Intelligent Automation & Soft Computing

Tech Science Press

DOI: 10.32604/iasc.2023.039761
Article

A Trailblazing Framework of Security Assessment for Traffic Data Management

Abdulaziz Attaallah[1], Khalil al-Sulbi[2], Areej Alasiry[3], Mehrez Marzougui[3], Neha Yadav[4], Syed Anas Ansar[5,*], Pawan Kumar Chaurasia[4] and Alka Agrawal[4]

[1]Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[2]Department of Computer Science, Al-Qunfudah Computer College, Umm Al-Qura University, Mecca, Saudi Arabia
[3]College of Computer Science, King Khalid University, Abha, 61421, Saudi Arabia
[4]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, Uttar Pradesh, India
[5]Department of Computer Applications, Babu Banarasi Das University, Lucknow, 226028, Uttar Pradesh, India
*Corresponding Author: Syed Anas Ansar. Email: syed000anas@gmail.com
Received: 15 February 2023; Accepted: 13 April 2023; Published: 23 June 2023

Abstract: Connected and autonomous vehicles are seeing their dawn at this moment. They provide numerous benefits to vehicle owners, manufacturers, vehicle service providers, insurance companies, etc. These vehicles generate a large amount of data, which makes privacy and security a major challenge to their success. The complicated machine-led mechanics of connected and autonomous vehicles increase the risks of privacy invasion and cyber security violations for their users by making them more susceptible to data exploitation and vulnerable to cyber-attacks than any of their predecessors. This could have a negative impact on how well-liked CAVs are with the general public, give them a poor name at this early stage of their development, put obstacles in the way of their adoption and expanded use, and complicate the economic models for their future operations. On the other hand, congestion is still a bottleneck for traffic management and planning. This research paper presents a blockchain-based framework that protects the privacy of vehicle owners and provides data security by storing vehicular data on the blockchain, which will be used further for congestion detection and mitigation. Numerous devices placed along the road are used to communicate with passing cars and collect their data. The collected data will be compiled periodically to find the average travel time of vehicles and traffic density on a particular road segment. Furthermore, this data will be stored in the memory pool, where other devices will also store their data. After a predetermined amount of time, the memory pool will be mined, and data will be uploaded to the blockchain in the form of blocks that will be used to store traffic statistics. The information is then used in two different ways. First, the blockchain's final block will provide real-time traffic data, triggering an intelligent traffic signal system to reduce congestion. Secondly, the data stored on the blockchain will provide historical, statistical data that can facilitate the analysis of traffic conditions according to past behavior.

Keywords: Connected and autonomous vehicles (CAVs); traffic data management; ethereum blockchain; road side units; smart cities

1 Introduction

Vehicles that are autonomous and connected are linked to other vehicles, the environment, and the internet. These vehicles are susceptible to security and privacy risks due to their high level of connectivity and data exchange. Critical information such as location and vehicle trajectories is included in the data transferred by the vehicle, which can create new privacy concerns. Miller and Valasek demonstrated a sophisticated attack on a Jeep Cherokee by remotely controlling the vehicle's key functions via the infotainment system's wireless interface [1–3]. More vehicles have recently been revealed to be vulnerable to an attack against a remote keyless entry, including the majority of Volkswagen cars after 1995 [2]. The issues listed in Table 1 show that traditional security and privacy approaches employed in smart vehicles are ineffective. At present, blockchain has emerged as the most secure method of data sharing. It is a kind of database that uses distributed ledger.

Although the data has traditionally been stored on a central server, Blockchain technology allows for a decentralized and distributed architecture with backups and redundancy processes [3]. A blockchain is a chain of blocks that are rendered functional by encryption and then linked. Every block of blockchain comprises the previous block hash, timestamp value, and transaction data. By its nature, a blockchain is immutable. Nodes are anonymous members of the system. Blockchain comprises simple components that, when combined, reflect the system's power. Decentralization, transparency, and immutability are three major characteristics of blockchain technology that contribute to its global popularity [4]. Blockchain stores data in blocks over the network in a decentralized manner. Data in a blockchain cannot be stolen or altered, hence can't be changed retrospectively as it stores blocks of distinct data via the blockchain system [5]. Everything that happens on a blockchain is part of the system. Fig. 1 illuminates blockchain properties, including privacy, decentralization, immutability, transparency, time stamping, programmability, security, privacy, and unanimity.

Table 1: Issues in conventional security and privacy approaches employed in smart vehicles

Issues	Explanation
Single point of failure	In modern smart car designs, centralized cloud servers link, identify, authenticate, and authorize all vehicles. Due to the large number of connected cars, this concept is unlikely to be scalable. In addition, cloud servers will continue to be an obstruction; it is a centralized system whose failure is capable of bringing down the entire network [6].
Lack of privacy	The majority of current secure communication architectures either disregard user privacy for instance, sharing complete vehicle data without authorization of its owner, or providing noisy or aggregated data. In certain smart car applications, however, the requester needs to know specific vehicle information in order to deliver individualized assistance [7].

(Continued)

Table 1: Continued

Issues	Explanation
Safety issues	Autonomous driving functions are becoming more popular in smart autos. A malfunction induced by a security breach (such as the installation of malicious software) could result in major accidents, putting the safety of commuters at risk [8].

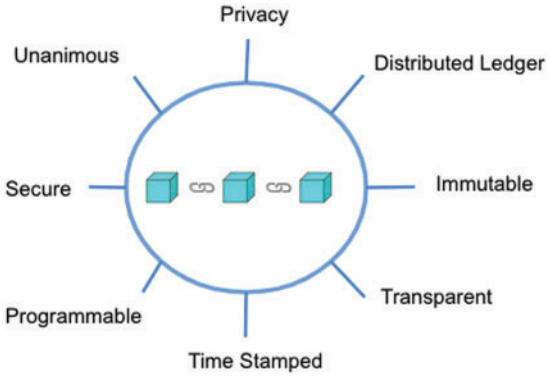

Figure 1: Lineaments of blockchain

Blockchain allows transparency of data as every node in the network has a copy of the chain, and each member of the network can access all the transactions at any moment. The use of cryptographic functions protects the privacy of the members of the network [9]. Transparency has made blockchain unique and popular as no one can be misled, as the whole network is transparent. One of the most important features of the blockchain is immutability, which means that once it is set up, no one can change it. It is defined as a blockchain distributed ledger's ability to remain unchanged and permanent, with no single piece of information in the system being modified [10,11]. This approach has the potential to reclassify the general information verification technique, making it more productive, financially sound, and reliable.

Ethereum is a public, decentralized blockchain network that enables the execution of any decentralized application programming code [11–13]. It is a global platform for exchanging information that cannot be edited or controlled. Hyperledger Fabric is a blockchain system that acts as a basis for distributed ledger solutions built according to a predetermined design that offers high confidentiality, versatility, and adaptability. For secure data transport, these two methods were employed [14–16]. Nevertheless, these blockchain-based frameworks for traffic data management are not extensively adopted or utilized. As per the available research, the Ethereum technique has not yet been implemented in traffic data management systems, and there is limited research on this topic. Fujihara [13] has examined some of the features of blockchain-based traffic information-gathering systems, detailing the system's incentives and the detection of automobile collisions and road conditions. This research examines the information and collection of traffic data in order to determine the road status (congested/normal) and mitigate it [14].

