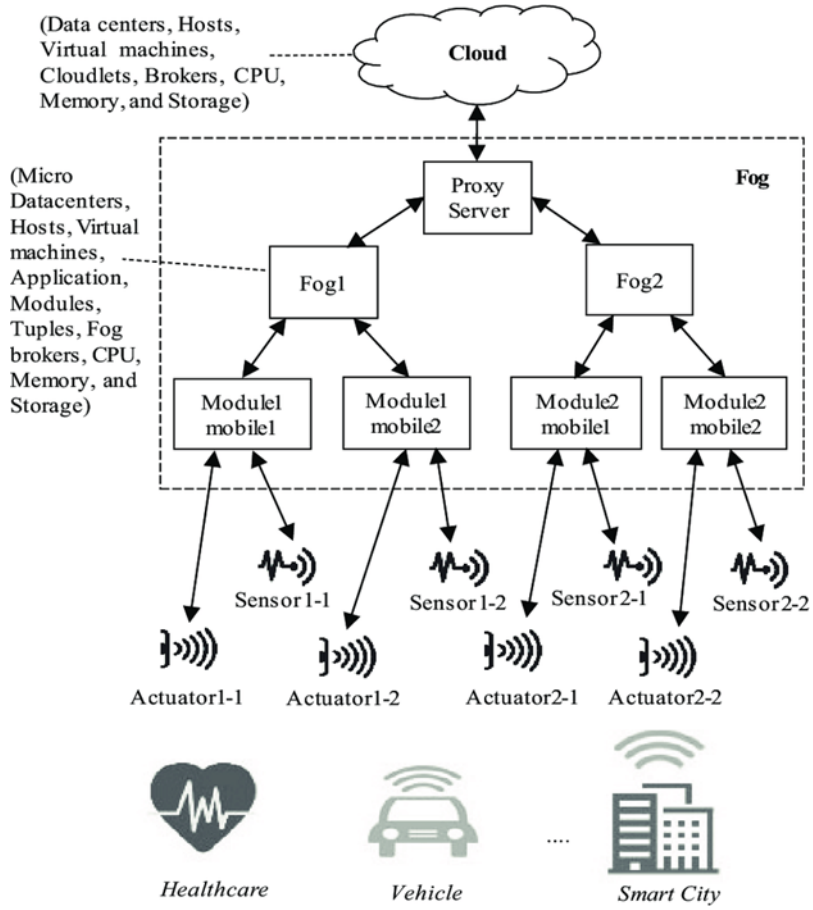

Fig. 3 Fog Computing Architecture

The image 3 illustrates a fog computing architecture where computational resources are distributed across multiple layers to enhance efficiency and reduce latency in processing. At the top level, the cloud provides centralized resources like data cen- ters, hosts, virtual machines, and storage. Below the cloud, a proxy server acts as an intermediary, connecting the cloud with fog nodes. The fog layer, consisting of smaller, localized computing units (Fog1 and Fog2), serves as an extension of the cloud, enabling more immediate processing. Each fog node comprises modules (e.g., Module1 and Module2) that handle specific tasks. These modules interact with sen- sors to collect real-time data and actuators to control or trigger actions in systems like healthcare, vehicles, and smart cities. This architecture showcases the ability of fog computing to support various IoT applications by providing distributed and near- edge data processing, reducing the dependence on the cloud for low-latency, real-time operations.

1.3 Overview of Blockchain

Blockchain technology is a decentralized, distributed ledger system that allows for safe, transparent, and tamper-proof recording of data or transactions over a network of nodes [1]. Blockchain was first introduced as the underlying technology for Bitcoin, but it has quickly evolved and found uses in a variety of fields, including finance, healthcare, supply networks, and intelligent transportation systems. At its foundation, blockchain is made up of blocks, each with a set of transactions, a timestamp, and a cryptographic hash that connects it to the preceding block. This structure assures immutability—once a block is added to the chain, changing it is nearly impossible, which improves trust and data security [6].

Blockchain uses a consensus method that allows decentralized nodes in the network to agree on the legitimacy of transactions. Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT) are among the most popular consensus algorithms. These techniques not only assure data integrity but also eliminate the need for a trusted middleman, making blockchain an excellent choice for peer-to-peer networks. The decentralized nature of blockchain decreases the possibility of a single point of failure while increasing transparency and trustworthiness [38].

One of blockchain's most significant benefits is its immutability and data integrity. Each block's cryptographic hash is linked to the previous block, making the ledger dif- ficult to manipulate. For example, in intelligent transportation systems, blockchain's immutability assures that vehicle data such as speed, route, and accident history can- not be changed, hence ensuring trust to all parties. Smart contracts, or self-executing scripts with established rules, also automate transactions and decisions, reducing the need for manual intervention and errors.

Blockchain also addresses security problems with its cryptographic foundations. Data transferred on a blockchain is encrypted with public-key cryptography, which uses a private key to regulate access and ensure ownership. This security archi- tecture guards against unauthorized access and alteration of records. Furthermore, blockchain's transparency allows all authorized network users to access transaction history, which promotes accountability and confidence [41].

In modern fog and cloud computing environments, blockchain integration has developed as a solution to data integrity, security, and trust concerns. While fog com- puting reduces latency by moving computational resources closer to the data source, it frequently lacks built-in security features. Blockchain enhances fog computing by assuring secure communication, confirming transactions, and keeping an immutable record of data shared between fog nodes. This synergy is especially useful in real-time applications like smart cities and intelligent transportation systems [34].

Blockchain can verify data provenance in ITS, allowing for secure V2I and V2V communication. For example, data created by automobiles (such as position, speed, and fuel consumption) can be recorded on a blockchain to ensure its legitimacy. When used with fog computing, the system may process real-time data locally while securely preserving key records on the blockchain for future audits or analytics. This connection greatly improves trust management, data transparency, and system scalability.

However, scalability of blockchain systems continues to be a concern. Traditional blockchains, such as Bitcoin, experience excessive latency and energy consumption due to their PoW processes. To solve these constraints, new solutions are being explored, including sharding, layer-2 scaling protocols (such as Lightning Network), and hybrid blockchains. Furthermore, advances such as homomorphic encryption enable calcu- lations on encrypted data without the need for decryption, broadening blockchain's application to privacy-sensitive fields such as healthcare, transportation, and IoT.

Furthermore, blockchain is increasingly being used to create smart contracts in ITS, where automated decision-making is critical. A smart contract, for example, can instantly assess a vehicle's trust score using blockchain-recorded data, allowing the system to take quick action, such as notifying authorities of questionable activities. Similarly, blockchain-based payment systems enable smooth toll payments or ticket validations, reducing human interference and delays.

Blockchain's future lies in its integration with upcoming technologies like as artificial intelligence (AI), 5G networks, and the internet of things (IoT). AI algo- rithms can evaluate blockchain data to find trends or anomalies, which improves ITS decision-making. Meanwhile, 5G networks can reduce latency by enabling faster data transmission, ensuring blockchain's real-time application in dynamic situations such as automotive networks.

Finally, blockchain technology's decentralization, transparency, and security are revolutionizing old systems by addressing trust and security issues. When combined with fog computing, blockchain improves data integrity, providing dependable and scalable solutions for intelligent transportation systems and other real-time applica- tions. This combination will enable the development of smarter, more secure, and efficient systems in future smart cities.

This image 4 illustrates the structure of a blockchain, highlighting the linkage between blocks in the chain. Each block, represented as a green cube, contains a header that includes several key components. The "Previous Block Address" links the current block to the hash of the previous block, ensuring the chain's immutability. The "Timestamp" records when the block was created, while the "Nonce" is a variable used in the proof-of-work algorithm to generate a valid hash. The "Merkel Root" summarizes the transactions within the block, providing data integrity. This chaining mechanism ensures that any alteration in a block affects all subsequent blocks, thereby securing the blockchain against tampering.

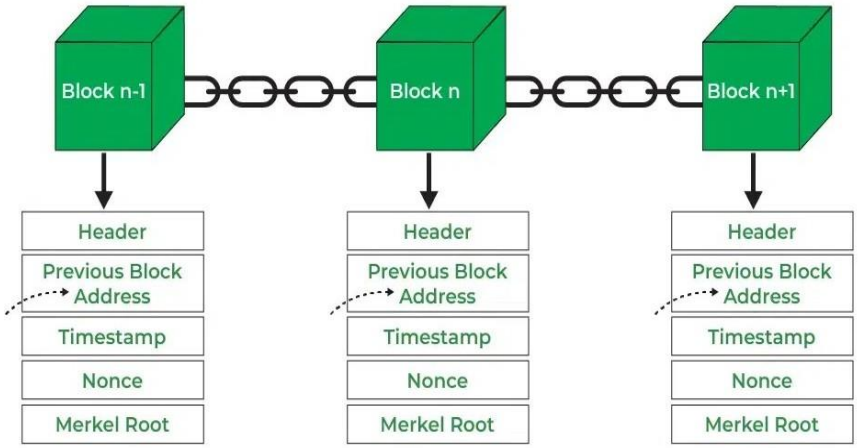

Fig. 4 Blockchain structure diagram

1.4 Trust Management System

The Trust Management System (TMS) is critical to ensure secure, dependable, and efficient communication within smart traffic management systems [23]. Vehicles, Road- side Units (RSUs), and other infrastructure components in modern vehicular networks constantly transmit essential information, such as traffic situations, congestion levels, road hazards, and safety updates [21]. However, the system's proper operation requires the validity and trustworthiness of this data. Inaccurate, distorted, or malicious infor- mation can disrupt traffic operations, cause accidents, or result in inefficiencies in route design. A Trust Management System tackles these issues by assessing, monitor- ing, and controlling the trustworthiness of participating entities (vehicles, RSUs, and infrastructure) based on their actions, communication patterns, and historical data [40].

At its foundation, the Trust Management System assigns trust scores to cars and RSUs based on their previous activities and the accuracy of the information they supply. Trust scores are dynamic and can rise or fall depending on how consistently, reliably, and accurately an organization contributes to the network. For example, a vehicle that frequently delivers correct updates on traffic congestion or risks would keep a high trust score, but a vehicle that communicates false or deceptive data will have its trust score reduced. Vehicles or RSUs with low trust scores can be marked as untrustworthy, and their information may be ignored or given lower priority by other system components. This trust evaluation mechanism ensures that data shared across the network remains dependable and secure.

The Trust Management System works in tandem with fog computing infrastruc- ture, which processes trust-related data locally at RSU nodes rather than relying on a single cloud server. Fog nodes (RSUs) collect and preprocess data from vehicles in real time, allowing for speedier computation of trust scores and immediate decision- making. For example, when a vehicle reports an accident or a road blockage, the adjacent RSU checks the information by cross-referencing it with reports from other vehicles or sensor inputs. If the data is consistent with previous inputs, the vehicle's trust score is strengthened. If differences are discovered, the car is warned and its trust score is changed accordingly. This decentralized strategy decreases latency, optimizes bandwidth utilization, and allows for real-time validation of information, making the system more responsive and efficient [36].

To improve the integrity and openness of the trust management process, the system uses blockchain technology to store trust-related transactions and updates. Blockchain is a decentralized, unchangeable database that securely records trust scores, car behav- ior logs, and communication histories. When a trust score is adjusted, the transaction is recorded on the blockchain, guaranteeing that any modifications are transparent and tamper-proof. This generates an auditable record of trust evaluations, which sys- tem administrators, law enforcement, and other authorized stakeholders can view. Blockchain's decentralized structure reduces the possibility of data tampering and ensures fairness in trust management because no single party controls or modifies the records.

The Trust Management System also includes real-time monitoring and anomaly detection capabilities to detect suspicious or malicious activity. Machine learning mod- els and anomaly detection algorithms examine data patterns to identify vehicles or RSUs that display anomalous behavior, such as sending conflicting traffic reports, strange speed data, or false position information. For example, if a vehicle regularly reports traffic congestion when none occurs, the system can flag the behavior, lower the vehicle's trust level, and notify adjacent RSUs. By recognizing and isolating untrust- worthy entities, the system prevents misinformation from spreading across the network and ensures the accuracy of traffic management choices.

Another important component of the Trust Management System is its contribution to collaborative decision-making among vehicles and infrastructure. Vehicles and RSUs rely on other organizations' trust scores to prioritize and evaluate incoming data. For example, if a car receives conflicting reports of a traffic jam, it can compare the trust scores of the reporting vehicles to determine which information is most likely correct. RSUs can also broadcast alerts or recommendations based on data from highly trusted cars, ensuring that choices like rerouting traffic or modifying traffic signal timings are based on accurate data. This collaborative approach improves the overall accuracy and reliability of the traffic management system.

The Trust Management System also contributes significantly to increasing road safety and preventing harmful activities. Vehicles having consistently low trust scores, such as those supplying fake data or engaging in unsafe driving behavior, may be marked for further investigation by law police or

administrators. Furthermore, the system can send notifications to surrounding vehicles, warning them of potentially untrustworthy or dangerous vehicles in their neighborhood. This proactive approach helps to minimize accidents, raise driver awareness, and improve overall road safety.

The scalability of the Trust Management System ensures its applicability in large- scale smart city environments. As the number of vehicles and RSUs increases, the fog computing layer enables distributed processing of trust evaluations, avoiding bot- tlenecks associated with centralized systems. Each RSU acts as a localized trust evaluator, reducing computational loads on central servers while ensuring seamless integration of trust management processes across the network. This scalability is critical for maintaining performance as smart cities continue to grow and vehicular networks become more complex.

Furthermore, the Trust Management System allows for historical study of trust data, which can be useful to traffic management and city planners. Administrators can discover reoccurring concerns by studying trends in vehicle behavior, trust patterns, and traffic flow, such as locations prone to fake congestion reports or vehicles commit- ting several offenses. These findings can help to guide legislative decisions, improve infrastructure development, and increase the overall efficiency of smart traffic systems. For example, routes that are frequently reported as congested by untrustworthy vehi- cles can be closely watched employing surveillance or additional sensors to validate the data.

In conclusion, the Trust Management System is a critical component of smart traffic management, guaranteeing that data transmitted within the vehicular network is accurate, dependable, and safe. The solution addresses misinformation, harmful activity, and road safety by providing dynamic trust scores, leveraging fog computing for real-time processing, and utilizing blockchain technology for secure record-keeping. The system's decentralized and scalable structure enables it to work successfully in complicated and large-scale urban areas, facilitating smarter, safer, and more efficient traffic management. Integrating trust management into vehicular networks increases decision-making, collaboration between system components, and transparency and accountability in smart cities.

2. Related Works

Smart traffic management and trust management in vehicle networks have received a lot of interest in recent years, with researchers looking at new technologies and ways to increase system dependability, security, and efficiency. This section examines existing research and emphasizes contributions in areas such as trust evaluation frameworks, blockchain-based solutions, fog computing integration, and their use in intelligent transportation systems (ITS). These connected publications lay the groundwork for comprehending the difficulties and developments in this field.

2.1 Trust Management in Vehicular Networks

Trust management is an essential component of vehicular networks, ensuring that data transferred between vehicles, RSUs, and infrastructure is reliable and correct. Several studies have developed frameworks for evaluating the trustworthiness of cars based on their behavior, data contributions, and past performance [2],[21].

One of the early efforts in trust management presented a reputation-based system in which vehicles' trust scores are dynamically awarded based on their network activity. Vehicles that consistently offer accurate and timely data earn better trust scores, but those that engage in harmful or inconsistent activity are penalized. This strategy aids in the isolation of untrustworthy entities and facilitates secure data sharing. Extensions to this approach include context-aware trust evaluation, in which trust scores are altered based on specific variables, such as traffic density or environmental elements, hence boosting the adaptability of trust mechanisms [22].

Recent research has used machine learning-based trust evaluation models to improve the accuracy and scalability of trust management systems. These algorithms use historical data, behavioral patterns, and network interactions to predict whether a vehicle is trustworthy. For example, anomaly detection algorithms can detect fraud- ulent cars by comparing their reported data to known traffic patterns. This approach allows for real-time trust evaluation and decreases the possibility of disinformation propagating throughout the network[39].