Also, this research paper suggests using blockchain to collect and store information about vehicles so that traffic jams can be found and fixed. The framework uses devices along the road to collect data from passing cars. This data is then put together on a regular basis to find the average travel time and traffic density on a particular road segment. The data is then put into a memory pool and mined every so often to add it to the blockchain as blocks [15–18]. By storing vehicle data on the blockchain, the

proposed framework gives vehicle owners security and privacy for their data. The data can be used in two different ways. First, the real-time traffic data stored on the blockchain can trigger an intelligent traffic signal system to reduce congestion. Second, the historical and statistical data stored on the blockchain can be used to analyze traffic conditions based on past behavior. Overall, the proposed blockchain-based framework has the potential to improve traffic conditions by providing real-time data for intelligent traffic management systems and historical data for analysis and optimization. However, the implementation of such a system would require significant infrastructure investment and widespread adoption to be effective. Sequential research contributions by authors are given below:

- In the first section of the paper, the authors introduce the framework's prerequisites. The software required to create this framework is included. It also covered the advantages of using them. In this part, the structure's two most well-known and significant uses are discussed, including Interplanetary File System and Ethereum (IPFS).
- In the next section, the authors present an elaborated system used for designing the framework. The system consists of physical components such as roadside units, connected and autonomous vehicles, and intelligent traffic signals; it also focuses on how blockchain technology is used for designing the framework.
- Exaggerates the system architecture, modules, and components. The system architecture consists of four layers: the user layer, infrastructure layer, blockchain layer, and application layer. Each layer contains distinct components. Blockchain nodes, traffic watchers, emergency vehicles, and other commuters comprise the user layer. Infrastructure layer components include Wi-Fi, GPS, RFID, and sensors. The blockchain layer comprises nodes and peers, a consensus protocol, encryption, and smart contracts, while the application layer comprises signal triggering, congestion detection, congestion alleviation, and security and privacy. In addition, different modules and workflows are also explained by the authors.
- At the end, the authors evaluated system performance by comparing the framework with the central server-based systems.

1.1 Related Work

The primary goal of Nakamoto's blockchain technology was to develop a decentralized and cryptographically secure currency that helps in financial transactions. The application of blockchain technology has grown over time in a variety of industries, including traffic data management systems. Several researchers have investigated this topic to determine whether the concept of using blockchain for traffic data security and privacy is feasible [19–21]. In addition, researchers identify the benefits, risks, concerns, and difficulties associated with employing this technology. A seven-layer conceptual model aimed at the intelligent transport system (ITS) is presented to address critical research concerns in the ITS [20,21]. A unique decentralized and secure design architecture for connected car data security is suggested using Hyperledger fabric. A framework for the application of blockchain technology to electronic health records in the healthcare sector is offered. This architecture's main goal is to use blockchain to store electronic health records. Secure data storage is the second goal. Additionally, by maintaining documents off-chain, this approach overcomes the scalability issue that blockchain technology in general faces [22,23]. In contrast to proof-of-work or proof-of-authority methods, the concept of proof-of-event consensus is relevant to vehicle networks. When passing vehicles receive an event notification, they will check the correctness of the traffic data provided by roadside equipment. In order to convey alarm messages at the appropriate times and locations, a two-phase transaction is implemented on the blockchain [24,25]. The notion of a tradable mobility permit (TMP) to reduce traffic congestion is devised and statistically tested [19], together with the principles of cryptocurrencies, Blockchain, and Ethereum. Multiple components make up

a permissioned blockchain system that is used to manage vehicle-related data. Utilize Vehicular Public Key Infrastructure (VPKI) to provide sponsorship creation and anonymity for the intended blockchain. Create a disjointed register next to store data related to a given car, such as maintenance details and histories, auto diagnosis reports, etc.

The forensic system outlined above offers post-accident investigation that is privacy-aware, traceable, and trust-less with little storage and processing overhead [26–28]. A synopsis of bitcoin, Ethereum, and blockchain technology was provided [29]. Bigdata analytics is used to enhance the design, operations, and technological aspects involved in traffic control by managing the large amount of data generated by Vehicular Ad hoc Networks (VANET) [30,31]. A novel metaheuristic is designed with an adaptive neuro-fuzzy inference system for decision-making named MANFIS-DM technique on autonomous UAV systems [32–34]. A thorough study of the literature is provided in Tables 2 and 3, with an emphasis on potential assaults on connected and autonomous vehicles and their defenses.

Table 2: List of possible attacks on CAVs

Related work	Details	Solution
Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications [24]	Tracking a user's location, even in an anonymous manner, allows for the surveillance of personal activities for purposes like shopping. It may be possible to detect competitors and behavioral trends, allowing service providers to enhance their offerings further. A fast-food restaurant, for instance, would definitely be interested in knowing the location of its clients before and after their visit.	Data should be adequately anonymized, thoroughly encrypted, and securely protected to prevent exposure in order to guarantee individual privacy.
Can blockchain Strengthen the internet of things? [25,26]	In cloud-based systems, the cloud becomes a single point of failure, as there are many factors such as Denial of service, which may deny the accessibility of data stored on cloud. Which can crash the whole system.	In contrast to centralized systems where information is stored centrally, blockchains are decentralized systems where each node in the network has a copy of the blockchain.
Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations [26]	To affect network performance through DoS attacks, eavesdropping, or changing gathered data, just one malicious node is required.	When insecurity from a node is detected, the system can halt its updates and distribute computational resources among different nodes.

(Continued)

Table 2: Continued

Related work	Details	Solution
Survey on cyber security of CAV [27]	Eavesdropping and Information Disclosure. While using connected automobiles the opponent can eavesdrop on the vehicle's condition and the communication messages exchanged. These messages may include the destination, and traveling trajectory.	Encrypt the messages using cryptography so that only authorized people or devices can decrypt the content.
Survey on cyber security of CAV [27]	Spoofing attacks include the fabrication of identities or data. This occurs when an unauthorized attacker poses as a legitimate user.	Before storing the information in the data center, it must be validated.
Denial of service (DOS) attack and its possible solutions in VANET [28]	Refusal to Provide (DoS). Denial of service will stop the access of the target server by exploiting vulnerabilities in the system or protocol to transmit massive amounts of data or requests to disrupt the network of the receivers. Denial of service will delay and degrade the recipients' ability to respond.	Decentralization of data.

Table 3: VANET system compared with the CAVs system

S. No.	Topics	Explanation	Reference
1.	Lattice-based lightweight quantum resistant scheme in 5G-enabled vehicular networks	Connected vehicles and vehicular networks rely on the exchange of sensitive data, such as location information, to enable communication and collaboration between vehicles and infrastructure. However, the security and privacy of this data can be compromised by malicious actors, that is why cryptography is used to protect communication and ensure data integrity. In this study, the lattice-based cryptography scheme is used to achieve quantum-resistant security in 5G-enabled vehicular networks. Unlike traditional public-key cryptography, which relies on the difficulty of certain mathematical problems to secure communication, lattice-based cryptography is based on the computational hardness of finding the shortest vector in a high-dimensional lattice. This makes it resistant to attacks from both classical and quantum computers.	[29]

(Continued)