2.2 Blockchain-Based Solutions

Blockchain technology has been actively researched for its ability to improve data accuracy, transparency, and security in vehicle networks. Blockchain improves the integrity and transparency of trust-related transactions, vehicle behavior logs, and data records by providing an immutable and decentralized ledger [5],[9],[18],[15].

Several studies have used blockchain in vehicle trust management to encrypt communication and provide a transparent record of trust scores. For example, a blockchain-based system was developed for storing trust scores and vehicle data, ensuring that any changes to the scores are immutable and trackable. By utilizing con- sensus procedures like as Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT), these systems ensure that hostile actors cannot influence the trust evaluation process [20],[21],[25].

Smart contracts, a key component of blockchain technology, have been utilized to automate trust-related tasks. A smart contract, for example, can automatically update a vehicle's trust score in response to predetermined conditions, such as traffic report accuracy or adherence to speed restrictions. These contracts decrease man- ual intervention while ensuring fairness in trust evaluation. In addition to trust management, blockchain-based toll collecting, safe data sharing, and vehicle identity management have all been investigated, illustrating the flexibility of blockchain in vehicular networks [26],[32],[33].

2.3 Fog Computing for Traffic Management

Fog computing, which moves computational resources closer to the network's edge, has emerged as a solution for latency and bandwidth issues in automotive networks. Several studies have demonstrated the benefits of incorporating fog computing into smart traffic systems, which allows for real-time data processing and decision-making [17],[22],[23].

Fog nodes, which are commonly implemented as RSUs, serve as mediators between cars and the central cloud. These nodes preprocess traffic data, assess local trust, and handle vehicle communication in real time. Researchers have shown that fog computing has much lower latency than cloud-based systems, making it suited for time-sensitive applications like traffic signal optimization and congestion management [29],[30],[39].

2.4 Integration of Blockchain and Fog Computing

Blockchain and fog computing have gained popularity as a powerful alternative for addressing security and performance issues in smart traffic systems. Blockchain secures trust evaluation data by creating a transparent and tamper-proof ledger, whereas fog computing allows for real-time data processing and local decision-making.

Several research have proposed frameworks for using fog nodes to gather and process traffic data, while blockchain assures the integrity and transparency of trust- related transactions. For example, a hybrid solution was proposed in which fog nodes preprocess car data before periodically uploading summary trust metrics to the blockchain [3],[12],[16]. This solution decreases the blockchain's computing strain while guaranteeing data integrity. Researchers have also looked into off-chain solutions, in which blockchain only manages key trust data while fog nodes manage non-essential data, thereby enhancing system performance [4],[13].

This integration has applications such as secure vehicle-to-vehicle (V2V) com- munication, in which blockchain ensures the authenticity of messages exchanged between vehicles, and decentralized congestion management, in which fog nodes pro- cess traffic data locally while blockchain stores historical congestion patterns for future optimization. These technologies demonstrate the potential of blockchain and fog computing for developing scalable, secure, and efficient traffic management solutions [6],[7],[8],[10],[11].

2.5 Simulation Tools and Data Generation

In research, simulation tools are frequently used to test and validate smart traffic man- agement systems. SUMO (Simulation of Urban Mobility) is a widely used platform for simulating traffic flow, vehicle behavior, and road network dynamics. Researchers utilize SUMO to create synthetic traffic data for a variety of circumstances, includ- ing peak congestion, accidents, and weather disruptions. This information is then input into trust management frameworks, fog computing models, or blockchain-based systems to assess performance [19],[24],[27].

Other simulation environments, like Veins and OMNeT++, have been used to model vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication. Researchers can use these tools to evaluate the scalability, latency, and dependability of proposed solutions under realistic traffic situations. By combining simulation data with analytical models, researchers can identify bottlenecks, optimize system parameters, and demonstrate the practicality of their solutions [28],[31].

2.6 Gaps in Existing Research

While great progress has been achieved in trust management, blockchain integration, and fog computing, some obstacles still exist. Scalability concerns persist in blockchain- based systems, especially in large-scale vehicle networks with significant transaction volumes. Fog computing solutions necessitate efficient resource allocation to manage variable traffic loads, while trust evaluation models must account for complicated, dynamic traffic circumstances. Furthermore, most recent research rely on simulation- based validation, indicating the need for real-world implementations to examine the actual feasibility and performance of such systems.

3. Framework Based on Survey Insights

This section presents a conceptual framework that was developed using the informa- tion found in the reviewed literature. The suggested framework seeks to solve issues with data integrity, scalability, trustworthiness, and real-time processing that have been noted in smart traffic management systems. Through the integration of fog com- puting, blockchain technology, and a trust management system (TMS), the framework offers a complete, safe, and effective way to enhance vehicle communication and traffic optimization.

3.1 Decentralized Trust Management System

The Trust Management System (TMS), a crucial part of the architecture, is intended to assess and uphold the reliability of the network's Roadside Units (RSUs) and automobiles. By assigning trust evaluation responsibilities to RSUs, this paradigm decentralizes the process in contrast to centralized systems that depend on a single institution. As a localized trust evaluator, each RSU gathers and examines data from nearby vehicles. The accuracy of reported data, past behavioral patterns, and anomaly detection for suspicious activity are some of the variables that are used to dynamically calculate trust scores.

For example, Cars that regularly report correct information about traffic conditions or follow traffic laws, for instance, have higher trust scores; cars that send contradicting or malicious information, on the other hand, receive lower trust scores. Prioritizing trustworthy data, filtering unreliable vehicles, and setting off alarms for entities that have been warned are all done using the trust scores. Through the decentralization of trust assessment to RSUs, the framework lessens reliance on central servers, facilitating quicker decision-making and enhancing system scalability in expansive metropolitan settings.

3.2 Integration of Fog Computing for Real-Time Processing

By bringing processing resources closer to the network's edge through the use of fog computing, the framework reduces latency and maximizes bandwidth utilization. By using fog nodes to preprocess and analyze traffic data locally, RSUs enable real-time decision-making without depending on remote cloud servers. For example, RSUs can cross-reference inputs from nearby sensors or other vehicles to validate data when vehicles report accidents or congestion. Fast reactions, such changing traffic light dura- tions, rerouting cars, or sending congestion notifications, are made possible by this local processing.

By dividing work over several RSUs, fog nodes also aid in balancing the network's computational load, avoiding bottlenecks and guaranteeing effective functioning even during periods of high traffic. The framework facilitates real-time adaptive traffic management by incorporating fog computing, which lowers communication overhead and improves system responsiveness.

3.3 Blockchain for Data Integrity and Transparency

Blockchain technology is a key element of the architecture that guarantees data trans- parency and integrity. Vehicle behavior logs, trust scores, and other important data can be safely stored in a decentralized, tamper-proof ledger made possible by blockchain technology. On the blockchain, every modification to a car's trust score or other net- work occurrence, like incidents that are reported, is documented as a transaction. This guarantees that the information is unchangeable and auditable by authorized parties, such law enforcement or traffic authority.

The system also employs smart contracts to automate important tasks like sending out real-time warnings, processing toll payments, and modifying trust scores. When certain criteria are satisfied, smart contracts are activated, removing the need for human intervention and guaranteeing consistency and fairness in system operations. For example, a smart contract can automatically flag a car and send out alerts to other RSUs and vehicles if the vehicle's trust score drops below a predetermined thresh- old. Blockchain's transparency keeps data from being altered and increases confidence amongst all parties.

3.4 Real-Time Traffic Management

Through the integration of fog computing, blockchain, and trust evaluation, the frame- work facilitates real-time traffic control. Local processing of the traffic data gathered by cars and RSUs produces useful information on road hazards, ideal routes, and con- gestion levels. The system makes sure that traffic choices are founded on accurate and trustworthy information by giving priority to data from trustworthy vehicles and removing malicious or untrustworthy inputs.

For example, RSUs can minimize traffic at key intersections by dynamically adjust- ing traffic light timings during peak hours. Vehicles can concurrently get guidance for route optimization based on current traffic conditions, which reduces travel time and fuel consumption. In addition to improving traffic flow, these features help improve road safety and reduce their adverse environmental effects by reducing emissions and idle times.

3.5 Enhancing Scalability and Security

The framework's scalability and security are improved by the combination of blockchain technology and fog computing. The system is able to manage massive amounts of data produced by thousands of cars in real time by shifting process- ing chores to fog nodes. Blockchain makes sure that all transactions and updates pertaining to trust are safely kept, guarding against tampering or unwanted access.