Table 3: Continued

S. No.	Topics	Explanation	Reference
2.	Chebyshev polynomial-based fog computing scheme supporting pseudonym revocation for 5G-enabled vehicular networks	Fog computing is a paradigm that allows for the processing of data closer to the source of the data, which can help to reduce latency and improve security. By using fog computing in 5G-enabled vehicular networks, it is possible to reduce the risk of insider attacks and improve the security of the information exchanged between automobiles. The use of Chebyshev polynomials in the fog computing strategy for 5G-enabled automotive networks can help to ensure the revocation of pseudonyms. Chebyshev polynomials are a type of mathematical function that can be used to generate a unique identifier for each vehicle in the network. This identifier can then be used to authenticate messages and verify the signature, which helps to improve the security of the system.	[30]
3.	COVID-19 vehicle based an efficient mutual authentication scheme for 5G-enabled vehicular fog computing;	The paper proposes a mutual authentication scheme for 5G-enabled vehicular fog computing to enable non-contact autonomous healthcare monitoring. The scheme utilizes two different flags, $SF = 0$ and $SF = 1$, to denote normal and COVID-19 vehicles, respectively. The proposed scheme aims to satisfy privacy and security requirements while providing COVID-19 and healthcare solutions. Overall, the proposed scheme aims to improve infection tracking and healthcare monitoring for high-mobility transportation systems by utilizing 5G-enabled vehicular fog computing. However, the effectiveness of the proposed scheme needs to be evaluated further, and practical implementation issues need to be considered.	[30]
4.	MSR-DoS: Modular square root-based scheme to resist denial of service (DoS) attacks in 5G-enabled Vehicular Networks	This paper proposes a new security scheme called MSR-DoS for 5G-enabled vehicular networks. The proposed scheme aims to prevent denial of service (DoS) attacks while satisfying privacy requirements such as authenticity, message integrity, pseudonym privacy-preserving, unlinkability, traceability, and revocability. The paper claims that the security of the proposed scheme is proved using Burrows-Abadi-Needham (BAN) logic and that the scheme has lower communication and computational costs compared to existing schemes.	[27]

(Continued)

Table 3: Continued

S. No.	Topics	Explanation	Reference
5.	Provably secure with efficient data sharing scheme for fifth-generation (5G)-enabled vehicular networks without road-side unit (RSU)	This paper proposes a new data-sharing scheme for 5G-enabled vehicular networks that is both secure and efficient, without requiring an expensive road-side unit (RSU) for authentication. The proposed scheme involves six phases, including TA initialization, pseudonym-identity generation, key generation, message signing, single verification, and batch signatures verification. The scheme allows vehicles to verify multiple signatures simultaneously, which helps to ensure privacy and security while also withstanding various security attacks on the network. The paper also claims that the proposed scheme is more cost-effective than existing schemes in terms of both communication and computation.	[28]

1.2 Observation

The literature review above presents the work where blockchain is used in vehicular networks or transportation and along with a listing of all possible attacks on CAV. None of the available research used a blockchain-based system that detects and mitigates congestion. The framework proposed in this paper uses blockchain technology to store traffic data to enhance the data's security, privacy, immutability, transparency, and traceability. Furthermore, the stored data is used to detect and mitigate congestion making the proposed framework different from the relevant literature found in this domain.

1.3 Paper Structure

The remaining paper is structured as follows. Section 2 introduces the prerequisites of the framework. The system proposal is presented in Section 3, while Section 4 exaggerates system architecture, modules, and components. Section 5 offers an evaluation of the system's performance, and Section 6 brings this study to a close with recommendations for the next enhancements.

2 Preliminaries

In this section, the proposed framework's prerequisites are formally explained. It includes the software needed to build this framework. It also discussed the benefits of utilizing them. The two most well-known and important applications of the structure are described in this section: Ethereum and Interplanetary File System (IPFS).

2.1 Ethereum

It is a decentralized blockchain that builds on the blockchain technology concept pioneered by Bitcoin [35–38]. Ethereum was introduced in 2015 as an open-source framework for trustless smart contracts with programmable blockchain capabilities. This technique also employs peer-to-peer networking to spread. This platform utilizes Ethers, its native coin [39–41]. This coin can be used to transfer funds between accounts on the Ethereum blockchain [42]. Solidity, a programming language provided by Ethereum, enables developers to personalize their blockchain. It was intended to facilitate smart contracts, the core feature of Ethereum.

2.2 Information Transaction

A transaction is an interaction between an external entity and the Ethereum network. It allows external users to edit the status of a record or piece of information on the Ethereum blockchain network. Table 4 shows the components of an Ethereum transaction [25–28,43–46]:

Table 4: Components of an Ethereum transaction

Ethereum components	Explanation
From	The sender of the message.
To	The recipient of a communication.
Value	Amount of money transmitted from sender to receiver (Wei).
Gas	The fees needed to complete the transaction is called gas. Every transaction includes gasoline price and limit.
Gas price	The cost of gas is paid by the transaction's sender.
Gas limit	The maximum amount of gas used for a transaction.

2.3 Smart Contracts

These make up the blockchain network's programming section; activities on the blockchain are carried out using the program's codes. When users submit transactions, this code is put into effect [3–6,38]. They work on the blockchain, making them impervious to change. Using the Solidity programming language, smart contracts may be used to write any form of action on the blockchain. After coding necessary functions, compilation takes place using EVM bytecode, detailed in the following section. After compilation, these functions were executed and deployed on the Ethereum blockchain [4,47,48]. JavaScript and Python are encased in Ethereum's Solidity programming language for writing code for smart contracts.

2.4 Ethereum Virtual Machine (EVM)

The Ethereum platform's programmable blockchain is the most essential feature. It allows users to create their Ethereum-based applications. Distributed Apps are applications developed using this platform (DApps). A DApp platform consists of a collection of protocols that have been bundled together. These DApps have smart contracts containing user-defined code to accomplish a particular application purpose. Execution and deployment of this code take place by EVM [5,6,49–51]. As a result, EVM is used to operate smart contract-based applications.

2.5 Interplanetary File System

The interplanetary file system is a distributed file system for storing data. It protects data from tampering as it uses encrypted identifiers to protect information. If data on IPFS is changed, then the identifier must be changed, and in IPFS, every data file has a unique hash value [8,9,52–55]. The IPFS protocol is suitable for storing vital and sensitive data due to its safe storage strategy. The decentralized application may save the created cryptographic hash, thereby decreasing the blockchain's computing activities. The IPFS protocol employs a peer-to-peer (P2P) network consisting of an IPFS object containing data and links. The link is an array, whereas the data is unstructured binary data [10,11,56–59].

3 System Proposal

An uninterrupted part of the road network is divided by intersections, as depicted in Fig. 2. Right to left or left to right are the two main directions in that cars travel down the road section. Although they periodically stop on a stretch of road, the vast majority of vehicles continue, and none may suddenly vanish. A sufficient number of roadside units (RSU) are installed along this road segment by anonymous neighboring residents, similar to how Wi-Fi routers are currently installed [60–62]. In general, the RSU is held by several citizens who are not necessarily dependable. When an RSU gets vehicle IDs via Wi-Fi scanning, it stores them as traffic data.

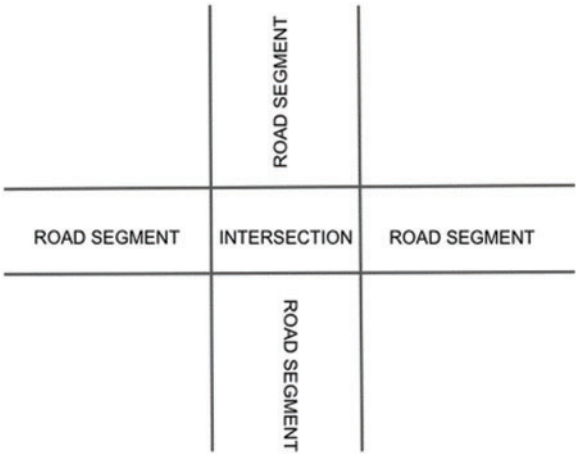

Figure 2: Visualization of the road network

3.1 Physical Components Used

The various physical components that make up the proposed structure are depicted in Fig. 3. Physical components include roadside units, autonomous and connected vehicles, and intelligent traffic signals. Below is a detailed explanation of each component. These vehicles are blockchain network nodes, so they are connected with each other. The roadside units also form the blockchain network nodes, so they are also connected to vehicles.