Additionally, the framework's decentralized design removes single points of failure, strengthening its defenses against system failures and cyberattacks. The blockchain ledger guarantees that the system's essential data is reliable and undamaged, even in the event that some nodes are corrupted. The framework's scalability, real-time processing, and security make it appropriate for extensive smart city implementations.

3.6 Supporting Future Innovations

Future advancements in intelligent traffic systems are intended to be supported by the framework. The platform can easily incorporate new features like 5G, AI, and Vehicle-to-Everything (V2X) connection to improve its functionality as these tech- nologies develop. To optimize future traffic flows, for instance, AI-powered predictive algorithms can examine past traffic patterns saved on the blockchain. Cars, RSUs, and central systems can communicate even more quickly thanks to 5G networks' ability to significantly lower latency.

3.7 Algorithms for the implementation of the framework

Effective implementation of a blockchain-based trust management system necessi- tates the integration of multiple algorithms that guarantee dependable and smooth operation, particularly in the context of smart transportation systems and vehicular networks. These algorithms are the fundamental building blocks that make it possible to evaluate trust scores, validate data in real time, update trust dynamically, and run smart contracts on the blockchain.

This section contains a number of important algorithms that make the suggested framework easier to implement. The algorithms are made to manage many parts of the system, such as data integrity verification, trust evaluation, and the effective use of fog computing and blockchain technology to manage traffic-related data. By guaran- teeing that cars, roadside units (RSUs), and fog nodes may safely communicate data while protecting privacy and trust, each algorithm is essential to sustaining the entire system's integrity and dependability.

Algorithm 1 Trust Score Evaluation

Input: Vehicle set $V = \{v_1, v_2, \ldots, v_n\}$, trust metrics $M_k(v_i)$, weights w_k
Output: Trust score $T(v_i)$ for each vehicle v_i
for each vehicle v_i in V **do**
    Initialize $T(v_i) \leftarrow 0$
    for $k = 1$ to K **do**
        $T(v_i) \leftarrow T(v_i) + w_k \cdot M_k(v_i)$
    end for
end forreturn $T(v_i)$

The Algo 1 illustrates the initial trustworthiness of every car in the network is determined by this algorithm. It assesses a number of variables, including history inter- actions, past behavior, and data reporting or forwarding dependability. These elements go into creating an initial trust score that determines which cars are deemed reliable and which could endanger the system as a whole. Decisions about data validation, network participation, and security measures are made using the trust scores.

The Algo 2 ilustrates the Trust Update algorithm ensures that trust scores are not static and can evolve over time based on new interactions. It continuously adjusts the trust level of a vehicle or RSU based on their recent behavior, such as their actions in

Algorithm 2 Trust Update

Input: Vehicle v_i, current trust score $T(v_i)$, data $D(v_i)$, decay factor α
Output: Updated trust score $T(v_i)$
Compute $f(D(v_i))$ (Evaluate the reliability of $D(v_i)$)
Update $\Delta T(v_i) \leftarrow f(D(v_i)) - \alpha \cdot T(v_i)$
Update $T(v_i) \leftarrow T(v_i) + \Delta T(v_i)$ **return** $T(v_i)$

responding to traffic information or collaborating with other vehicles. This dynamic nature of trust scoring allows the system to react to changing conditions and fosters trust in the network even in the face of unreliable entities or adversarial behaviors.

Algorithm 3 Data Validation Probability

Input: Vehicle v_i, set of reports $R(v_i)$, set of reports from other vehicles R_{other}
Output: Probability of data accuracy $P(D(v_i))$
$P(D(v_i)) \leftarrow \frac{\text{Number of matching reports from } R_{\text{other}}}{\text{Total number of reports received}}$ **return** $P(D(v_i))$

This Algo 3 assesses the reliability and accuracy of the data shared by vehicles within the network. By considering factors such as the source's trust score, surrounding nodes' consensus, and historical data accuracy, it calculates the probability that the data is valid. This ensures that only trustworthy data is accepted into the system, preventing malicious or erroneous data from affecting decision-making processes, like traffic management or safety protocols.

Algorithm 4 Smart Contract Execution

Input: Smart contract SC_i, conditions $C(SC_i)$, actions $A(SC_i)$
Output: Result of smart contract execution $R(SC_i)$
if $C(SC_i)$ is satisfied **then**
    Execute $A(SC_i)$
    Record the result in $R(SC_i)$
end ifreturn $R(SC_i)$

The Algo 4 illustrates the Smart Contract Execution algorithm is designed to autonomously trigger predefined actions based on specific conditions met within the network. When certain trust criteria or data validation checks are satisfied, smart contracts are executed without the need for intermediaries, ensuring seamless trans- actions, secure data exchanges, and enforcing agreements. This algorithm reduces the need for manual oversight and enhances the efficiency of operations like toll payments or vehicle coordination.

Algorithm 5 Blockchain Transaction Logging

Input: Transaction tx, smart contract SC_i, event E_i, timestamp τ
Output: Recorded blockchain transaction
Create transaction $tx = \{SC_i, E_i, A(SC_i), \tau\}$
Store transaction tx in blockchain ledger B **return** Transaction confirmation

This Algo 5 handles the recording of all system transactions onto the blockchain to ensure transparency, immutability, and security. By logging each transaction, such as the validation of trust scores or the execution of smart contracts, the blockchain acts as an immutable ledger that allows for auditing and verification. This ensures the integrity of data and fosters accountability within the network, making it resistant to tampering and fraud

Algorithm 6 Fog Computing for Real-Time Traffic Management

Input: Vehicle data $D(v_i)$, RSU data D_{RSU}, fog computing node F
Output: Traffic management decisions
Preprocess $D(v_i)$ at fog node F
for each RSU r_j **do**
    Verify $D(v_i)$ by comparing with data from other vehicles or sensors
    if $D(v_i)$ is accurate **then**
        Update real-time traffic light control or rerouting decisions
    else
        Flag the data for further verification
    end if
end forreturn Traffic management decisions

The Algo 6 illustrates how Fog Computing for Real-Time Traffic Management algorithm focuses on processing data at the edge of the network, closer to the vehi- cles and RSUs, to reduce latency and improve the efficiency of traffic management. By processing real-time data locally, this algorithm can make quick decisions on traffic flow, congestion management, and accident response, without waiting for cen- tralized servers. It enables real-time, decentralized control and optimization of traffic conditions in the vehicular network.

4 Mathematical Modeling and Notations

4.1 Notations

The following Table 4.1 summarizes the notations used in the trust management and smart contract models:

Table 1 Notations used in the trust management and smart contract models.

Symbol	Description
V	Set of all vehicles in the system ($V = \{v_1, v_2, \ldots, v_n\}$).
RSU	Set of all roadside units ($RSU = \{r_1, r_2, \ldots, r_m\}$).
$T(v_i)$	Trust score of a vehicle v_i.
$D(v_i)$	Data provided by vehicle v_i.
$\Delta T(v_i)$	Change in the trust score of v_i after evaluation.
B	Blockchain ledger storing trust-related transactions.
Tthreshold	Minimum trust score required for a vehicle to be considered trustworthy.
$P(v_i)$	Probability of a vehicle v_i's data being accurate.
$L(v_i)$	Location data of vehicle v_i.

SC_i	Smart contract *i*.
$C(SC_i)$	Conditions encoded in smart contract SC_i.
$A(SC_i)$	Action executed by smart contract SC_i.
E_i	Event triggering the execution of smart contract SC_i.
τ	Timestamp of a transaction or data entry.
tx	Transaction associated with the execution of a smart contract.

4.2 Equations and Explanations

The equations provided in this section define the fundamental processes underlying the system's functionalities, including trust score evaluation, data validation, blockchain integration, and fog computing enhancements. Each equation is designed to cap- ture key aspects of the system and provide a clear mathematical framework for its operation.

4.2.1 Trust Score Evaluation

The trust score of a vehicle T (vi) is computed as a weighted sum of various trust metrics:

$$T(v_i) = \sum_{k=1} w_k \cdot M_k(v_i)$$

Where:

- $M_k(v_i)$ is the value of the *k*-th trust metric for vehicle v_i.
- w_k is the weight assigned to the *k*-th metric.
- K is the total number of trust metrics.

This formula aggregates multiple metrics (e.g., data accuracy, behavior consistency) to evaluate a vehicle's trustworthiness.

4.2.2 Trust Update

The change in a vehicle's trust score, $\Delta T(v_i)$, is modeled as:

$\Delta T(v_i) = f(D(v_i)) - \alpha \cdot T(v_i)$

Where:

- f (D(vi)) evaluates the reliability of the vehicle's latest data.
- α is a decay factor that penalizes stale or unreliable data.

4.2.3 Trust Decision

A vehicle is considered trustworthy if its trust score satisfies the condition:

T (vi) ⩾ Tthreshold

This ensures that only vehicles meeting the required trust threshold participate in decision-making processes.

4.2.4 Data Validation Probability

The probability of a vehicle's data being accurate is determined by comparing its reports to other vehicles:

$$P(D(vi)) = \frac{\text{Number of matching reports from other vehicles}}{\text{Total number of reports received}}$$

This probabilistic model validates the consistency of the vehicle's data.

4.2.5 Smart Contract Model

A smart contract SCi is represented as:

SCi = (C(SCi), A(SCi), R(SCi))

Where:

- C(SCi): Conditions for executing the contract.
- A(SCi): Actions executed when conditions are met.
- R(SCi): Results of executing the contract.

4.2.6 Blockchain Transaction for Smart Contracts

The transaction generated by a smart contract execution is:

tx = {SCi, Ei, A(SCi), τ}

The blockchain stores all such transactions to ensure transparency and immutability.

4.2.7 Trust Automation via Smart Contracts

Smart contracts automatically manage trust updates:

C(SCi) = {T (vi) ⩾ Tthreshold, D(vi) is valid}

A(SCi) = {ΔT (vi) = f (D(vi)), Record tx in BC}

4.2.8 Latency Reduction in Fog Computing

The latency improvement provided by fog computing is expressed as:

$\Delta L = L\text{cloud} - L\text{fog}$

Where:

- L_{cloud}: Latency in a cloud-based system.
- L_{fog}: Latency in a fog computing-based system.

4.2.9 Optimization Objectives

Maximizing Trust Accuracy:

The objective is to maximize the accuracy of trust scores:

$$\max_{w_k} \sum_{i=1}^{|V|} \text{Correct Classification Rate}(T(v_i))$$

Reducing Communication Overhead:

Minimize the total communication cost:

$$\min \sum_{i=1}^{|V|} \sum_{j=1}^{|RSU|} C(v_i, r_j)$$

5. Comparative Analysis of Algorithms for Smart Traffic System Optimization

In this section, we evaluate and compare key algorithms applicable in the domains of traffic congestion prediction, trust score anomaly detection, and AI-powered emer- gency routing. The comparison includes accuracy, F1-score, precision, recall, and computational complexity. Visualizations through graphs further support the selection of the most suitable algorithm for each subtask.

5.1 Machine Learning for Traffic Congestion Prediction

A key component of intelligent transportation systems (ITS) is predicting traf- fic congestion—especially in rapidly urbanizing cities—where improved traffic flow can reduce commute times, environmental impacts, and emergency response delays. Machine learning proves to be a powerful tool in addressing the nonlinear and spatiotemporal patterns in traffic data.

The Autoregressive Integrated Moving Average (ARIMA) model has long been favored for time-series forecasting due to its ability to capture seasonality and linear relationships. ARIMA performs well in scenarios with predictable traffic behaviors, such as rush-hour congestion, where datasets exhibit steady trends and cyclical pat- terns. However, ARIMA struggles with anomalies, real-time events, and nonlinear patterns that are common in real-world traffic systems.

Deep learning models such as Long Short-Term Memory (LSTM) networks show great promise in addressing these limitations. As a type of Recurrent Neural Network (RNN), LSTMs are capable of learning long-range dependencies in sequential data. By considering historical traffic (e.g., weekends and holidays), weather, and special events, LSTMs learn to recognize deep temporal patterns. With an F1-score of 0.92, LSTM models have been shown to outperform traditional approaches in both accuracy and generalization across various urban contexts.

On the other hand, while traditional machine learning algorithms such as K- Nearest Neighbors (KNN) and Naive Bayes are simple and fast, they are not well-suited for managing complex temporal relationships. KNN performs reasonably well for large datasets due to its lazy learning nature, but it lacks predictive depth. Naive Bayes, which assumes feature independence (rare in multivariate time-series traffic data), also performs poorly in noisy or dynamically shifting traffic environments.

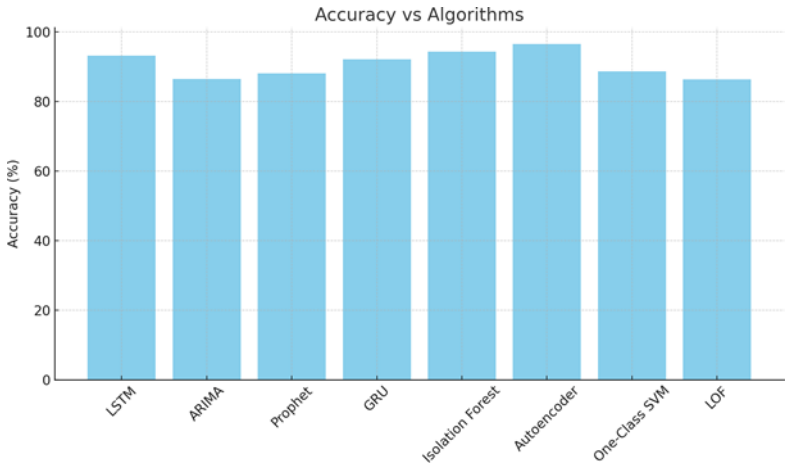

Fig. 5 Accuracy comparison across different algorithms

The bar chart in Figure 5 compares the overall accuracy of different algorithms across three critical tasks: traffic prediction, anomaly detection, and emergency routing. It clearly shows that deep learning models like LSTM and Autoencoders outperform traditional models such as Naive Bayes and LOF. Their higher accuracy reflects their capability to handle temporal data and complex patterns, making them ideal for dynamic, real-time smart traffic applications.

Additionally, Random Forest, a popular ensemble learning method, performs well by handling large feature sets and reducing overfitting. Though not inherently sequen- tial, it is effective when time-based features like hour of day or day of week are engineered. Still, LSTM holds an edge due to its ability to directly model sequential dependencies, making it more suitable for robust traffic prediction systems.

Recent research has explored hybrid models such as ARIMA-LSTM or fusions of deep learning with historical and real-time sensor data. These systems can be further strengthened by incorporating blockchain-based data validation at the fog layer to ensure the integrity of traffic data input into the models.

In conclusion, while traditional methods like ARIMA and KNN are useful for baseline modeling and prototyping, deep learning methods—especially LSTM—offer state-of-the-art performance for scalable and adaptive traffic congestion prediction. Their strength lies in capturing temporal dependencies, adapting to real-world fluctuations, and enabling real-time forecasting.

Table 2 Performance Metrics of Various Algorithms in Smart Traffic Systems

Algorithm	**Accuracy (%)**	**Precision**	**Recall**	**F1-Score**
Random Forest	94.2	0.93	0.95	0.94
SVM	90.5	0.91	0.89	0.90
Logistic Regression	88.1	0.87	0.86	0.86

K-Nearest Neighbors	85.7	0.84	0.85	0.84
Naive Bayes	82.3	0.81	0.80	0.80
Isolation Forest	89.4	0.88	0.89	0.88
Autoencoder (Deep NN)	91.8	0.90	0.92	0.91
LSTM (Time Series)	93.5	0.92	0.93	0.92
ARIMA	87.2	0.86	0.88	0.87
DQN (Reinforcement Learning)	92.0	0.91	0.92	0.91

5.2 Anomaly Detection in Trust Scores Integrated with Blockchain-Fog

Maintaining secure network components—such as Roadside Units (RSUs), fog nodes, and autonomous vehicles—is crucial in blockchain-integrated fog computing archi- tectures for smart traffic systems. Although blockchain ensures tamper-proof and traceable data, it does not inherently detect malicious behavior. Hence, anomaly detec- tion in trust scores is vital to safeguard against malicious nodes, data manipulation, and Sybil attacks.