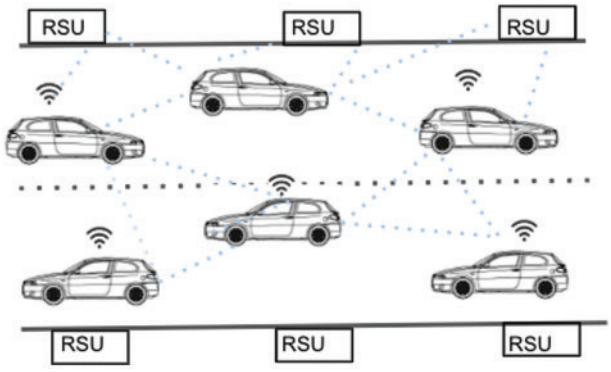

Figure 3: Car and road side units

3.1.1 Road Side Devices (RSD)

Road Side Devices are part of the roadside infrastructure. They facilitate Vehicle-to-infrastructure (V2I) communications [63,64]. They interact with the OBU (onboard units). This work uses RSDs to validate the data acquired by automobiles acting as Blockchain nodes.

3.1.2 Connected Vehicles

Vehicles that can communicate both inside and outside are said to be connected. These vehicles are equipped with communication devices and onboard sensors that enable connectivity with external devices, networks, applications, and services [65,66]. These cars support Vehicle-with-its sensors (VwS), Vehicle-with-vehicle (VwV), and Vehicle-with-environment (VwE). In this research study, linked vehicles collect information about nearby vehicles, which is subsequently confirmed by the RSU and finally stored on the blockchain [67,68].

3.1.3 Intelligent Traffic Signals

In this article, the activation of the traffic signal will vary based on the Blockchain data. The congestion level will be inferred from the data on a block formed in real time, and the traffic signal on the Road Segment will be activated based on the congestion level.

3.2 How to Use Blockchain

Previously proposed Proof-of-work (PoW) by Back [11,69,70] in Hashcash is employed in the Bitcoin blockchain. PoW is a consensus mechanism for demonstrating to users that a specific amount of computational power is used for a specific period. The Bitcoin Proof-of-work function is described by Eq. (1).

Function of difficulty (fxnD):

$$\text{SHA } 2562\,(\text{ch} + \text{n}) < 2256/\text{D } \varepsilon \ \{\text{T},\ \text{F}\} \tag{1}$$

where D, ch, n, T, and F represent difficulty, challenge, nonce, true and false, respectively. The hash function is Double SHA256, and the PoW method returns True if the returned hash value is lower than the target number 2256/D. It is computationally challenging but possible to identify n such that FxnD (ch, n) = T, for parameters D and ch that are fixed. In Bitcoin, full node users compete in Proof-of-Work to select golden nonce n, and the winner is granted the ability to mine a new block and coin base. In the proposed system, roadside units (RSU) will perform PoW to generate a memory block, including Vehicle Identification number and road status (regular/congested). Proof-of-Work method in a roadside unit is outlined in Algorithm 1. Each roadside unit automatically connects the newly formed block to the blockchain after ensuring that PoW is conducted correctly. Below is described the proposed block and block header structure. This approach allows for the management of the blockchain for each segment of the road. The system's blockchains fork from the genesis block to form RS genesis.

Algorithm 1: Proof-of-Work (PoW) in road side units

1: nonce n = 0
2: while FxnD (ch, n) = = F else do
3: n = n + 1
4: close while loop

3.3 Ethereum Block Structure

As shown in Fig. 4, the Ethereum block structure includes the block's size, information on the traffic, a unique vehicle ID, and the block header. Additionally, Parts of the block header are also depicted. The block header contains the previous block hash function, the root of the hash found using the Merkle tree, the date of the block, the difficulty level, the nonce, the gas limit and amount used, and any other data [71–73].

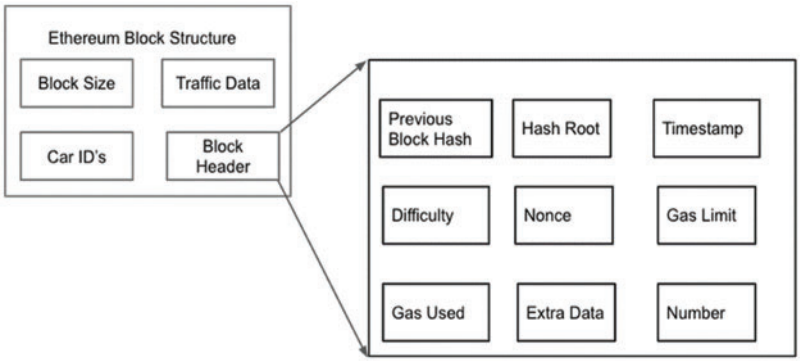

Figure 4: Structure of block and its header

3.4 Layered Architecture

The suggested framework's layered architecture is depicted in Fig. 5. It consists of four layers, namely the user layer, infrastructure layer, blockchain layer, and application layer. Each layer contains distinct components. Blockchain Nodes, traffic watchers, emergency vehicles, and other commuters comprise the User Layer. Infrastructure layer components include Wi-Fi, GPS, RFID, and sensors. The Blockchain layer comprises nodes/peers, consensus protocol, encryption, and smart contracts, while the application layer comprises signal triggering, congestion detection, congestion alleviation, and security & privacy. A brief explanation of each component is discussed in Table 5.

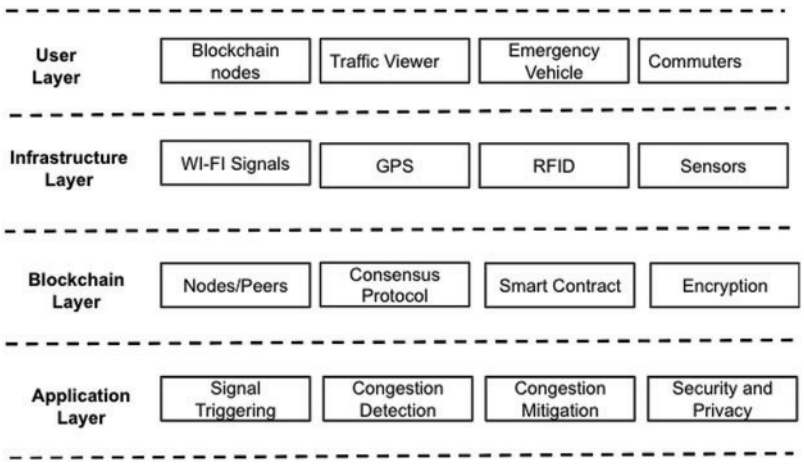

Figure 5: Four-layer architecture of the proposed framework

Table 5: Brief explanation of each component of layered architecture

Layers	Components	Explanation
User layer	Blockchain nodes	The vehicles that are willing to become part of the blockchain will sign in as blockchain nodes and join the blockchain network.
	Emergency vehicles	The vehicles such as ambulances, police cars, and convoys will sign in as Emergency nodes.
	Traffic viewer	Some vehicles will log in just to get the status of traffic on a particular route.
	Commuters	It will include all the commuters on the road.
	On-road sensors	The sensors on the road will detect the vehicular speed, trajectory, and also size of the vehicle.
Infrastructure layer	Wi-Fi	Wi-Fi will be used to get the vehicle data.
	GPS	The onboard GPS will help in locating the vehicle and finding its route.
	RFID	RFID will also help to get vehicular data.
	Nodes/Peers	Peers are the vehicles that are part of the blockchain network.
Blockchain layer	Consensus protocol	The consent protocol helps the nodes in the network to verify the transaction.
	Encryption	Public-key cryptography is hardened to encode the data.
	Smart contract	Intelligent contracts are the programmable part of blockchain.
	Congestion detection	The road status will be asserted in this layer
	Data security	Storing traffic data on the blockchain will increase its security.
Application layer	Signal triggering	Adaptive signals will get triggered as per the data on blockchain.
	Congestion mitigation	Triggering of signals according to blockchain data will mitigate the congestion.