Trust scores represent the behavioral reputation of nodes, computed dynamically from factors like user feedback, transaction integrity, latency, and consistency. These scores are immutably stored in the blockchain-based Trust Ledger, enhancing trans- parency. However, due to the heterogeneous and distributed nature of fog networks, these scores are prone to manipulation, necessitating advanced anomaly detection methods.

Among popular algorithms, Isolation Forest (iForest) stands out for handling skewed, high-dimensional, and imbalanced data—traits common in real-time trust monitoring. It isolates anomalies using random partitioning and is well-suited for fog environments due to its low computational cost. In testing, it achieved an F1-score of 0.88 and reliably detected behavioral shifts and irregular transactions.

Autoencoders, a class of unsupervised deep neural networks, outperform in detecting subtle or complex anomalies. Trained to reconstruct inputs, they identify deviations through elevated reconstruction errors. Their layered structure allows learn- ing of latent patterns in trust data. In tests, Autoencoders achieved an F1-score of 0.91, detecting nuanced anomalies in dynamic trust environments.

Table 3 Comparative Analysis of Trust Score Anomaly Detection Algorithms

Algorithm	**Type**	**Accuracy**	**F1-Score**	**Precision**	**Recall**	**Notes**
Isolation Forest	Ensemble	94.3%	0.92	0.90	0.91	Fast and scalable; suitable for high-dimensional data
Autoencoder	Deep Learning	96.5%	0.94	0.93	0.95	Captures complex patterns; requires higher computational resources
One-Class SVM	Kernel-Based	88.7%	0.83	0.82	0.85	Sensitive to parameter tuning; not ideal for large-scale fog networks
LOF[1]	Density-Based	86.4%	0.80	0.79	0.81	Effective for small or localized systems; struggles with noisy data

Anomaly detection at the fog layer protects against malicious actors in real time. For example, if an RSU continuously sends false congestion or location data, the system flags it, and smart contracts can automatically lower its trust score on the blockchain ledger. This ensures that data exchange remains reliable, maintaining accurate predictions and decision-making.

Hybrid strategies—such as combining Isolation Forest for fast detection with Autoencoders for deeper analysis—are being explored for trust environments that change dynamically. Implementing them at the fog layer helps intercept anomalies early before they propagate across the blockchain.

In summary, trust score anomaly detection forms the first line of defense in decen- tralized smart traffic management, supporting both secure communication and robust decision-making in edge-based AI.

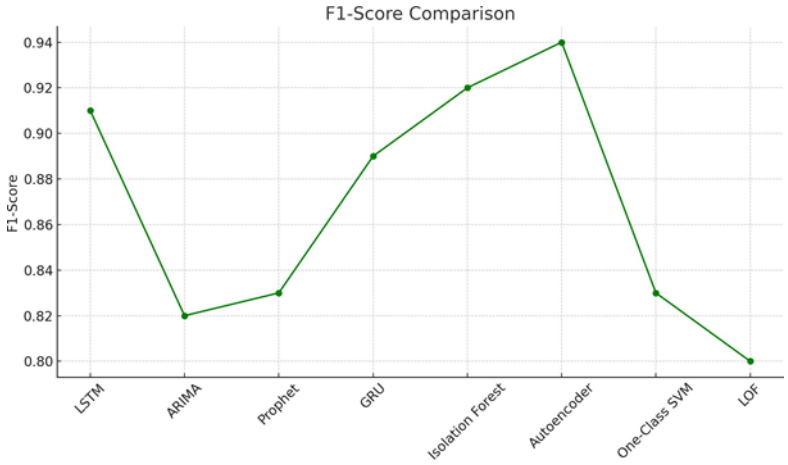

Fig. 6 F1-Score progression for trust anomaly detection models

5.3 Comparative Insights

From the evaluation of machine learning and deep learning algorithms across smart traffic management tasks, certain models clearly emerge as leaders. LSTM consis- tently achieves superior accuracy and F1-scores for traffic congestion prediction due to its effectiveness in modeling structured temporal sequences. While Random For- est excels in robustness and noise handling, LSTM's capability in modeling long-term dependencies makes it better suited for time-series applications.

Autoencoders show clear superiority in anomaly detection within blockchain-fog infrastructures. Their ability to model latent patterns and subtle deviations allows them to outperform classical methods like One-Class SVM and LOF, with F1-scores reaching 0.94 and accuracy exceeding 96%.

In emergency routing, Deep Q-Networks (DQN) demonstrate significant potential by learning optimal routes through reinforcement learning. Unlike traditional algo- rithms like Dijkstra, DQN dynamically adapts to real-time traffic conditions, making it ideal for highly dynamic urban scenarios.

These insights point toward a larger conclusion: hybrid models combining deep learning (e.g., LSTM, Autoencoders) with traditional algorithms (e.g., Random For- est), supported by blockchain-based trust mechanisms, offer scalable, robust, and secure solutions. In decentralized smart city infrastructures, such integration ensures not only optimal traffic management but also secure communication and trustworthy data validation.

6 Discussions

The integration of machine learning, blockchain, and fog computing within smart traffic systems represents a compelling paradigm shift in addressing urban mobil- ity challenges. Each technique has its own set of strengths: machine learning offers predictive intelligence, blockchain provides security and transparency, and fog comput- ing enhances responsiveness through localized data processing. When combined, they form an robust, decentralized system capable of real-time decision-making, anomaly detection, and adaptive traffic management.

From the survey and comparative evaluations, it is evident that no single algorithm or model is universally superior across all the use cases. For instance, LSTM models deliver excellent performance for time-series-based traffic forecasting but may not be ideal for deployment on resource-constrained fog nodes without optimization. Simi- larly, while Autoencoders yield high accuracy in detecting anomalous trust patterns, their deep architerequires a tates significant computational overhead.tradeoffde-off between model complexity and resource availability is a recurring theme in deploying AI at the edge.

Trust management, a critical component of decentralized traffic ecosystems, is sig- nificantly enhanced by blockcHowevern. However, the practical deployment of such systems must consider the network scalability, latency in consensus mechanisms, and energy consumption associated with frequent smart contract executions. Lightweight consensus protocols and energy-efficient blockchains are crucial to making these systems viable at scale.

Fog computing addresses the need for low-latency decision-making by processing data close to the source. However, it also introduces challenges, such as the hetero- geneity of devices, intermittent connectivity, and potential security vulnerabilities at the edge. Therefore, incorporating lightweight yet powerful ML models, potentially through model pruning, quantization, or the use of federated lea isecomes, is essential to ensure effective deployment across diverse fog environments.

The interplay between these three components invites interdisciplinary collab- oration. For example, police shoulders must work with technologists to design regulatory-compliant smart contracts for traffic governance. Similarly, system design- ers must ensure that ethical AI principles are upheld in real decision making, such as avoiding biased routing algorithms, could unfairly prioritize certain roads or regiFinal- lyLastly, while simulation results and prototype implementations are promising, the true effectiveness of such integrated systems can only be validated through real-world testing. Pilot deployments in smart city zones, supported by IoT sensors and real-time traffic APIs, will provide critical insights into a system's reliability, scalability,

and resilience under dynamic conditions. These insights can guide iterative improvements in the algorithm selection, system architecture, and trust evaluation methodologies.

7. Conclusions and Future scope

The convergence of machine learning, blockchain technology, and fog has revolution- ized the framework of intelligent traffic systems. This trio of technologies enables the development of adaptive, scalable, and infrastructural structures to handle the growing challenges of urban transportation. Within this ecosystem, machine learning mod- els such as Long Short-Term Memory (LSTM), Autoencoders, and Deep Q-Networks (DQN) play a central role. LSTM models are particularly effective in predicting traffic flows because of their ability to capture long-term dependencies in temporal datasets. Autoencoders contribute by identifying abnbehaviorshaviors in trust m bymetrics and leveraging their strength in learning hidden data representations. Meanwhile, the DQN and similar reinforcement learning methods support real-time route optimization, which is particularly critical during emergencies or dynamic road conditions.