4 System Design

System design is the most fundamental and essential aspect of any architecture as it is used to develop the system from its theoretical basis. This section includes the system's modules, architecture, and other components. As stated previously, the purpose of this proposed framework is to create a decentralized, tamper-resistant, secure, and private blockchain-based traffic data management system.

4.1 Real-World Representation of the Framework

The real-world representation of the proposed architecture consisting of connected and autonomous vehicles is shown in Fig. 6. These vehicles will collect each other's data based on proximity. Roadside units will also collect the data of all the vehicles. These data/transactions will be stored in the data pool. Part of the data from the pool will form a block. In the end, the block thus formed was added to the blockchain. According to the data on the last block (Current Road Condition), the intelligent traffic signal will get triggered to remove congestion if it exists.

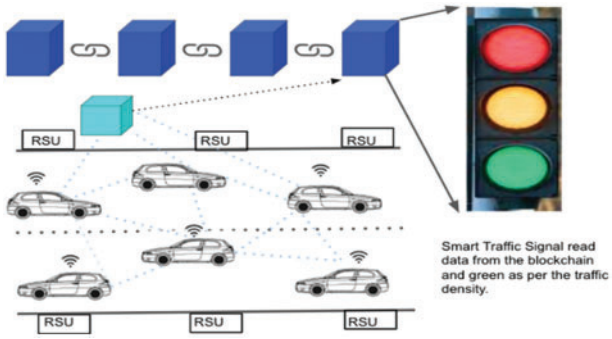

Figure 6: Real-world representation of the proposed framework

Fig. 7 demonstrates the system design of the proposed framework, which comprises three levels, namely the user layer, the blockchain layer, and the system implementation that are discussed. Further, the suggested framework or system contains three components or modules, depicted in Figs. 8–10, respectively. When these components are merged, our system will continue to function. These modules have additional notions that must be grasped, as described below:

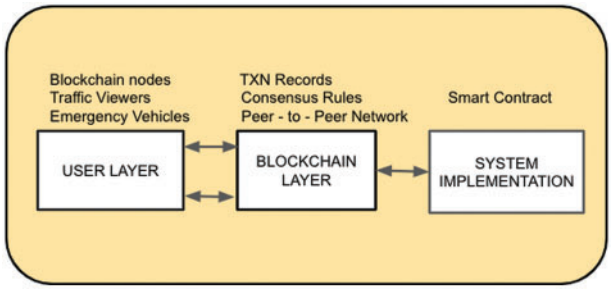

Figure 7: System design of the proposed framework

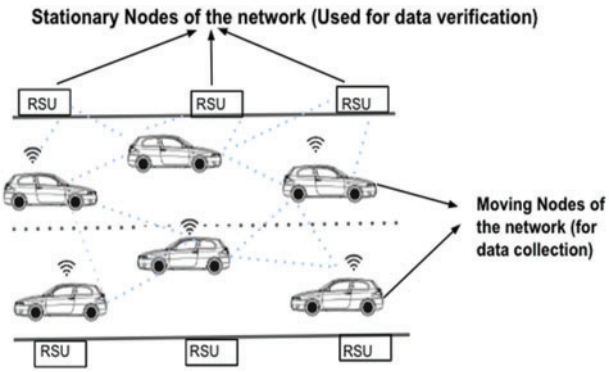

Figure 8: Module 1:-collection of data through road-side devices

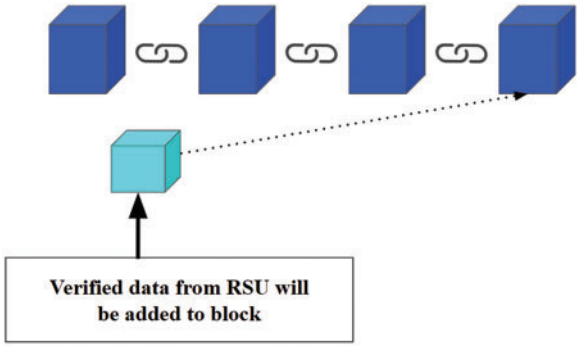

Figure 9: Module 2-verified data from roadside units

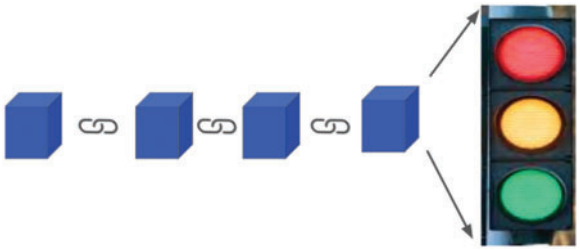

Figure 10: Module 3-traffic signal triggering based on blockchain data

4.1.1 User Layer

A structure customer is someone that uses the structure and its assets effectively. On the system, a user is recognisable by multiple roles and qualities. Potential users of this system include vehicle owners who wish to exchange information (blockchain nodes), single-traffic viewers, and emergency vehicles. The primary responsibility of these users would be to interact with the system and do simple tasks such as creating, reading, updating, and deleting traffic data. To access the system's capabilities, users would employ a prospect that we indicate to be the same as a DApp prospect in technical terms while it incorporates the DApp's GUI (Graphical User Interface), which is our suggested system framework. The GUI contains every function to which a particular user has access. Depending on their employment, the user could utilize this GUI to interface with the system's other layer, the blockchain layer. The information of the person registered as a blockchain node will be shared with the environment and other vehicles. This part will collect and provide data from neighboring vehicles to the data pool. Blockchain nodes can only be generated by interconnected vehicles. As emergency vehicles, anybody can register ambulances, police cars, and essential convoys. One who registers as a traffic viewer will be able to gauge the status (congested/normal) of a particular route.

Roadside Units and Connected Vehicles are shown in Fig. 8. Roadside Devices and Connected automobiles are the network's stationary and mobile nodes, respectively. The data of connected automobiles are exchanged (i.e., vehicular data). Data gathered by connected vehicles will be verified by roadside devices. The perception devices placed on the road also gather data about vehicles.

4.1.2 Blockchain Layer

The blockchain layer provides the code or method enabling the user to communicate with the blockchain-based DApp. There are three elements contained within this layer. They are listed below:

- Cryptocurrency Assets: The transactions on the Ethereum blockchain are known as cryptocurrency assets. These transactions can modify the data stored on the blockchain. These transactions are referred to as assets since they involve data that one user transfers to another [5].
- Governance Rules: Blockchain technology adheres to particular consensus standards to execute and calculate transactions. Some consensus procedures are essential to maintain the blockchain secure and tamper-proof. Proof of Work (PoW) is employed on the Ethereum blockchain to guarantee that the blockchain's governance is sustained trustfully, with the agreement of all nodes on the blockchain network [6].
- Network: The Ethereum blockchain utilizes the peer-to-peer network. Every point in this system is connected to its peers. There is no central node in the network that controls all network operations. The purpose was to develop a decentralized platform, not a central one; hence this system was chosen. Therefore, utilizing a system along with equivalent positions and rights used for the whole connected nodes was the best option for this technology [7].
- The data collected at the pool will form a block at this layer. As Fig. 9 shows, the block thus formed is then added to the blockchain, so the Verified data from Roadside Units will be added to "BLOCK," and then the block gets added to the blockchain.

4.1.3 System Implementation

As described in earlier sections, Ethereum and its dependencies were used to create the system. This section examines system implementation in further depth to provide insight into the system's many functions.

- Smart Contract: As was already mentioned, smart contracts are a crucial part of decentralized applications (DApps) and are used to carry out essential functions [8]. They are basically blockchain-based codes that execute when particular conditions are met. Usually, they are employed to automate the execution of a contract so that all parties can be informed of the result instantly, without the need for an intermediary or any time lost. This framework will be governed by a contract with vehicle records.
- Vehicle Records: Vehicle records will have vehicular data such as vehicle ID, location, speed, and time stamp. It will also have code to trigger intelligent traffic signals according to the data on the last block of the blockchain. The adaptive traffic signal reads data from the blockchain and changes light (green/red) according to real-time traffic density, as shown in Fig. 10.

4.2 Flowchart

The flowchart shown in Fig. 11 presents the workflow of the proposed framework. The vehicle owner who wants to be part of the blockchain network will login to the Dapp and become the blockchain node. The vehicular data will be collected by connected and autonomous vehicles and roadside units. When the information collected by roadside devices and connected automobiles matches, it gets stored in the memory pool; data extracted from the memory pool then forms a blockchain block. As per the data on the last block of the blockchain, the intelligent signal system gets triggered to control congestion.

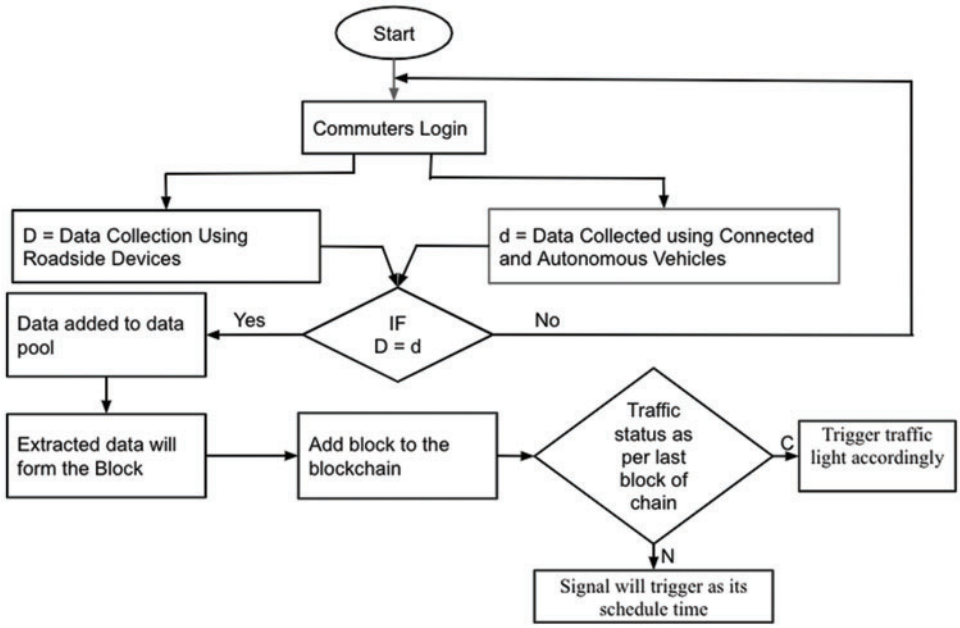

Figure 11: Workflow of the proposed framework

5 Performance Evaluation

Table 6 below shows the parameters for which the proposed framework will be expected to perform more efficiently compared to the centralized systems: reliability, security, privacy, authenticity, immutability, transparency and traceability. Still, some parameters need to be worked upon to improve the proposed framework: scalability, efficiency, and speed of action. Parallel research is going on to improve these parameters in the blockchain paradigm.

Table 6: Comparison of the central server-based traffic system and blockchain-based traffic system

S. No	Parameters	Central server-based traffic system	Blockchain based solution
1.	Reliability	×	✓
2.	Security	×	✓
3.	Authenticity	×	✓
4.	Immutability	×	✓
5.	Efficiency	✓	×
6.	Scalability	✓	×
7.	Speed of action	✓	×
8.	Transparency	×	✓
9.	Privacy	×	✓
10.	Encryption	×	✓
11.	Traceability	×	✓

Notes: ×: Shows reduced the extent of parameters as compared to other & ✓: shows enhanced the capacity of parameters as compared to other.

Table 6 compares two traffic systems, i.e., central server-based and blockchain-based. It shows that storage of traffic data on central servers will lead to data hacking and tampering and the risk of single-point failure, making it less reliable. On the other hand, the storage of data on blockchain makes it immutable, secure, reliable, and transparent due to the inbuilt security features of blockchain technology. Efficiency and scalability factors still need to be improved for blockchain-based systems for implementation in real-time scenarios. The blockchain system is still incompatible with the existing system based on old technologies, making it less interoperable. Fig. 12 shows the graphical representation of the extent of parameters of central server-based and block-based systems.

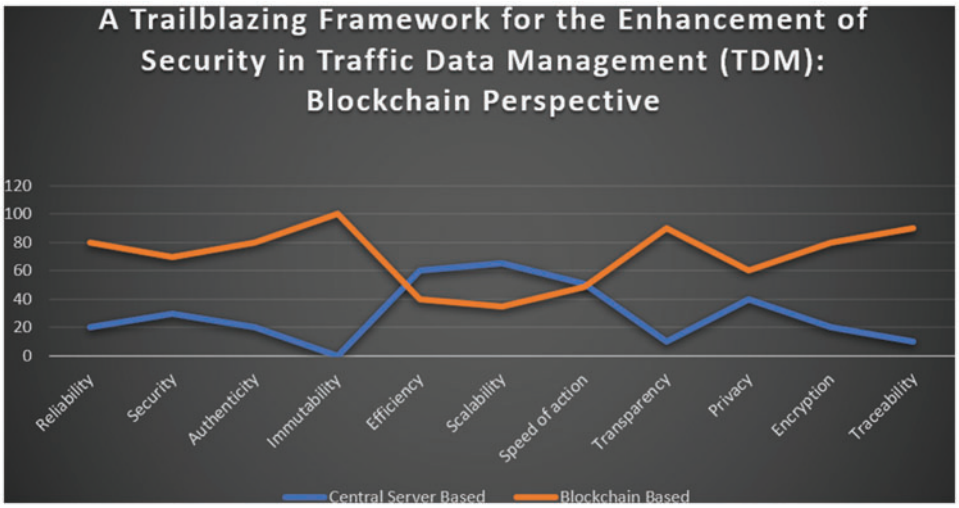

Figure 12: Comparison of the central server-based traffic system and blockchain-based traffic system

6 Conclusion

The automobile sector is going through a significant digital change. By 2030, automobiles will have more connectivity and autonomy. These cars will share a vast amount of data on a daily basis, which will require confidentiality, openness, and safety. Use of blockchain to store the data created by these vehicles will safeguard the data from tampering, spoofing, and other threats, as well as improve its traceability. It also assists commuters in determining the condition of the road. Accidents and traffic congestion will be identified immediately. This article proposes a blockchain-based infrastructure for securing traffic data, detecting congestion, and mitigating its effects. Security, privacy, and reliability of traffic data are the focal points of this research. The storage of traffic data on blockchain will facilitate future data tracing for accident and traffic case studies. The data will be unchangeable. Blockchain eliminates the chance of single-point failure by storing data in a decentralized fashion. As the number of automobiles on the road continues to rise, the appropriate application of the proposed framework can result in a traffic system that is efficient, intelligent, and transparent, making life easier. Additionally, it facilitates commuters' access to road traffic. The activation of an adaptive traffic signal system based on blockchain data would alleviate congestion on the road. This framework brings a centralized approach to a decentralized form, which reduces the risk of a single point of failure. It increases the security, reliability, and authenticity of data stored on it. Additionally, it makes the data immutable and also enhances privacy.