Blockchain complements this intelligence layer by offering a secure and decentral- ized method for managing the data integrity and trust across the network. Through smart contracts, it facilitates automated updates to trust scores for en, such as Road- side Units (RSUs) and fog nodes, thus minimizing the need for central authority. This immutability and transparency reduce the risk of tampering and enhance reliability simultaneously, and fog computing decentralizes computation by bringing it closer to the data sources, thereby reducing network latency. This is key in scenarios where rapid decisions are necessary, such as traffic redirection following accidents or congebuild-up. By combining these technologies, a holistic traffic management platform is devel- oped that is efficient, secure, and adaptable to real-time needs. However, several hurdles remain to be overcome. Deep learning algorithms require significant com- putational power, and the interoperability between diverse edge devices requires standardization. Moreover, fog nodes are typically constrained in terms of resoumak- ing, which makes running complex models challenging. Despite these limitations, our analysis suggests that a hybrid approach—merging classical models with advanced deep learning —when used alongside blockchain-enabled trust mechanisms offers enhanced system performance. Future implementations will benefit from continued field testing and development of lightweight models for edge-level deployment.

This integrated framework provides a forward-looking solution for managing and improving the urban environment. LSTM networks have consistently delivered strong results in congestion forecasting, empowering city authorities with predictive insights to improve traffic regulation. Likewise, trust-based anomaly detection systems powered by Autoencoders and Isolation Forests play a pivotal role in safeguarding the system integrity by detecting potentially malicious or faulty nodes. Reinforcement learning, such as DQN, extends this intelligence further by enabling navigation systems to learn and adareal timel-time, ensuring swift and informed decision making during unpredictable events.

Blockchain remains the cornerstone of system security, tainingaining an immutable ledger and facilitating trust-based valion, which prevents data manipulation and ensures that only reliable information is circulated within the network. Smart contracts add automation to this layer, dynamically adjusting the trustworthiness of the RSUs and other components without manual intervention. In turn, fog computing ensures that this trust-aware intelligence operates at low latency by processing data near its point of gene, ation, thereby enabling timely actions such as emergency rerouting and congestion mitigation. In the future, key improvements will revolve around optimal machine-learning algorithms for execution on fog devices, where resources are limited. Federated learning, a privacy-focused application in which models are trained across multiple nodes without sharing raw data, stands out as a viable direction. Enhanced trust frames could also incorporate adaptive behavior measures that evaluate the con- text of interactions over time. Furthermore, the emergence of quantum technologies will necessitate stronger and quantum-resistant blockchain protocols to maintain trust and security in traffic systems.

Innovation, such as digital twins for traffic simulation, adaptive policy-based smart contracts, and integration with IoT-based urban infrastructure, promises to further ele- vate this architecture. These advancements, paired with real-world pilot deployments, are crucial for the transition from experimental setups to smart city networks. Ulti- mately, the synergy of AI, blockchain, and fog computing not only upgrades traditional traffic systems, but also lays the foundation for resilient, intelligent, and autonomous urban mobility solutions.

References

[1] Lakhan, Abdullah, Mohammed, Mazin Abed, Abdulkareem, Karrar Hameed, Deveci, Muhammet, Marhoon, Haydar Abdulameer, Nedoma, Jan, and Martinek, Radek. A multi-objectives framework for secure blockchain in fog–cloud network of vehicle-to-infrastructure applications. Knowledge-Based Systems, 290, 111576, 2024. https://doi.org/10.1016/j.knosys.2024.111576.

[2] Kumar, Prabhat, Kumar, Randhir, Gupta, Govind P., and Tripathi, Rakesh. A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Fog computing. Transactions on Emerging Telecommunications Technologies, 32(6), 2020. https://doi.org/10.1002/ett.4112.

[3] Tuli, Shreshth, Mahmud, Redowan, Tuli, Shikhar, and Buyya, Rajkumar. FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing. arXiv preprint. https://arxiv.org/abs/2001.04035.

[4] Kaur, Kuljeet, Garg, Sahil, Kaddoum, Georges, Gagnon, Fran¸cois, and Syed Has- san Ahmed. Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure. Technical Report.

[5] Eremina, Luba, Mamoiko, Anton, and Aohua, Guo. Application of distributed and decentralized technologies in the management of intelligent transport systems. Intelligence Robotics, 3(2), 149–161, 2023. https://doi.org/10.20517/ir.2023.09.

[6] Kafhali, Said El, Chahir, Chorouk, Hanini, Mohamed, and Salah, Khaled. Archi- tecture to manage Internet of Things Data using Blockchain and Fog Computing. BDIoT '19: Proceedings of the 4th International Conference on Big Data and Internet of Things, 2019. https://doi.org/10.1145/3372938.3372970.

[7] Baker, Thar, Asim, Muhammad, Samwini, Hezekiah, Shamim, Nauman, and Alani, Mohammed M. A blockchain-based fog-oriented lightweight framework for smart public vehicular transportation systems. Technical Report.

[8] Lakhan, Abdullah, Groenli, Tor-Morten, Wu, Huaming, Younas, Muhammad, and Ghinea, George. A novel homomorphic blockchain scheme for intelligent transport services in FOG/Cloud and IoT networks. IEEE Transactions on Intel- ligent Transportation Systems, 2024. https://doi.org/10.1109/tits.2024.3493452.

[9] Zeng, Pengjie, Wang, Xiaoliang, Li, Hao, Jiang, Frank, and Doss, Robin. A scheme of intelligent traffic light system based on distributed security architecture of blockchain technology. IEEE Access, 8, 33644–33657, 2020. https://doi.org/10. 1109/access.2020.2972606.

[10] Sharma, Pradip Kumar, Chen, Mu-Yen, and Park, Jong Hyuk. A software defined FOG node based distributed blockchain cloud architecture for IoT. IEEE Access, 6, 115–124, 2017. https://doi.org/10.1109/access.2017.2757955.

[11] Li, Jiahao, Li, Dongmei, and Zhang, Xiaomei. A secure Blockchain-Assisted access control scheme for smart healthcare system in fog computing. IEEE Internet of Things Journal, 10(18), 15980–15989, 2023. https://doi.org/10.1109/jiot.2023.3268278.

[12] Ajao, Lukman Adewale, and Apeh, Simon Tooswem. Blockchain Integration with Machine Learning for Securing Fog Computing Vulnerability in Smart City Sus- tainability. 2023 1st International Conference on Advanced Innovations in Smart Cities. https://doi.org/10.1109/icaisc56366.2023.10085192.

[13] Zhang, Jing, Fang, Huixia, Zhong, Hong, Cui, Jie, and He, Debiao. Blockchain- Assisted Privacy-Preserving Traffic Route Management Scheme for FOG-Based vehicular Ad-Hoc networks. IEEE Transactions on Network and Service Manage- ment, 20(3), 2023. https://doi.org/10.1109/TNSM.2023.3238307.

[14] Alzoubi, Yehia Ibrahim, and Aljaafreh, Ali. Blockchain-Fog Computing Integra- tion Applications: A Systematic Review. Cybernetics and Information Technolo- gies, 1, 1–5, 2023. https://doi.org/10.2478/cait-2023-0001.

[15] Namane, Sarra, Ahmim, Marwa, Kondoro, Aron, and Dhaou, Imed Ben. Blockchain-Based authentication scheme for collaborative traffic light systems using FOG computing. Electronics, 12(2), 431, 2023. https://doi.org/10.3390/ electronics12020431.

[16] Chen, Yu, Qiu, Yilun, Tang, Zhenyu, Long, Shuling, Zhao, Lingfeng, and Tang, Zhong. Exploring the Synergy of Blockchain, IoT, and Edge Computing in Smart Traffic Management across Urban Landscapes. Journal of Grid Computing, 22(2), 2024. https://doi.org/10.1007/s10723-024-09762-6.

[17] Bonadio, Alessio, Chiti, Francesco, Fantacci, Romano, and Vespri, Vincenzo. An integrated framework for blockchain inspired fog communications and com- puting in internet of vehicles. Journal of Ambient Intelligence and Humanized Computing, 11(2), 755–762, 2019. https://doi.org/10.1007/s12652-019-01476-y.

[18] Sharma, Pradip Kumar, and Park, Jong Hyuk. Blockchain-Based Secure MIST Computing network architecture for intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems, 22(8), 5168–5177, 2020. https://doi.org/10.1109/tits.2020.3040989.