The corporate sector, where technology companies and automakers are at the forefront of the development of actual vehicle networks, and the public sector, which can use this design to advance the development of smart city roads, can both benefit from this work by lowering implementation difficulties and showcasing how the primary user concerns are addressed. Using smart contracts and storing traffic data on the blockchain will simplify driving in a number of ways, including the payment of auto insurance, vehicle maintenance, and toll costs. Working with various stakeholders both physically and online is facilitated by the interactions between the vehicle and the infrastructure. For such practical applications, integrity and dependability are necessary. The architecture on which the application is built primarily incorporates the security and privacy features of the underlying blockchain technology. The size issue was not included in the scope of this suggested framework because it could be the focus of a different research project. This framework may be expanded to include green lanes for ambulances, police cars, and other emergency vehicles. The roadside devices of this system, which must identify autos and collect data from them, require a mechanical component that can manage this type of communication swiftly and flawlessly under real-world network conditions.

Acknowledgement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number RGP2/249/44.

Funding Statement: This Project was funded by the Deanship of Scientific Research at King Khalid University, Kingdom of Saudi Arabia for large group Research Project under grant number: RGP2/249/44.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] R. Kumar, A. Baz, H. Alhakami, W. Alhakami, A. Agrawal *et al.,* "A hybrid fuzzy rule-based multi-criteria framework for sustainable-security assessment of web application," *Ain Shams Engineering Journal*, vol. 12, no. 2, pp. 2227–2240, 2021.

[2] Ş. Okul, M. A. Aydin and F. Keleş, "Security problems and attacks on smart cars," in *Int. Telecommunications Conf.*, Singapore, Springer, vol. 4, no. 6, pp. 203–213, 2019.

[3] F. Casino, T. Dasaklis and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, no. 2, pp. 55–81, 2019.

[4] R. A. Latif, K. Hussain, N. Jhanjhi, A. Nayyar and O. Rizwan, "Retracted article: A remix ide: Smart contract-based framework for the healthcare sector by using blockchain technology," *Multimedia Tools and Applications*, vol. 81, no. 19, pp. 26609–26632, 2020.

[5] W. Serrano, "Verification and validation for data marketplaces via a blockchain and smart contracts," *Blockchain: Research and Applications*, vol. 1, no. 5, pp. 100–112, 2022.

[6] A. Dorri, M. Steger, S. Kanhere and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.

[7] A. Haque, B. Bhushan and G. Dhiman, "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends," *Expert Systems*, vol. 39, no. 5, pp. 145–157, 2021.

[8] M. Ryan, "The future of transportation: Ethical, legal, social and economic impacts of self-driving vehicles in the year 2025," *Science and Engineering Ethics*, vol. 26, no. 3, pp. 1185–1208, 2019.

[9] S. Halder, A. Ghosal and M. Conti, "Secure over-the-air software updates in connected vehicles: A survey," *Computer Networks*, vol. 178, no. 4, pp. 1043–107373, 2020.

[10] J. Wang, W. Chen, L. Wang, R. S. Sherratt, O. Alfarraj *et al.,* "Data secure storage mechanism of sensor networks based on blockchain," *Computers, Materials and Continua*, vol. 65, no. 3, pp. 2365–2384, 2020.
[11] S. A. Ansar, S. Arya, S. Aggrawal, J. Yadav and C. Prabhash, "Bitcoin-blockchain technology: Security perspective," *3rd Int. Conf. on Intelligent Engineering and Management (ICIEM)*, London, United Kingdom, pp. 291–296, 2022.
[12] Z. Xu, W. Liang, K. C. Li, J. Xu and H. Jin, "A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles," *Journal of Parallel and Distributed Computing*, vol. 149, no. 6, pp. 29–39, 2021.
[13] A. Fujihara, "Proposing a system for collaborative traffic information gathering and sharing incentivized by blockchain technology," in *Advances in Intelligent Networking and Collaborative Systems, Lecture Notes on Data Engineering and Communications Technologies*, vol. 23, Barcelona, Spain: Springer, pp. 457–469, 2019.
[14] J. Wang, B. Wei, J. Zhang, X. Yu and P. K. Sharma, "An optimized transaction verification method for trustworthy blockchain-enabled IIOT," *Ad Hoc Networks*, vol. 119, no. 45, pp. 1478–1489, 2021.
[15] S. Zhang and J. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Express*, vol. 6, no. 2, pp. 93–97, 2020.
[16] S. A. Ansar, A. Agrawal and R. A. Khan, "A phase-wise review of software security metrics," in *Proc. of the Second Int. Conf. on Inventive Communication and Computational Technologies*, Coimbatore, India, pp. 219–223, 2018.
[17] W. Li, M. Nejad and R. Zhang, "A blockchain-based architecture for traffic signal control systems," in *Proc. of the IEEE Int. Congress on the Internet of Things*, Newark, NJ, USA, pp. 33–38, 2019.
[18] Y. Yang, L. Chou, C. Tseng, F. Tseng and C. Liu, "Blockchain-based traffic event validation and trust verification for VANETs," *IEEE Access*, vol. 7, no. 8, pp. 30868–30877, 2019.
[19] S. A. Bagloee, M. Tavana, G. Withers, M. Patriksson and M. Asadi, "Tradable mobility permit with bitcoin and Ethereum–A blockchain application in transportation," *Internet of Things*, vol. 8, no. 8, pp. 100103, 2019.
[20] M. Cebe, E. Erdin, K. Akkaya, H. Aksu and S. Selcuk, "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 102–108, 2018.
[21] P. Dhulavvagol, V. Bhajantri and S. Totad, "Blockchain ethereum clients performance analysis considering e-voting application," in *Proc. of the Int. Conf. on Computing and Network Communications*, Hubballi, India, pp. 7–11, 2020.
[22] N. O. Aljehane and R. F. Mansour, "Big data analytics with oppositional moth flame optimization based vehicular routing protocol for future smart cities," *Expert Systems*, vol. 39, no. 5, pp. 12718–12723, 2021.
[23] M. Ragab, E. B. Ashary, W. H. Aljedaibi, I. R. Alzahrani, A. Kumar *et al.,* "A novel metaheuristics with adaptive neuro-fuzzy inference system for decision making on autonomous unmanned aerial vehicle systems," *ISA Transactions*, vol. 132, no. 8, pp. 16–23, 2023.
[24] Q. Wu, J. D. Ferrer and U. G. Nicolas, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 559–573, 2010.
[25] N. Kshetri, "Can blockchain strengthen the internet of things," *IT Professional*, vol. 19, no. 4, pp. 68–72, 2017.
[26] Q. Xu, P. Ren, H. Song and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, no. 1, pp. 2840–2853, 2016.
[27] A. K. Singh and R. Kumar, "Indian vision-2047 for cyber defence security: Needs and importance," *Indian Defence Review*, 2023. [Online]. Available at: http://www.indiandefencereview.com/news/indian-vision-2047-for-cyber-defence-security-needs-and-importance/
[28] Q. He, V. Manickam and R. Kumar, "Role of secure internet of things applications in Indian defence," *South Asia Defence and Strategic Review*, vol. 16, no. 4, pp. 18–22, 2022.