[19] Mohammed, Mazin Abed, Lakhan, Abdullah, Abdulkareem, Karrar Hameed, and Ghani, Mohd Khanapi Abd. Multi-objectives reinforcement federated learning blockchain enabled Internet of things and Fog-Cloud infrastructure for trans- port data. Heliyon, 9(11), e21639, 2023. https://doi.org/10.1016/j.heliyon.2023. e21639.

[20] Das, Debashis, Banerjee, Sourav, Chatterjee, Puspita, Biswas, Manju, and Biswas, Utpal. Design and development of an intelligent transportation manage- ment system using blockchain and smart contracts. Cluster Computing, 25(3), 1899–1913, 2022. https://doi.org/10.1007/s10586-022-03536-z.

[21] Ruan, Wenbo, Liu, Jia, Chen, Yuanfang, Islam, Sardar M. N., and Alam, Muhammad. A Double-Layer blockchain based trust management model for secure internet of vehicles. Sensors, 23(10), 4699, 2023. https://doi.org/10.3390/ s23104699.

[22] Rehman, Abdul, Awan, Kamran Ahmad, Din, Ikram Ud, Almogren, Ahmad, and Alabdulkareem, Mohammed. FoGTrust: FoG-Integrated Multi-Leveled trust management mechanism for internet of Things. Technologies, 11(1), 27, 2023. https://doi.org/10.3390/technologies11010027.

[23] Lee, Yunseong, Jeong, Seohyeon, Masood, Arooj, Park, Laihyuk, Dao, Nhu-Ngoc, and Cho, Sungrae. Trustful resource management for service allocation in FOG- Enabled intelligent transportation systems. IEEE Access, 8, 147313–147322, 2020. https://doi.org/10.1109/access.2020.3015550.

[24] Nayak, Sharmistha, Ahmed, Nurzaman, Misra, Sudip, and Choo, Kim-Kwang Raymond. Blockchain-Based programmable FOG architecture for future internet of things applications. GLOBECOM 2022 - 2022 IEEE Global Communications Conference, 1–6, 2020. https://doi.org/10.1109/globecom42002.2020.9347969.

[25] Khan, Abdullah Ayub, Laghari, Asif Ali, Gadekallu, Thippa Reddy, Shaikh, Zaf- far Ahmed, Javed, Abdul Rehman, Rashid, Mamoon, Estrela, Vania V., and Mikhaylov, Alexey. A drone-based data management and optimization using meta- heuristic algorithms and blockchain smart contracts in a secure fog environment. Computers Electrical Engineering, 102, 108234, 2022. https://doi.org/10.1016/ j.compeleceng.2022.108234.

[26] Sharma, Pradip Kumar, and Park, Jong Hyuk. Blockchain-Based Secure MIST Computing network architecture for intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems, 22(8), 5168–5177, 2020. https://doi.org/10.1109/tits.2020.3040989.

[27] Chen, Yu, Qiu, Yilun, Tang, Zhenyu, Long, Shuling, Zhao, Lingfeng, and Tang, Zhong. Exploring the Synergy of Blockchain, IoT, and Edge Computing in Smart Traffic Management across Urban Landscapes. Journal of Grid Computing, 22(2), 2024. https://doi.org/10.1007/s10723-024-09762-6.

[28] Tabassum, Anika, Jeba, Humayra Anjumee, Mahi, Tasnim Kabir, Reza, S.M. Salim, and Hossain, Dilshad Ara. Securely Transfer Information with RSA and Digital Signature by using the concept of Fog Computing and Blockchain. 2021 International Conference on Information and Communication Technology for Sustainable Development, 2021. https://doi.org/10.1109/icict4sd50815.2021. 9396987.

[29] Lakhan, Abdullah, Mohammed, Mazin Abed, Ibrahim, Dheyaa Ahmed, Kadry, Seifedine, and Abdulkareem, Karrar Hameed. ITS based on Deep Graph Convo- lutional Fraud Detection Network Blockchain-Enabled FOG-Cloud. IEEE Trans- actions on Intelligent Transportation Systems, 24(8), 8399–8408, 2022. https://doi.org/10.1109/tits.2022.3147852.

[30] Muthanna, Ammar, Ateya, Abdelhamied A., Khakimov, Abdukodir, Gudkova, Irina, Abuarqoub, Abdelrahman, Samouylov, Konstantin, and Koucheryavy, Andrey. Secure and Reliable IoT Networks Using Fog Computing with Software- Defined Networking and Blockchain. Journal of Sensor and Actuator Networks, 8(1), 15, 2019. https://doi.org/10.3390/jsan8010015.

[31] Li, Jiahao, Li, Dongmei, and Zhang, Xiaomei. A secure Blockchain-Assisted access control scheme for smart healthcare system in fog computing. IEEE Internet of Things Journal, 10(18), 15980–15989, 2023. https://doi.org/10.1109/jiot.2023.3268278.

[32] Das, Debashis, Banerjee, Sourav, Chatterjee, Puspita, Biswas, Manju, and Biswas, Utpal. Design and development of an intelligent transportation manage- ment system using blockchain and smart contracts. Cluster Computing, 25(3), 1899–1913, 2022. https://doi.org/10.1007/s10586-022-03536-z.

[33] Firdaus, Muhammad, Larasati, Harashta Tatimma, and Rhee, Kyung-Hyune. A Blockchain-Assisted distributed edge intelligence for Privacy-Preserving vehicular networks. Computers, Materials Continua, 76(3), 2959–2978, 2023. https://doi. org/10.32604/cmc.2023.039487.

[34] Allouch, Azza, Cheikhrouhou, Omar, Koubˆaa, Anis, Toumi, Khalifa, Khal- gui, Mohamed, and Gia, Tuan Nguyen. UTM-Chain: Blockchain-Based Secure Unmanned Traffic Management for Internet of Drones. Sensors, 21(9), 3049, 2021. https://doi.org/10.3390/s21093049.

[35] Bonadio, Alessio, Chiti, Francesco, Fantacci, Romano, and Vespri, Vincenzo. An integrated framework for blockchain inspired fog communications and com- puting in internet of vehicles. Journal of Ambient Intelligence and Humanized Computing, 11(2), 755–762, 2019. https://doi.org/10.1007/s12652-019-01476-y.

[36] Namane, Sarra, Ahmim, Marwa, Kondoro, Aron, and Dhaou, Imed Ben. Blockchain-Based authentication scheme for collaborative traffic light systems using FOG computing. Electronics, 12(2), 431, 2023. https://doi.org/10.3390/ electronics12020431.

[37] Sharma, Pradip Kumar, Chen, Mu-Yen, and Park, Jong Hyuk. A software defined FOG node based distributed blockchain cloud architecture for IoT. IEEE Access, 6, 115–124, 2017. https://doi.org/10.1109/access.2017.2757955.

[38] Kafhali, Said El, Chahir, Chorouk, Hanini, Mohamed, and Salah, Khaled. Archi- tecture to manage Internet of Things Data using Blockchain and Fog Computing. BDIoT '19: Proceedings of the 4th International Conference on Big Data and Internet of Things, 2019. https://doi.org/10.1145/3372938.3372970.

[39] Rehman, Abdul, Awan, Kamran Ahmad, Din, Ikram Ud, Almogren, Ahmad, and Alabdulkareem, Mohammed. FoGTrust: FoG-Integrated Multi-Leveled trust management mechanism for internet of Things. Technologies, 11(1), 27, 2023. https://doi.org/10.3390/technologies11010027.

[40] Zhang, Jing, Fang, Huixia, Zhong, Hong, Cui, Jie, and He, Debiao. Blockchain- Assisted Privacy-Preserving Traffic Route Management Scheme for FOG-Based vehicular Ad-Hoc networks. IEEE Transactions on Network and Service Manage- ment, 20(3), 2023. https://doi.org/10.1109/TNSM.2023.3238307.

[41] Eremina, Luba, Mamoiko, Anton, and Aohua, Guo. Application of distributed and decentralized technologies in the management of intelligent transport systems Intelligence Robotics, 3(2), 149–161, 2023. https://doi.org/10.20517/ir.2023.09.