[29] Z. G. Almekhlafi, M. A. Alshareeda, S. Manickam, B. A. Mohammed and A. Qtaish, "Lattice-based lightweight quantum resistant scheme in 5G-enabled vehicular networks," *Mathematics*, vol. 11, no. 2, pp. 1–18, 2023.
[30] Z. G. Almekhlafi, M. A. Alshareeda, S. Manickam, B. A. Mohammed, A. Qtaish *et al.,* "Chebyshev polynomial-based fog computing scheme supporting pseudonym revocation for 5G-enabled vehicular networks," *Electronics*, vol. 12, no. 4, pp. 1–18, 2023.
[31] M. A. Alshareeda and S. Manickam, "Covid-19 vehicle based on an efficient mutual authentication scheme for 5G-enabled vehicular fog computing," *International Journal of Environmental Research and Public Health*, vol. 19, no. 23, pp. 1–18, 2022.
[32] Z. G. Almekhlafi, M. A. Alshareeda, S. Manickam, B. A. Mohammed, A. Qtaish *et al.,* "Provably secure with efficient data sharing scheme for fifth-generation (5G)-enabled vehicular networks without road-side unit (RSU)," *Sustainability*, vol. 14, no. 16, pp. 1–18, 2023.
[33] K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Hesitant fuzzy sets based symmetrical framework of decision-making for estimating the durability of web application," *Symmetry*, vol. 12, no. 6, pp. 1770–1792, 2020.
[34] V. Raghuwanshi and S. Jain, "Denial of service attack in VANET: A survey," *International Journal of Engineering Trends and Technology*, vol. 28, no. 1, pp. 15–20, 2015.
[35] S. A. Khan, R. Kumar, O. Kaiwartya, M. Faisal and R. A. Khan, "Computational intelligent security in wireless communications," CRC Press, Boca Raton, vol. 1, pp. 1–296, 2023. [Online]. Available at: https://www.taylorfrancis.com/books/edit/10.1201/9781003323426/computational-intelligent-security-wireless-communications-suhel-ahmed-khan-rajeev-kumar-omprakash-kaiwartya-raees-ahmad-khan-mohammad-faisal?context=ubx&refId=9531ba02-dbbc-4414-a8bd-4d5b70a62896
[36] N. Nizamuddin, K. Salah, M. A. Azad, J. Arshad and M. Rehman, "Decentralized document version control using ethereum blockchain and IPFS," *Computers & Electrical Engineering*, vol. 76, no. 6, pp. 183–197, 2019.
[37] A. Pinna, S. Ibba, G. Baralla, R. Tonelli and M. Marchesi, "A massive analysis of ethereum smart contracts empirical study and code metrics," *IEEE Access*, vol. 7, no. 1, pp. 78194–78213, 2019.
[38] D. L. Bhaskari and P. Bhaskari, "Ethereum blockchain framework for healthcare applications," *Information Technology in Industry*, vol. 9, no. 1, pp. 1242–1249, 2021.
[39] A. Attaallah, M. Ahmad, M. Tarique, A. K. Pandey, R. Kumar *et al.,* "Device security assessment of internet of healthcare things," *Intelligent Automation & Soft Computing*, vol. 27, no. 2, pp. 593–603, 2021.
[40] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis and S. Shiaeles, "On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance," *Computer Networks*, vol. 191, no. 4, pp. 1–18, 2021.
[41] A. Raj, K. Maji and S. Shetty, "Ethereum for internet of things security," *Multimedia Tools and Applications*, vol. 80, no. 12, pp. 18901–18915, 2021.
[42] N. Nawari and S. Ravindran, "Blockchain and building information modeling (BIM): Review and applications in post-disaster recovery," *Buildings*, vol. 9, no. 6, pp. 1–18, 2019.
[43] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," *Journal of Parallel and Distributed Computing*, vol. 164, no. 9, pp. 152–167, 2022.
[44] E. Nyaletey, R. Parizi, Q. Zhang and K. Choo, "Block IPFS-blockchain-enabled interplanetary file system for forensic and trusted data traceability," in *IEEE Int. Conf. on Blockchain (Blockchain)*, Atlanta, GA, USA, pp. 18–25, 2019.
[45] B. Notheisen, J. Cholewa and A. Shanmugam, "Trading real-world assets on blockchain," *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 425–440, 2017.
[46] R. Kumar, S. A. Khan and R. A. Khan, "Revisiting software security risks," *British Journal of Mathematics & Computer Science*, vol. 11, no. 6, pp. 1–10, 2015.
[47] Q. Thai, N. Ko, S. Byun and S. Kim, "Design and implementation of NDN-based ethereum blockchain," *Journal of Network and Computer Applications*, vol. 1, no. 19, pp. 1512–1517, 2022.

[48] R. Kumar, S. A. Khan and R. A. Khan, "Software security testing: A pertinent framework," *Journal of Global Research in Computer Science*, vol. 5, no. 3, pp. 23–27, 2014.
[49] W. Wang, D. Hoang, P. Hu, Z. Xiong, D. Niyato *et al.,* "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, no. 5, pp. 22328–22370, 2019.
[50] M. Kaur, M. Khan, S. Gupta, A. Noorwali, C. Chakraborty *et al.,* "MBCP: Performance analysis of large-scale mainstream blockchain consensus protocols," *IEEE Access*, vol. 9, no. 6, pp. 80931–80944, 2021.
[51] S. Khan, F. Loukil, C. G. Guegan, E. Benkhelifa and A. B. Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2901–2925, 2021.
[52] S. A. Khan, R. Kumar and R. A. Khan, "Software security: Concepts & practices," CRC Press, New York, vol. 1, pp. 1–330, 2023. [Online]. Available at: https://www.taylorfrancis.com/books/mono/10.1201/9781003330516/software-security-suhel-ahmad-khan-rajeev-kumar-raees-ahmad-khan
[53] A. H. Almulihi, F. Alassery, A. I. Khan, S. Shukla, B. K. Gupta *et al.,* "Analyzing the implications of healthcare data breaches through computational technique," *Intelligent Automation and Soft Computing*, vol. 5, no. 6, pp. 1763–1779, 2022.
[54] S. A. Ansar, A. Singh, S. Aggrawal, A. Yadav, P. C. Pathak *et al.,* "Modernizing CPS with blockchain: Applications, challenges & future directions," *Second Int. Conf. on Interdisciplinary Cyber Physical Systems (ICPS)*, Chennai, India, pp. 124–129, 2022.
[55] K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Evaluating the impact of prediction techniques: Software reliability perspective," *Computers, Materials & Continua*, vol. 67, no. 2, pp. 1471–1488, 2021.
[56] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.,* "An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable-security of web applications," *IEEE Access*, vol. 8, no. 8, pp. 50944–50957, 2020.
[57] R. Kumar, S. A. Khan and R. A. Khan, "Durability challenges in software engineering," *CrossTalk*, vol. 42, no. 4, pp. 29–31, 2016.
[58] R. Kumar, M. T. J. Ansari, A. Baz, H. Alhakami, A. Agrawal *et al.,* "A multi-perspective benchmarking framework for estimating usable-security of hospital management system software based on fuzzy logic, ANP and TOPSIS methods," *KSII Transactions on Internet and Information Systems*, vol. 15, no. 1, pp. 240–263, 2021.
[59] K. Sahu and R. K. Srivastava, "Soft computing approach for prediction of software reliability," *ICIC Express Letters*, vol. 12, no. 12, pp. 1213–1222, 2018.
[60] R. Kumar, M. Zarour, M. Alenezi, A. Agrawal and R. A. Khan, "Measuring security durability of software through fuzzy-based decision-making process," *International Journal of Computational Intelligence Systems*, vol. 12, no. 2, pp. 627–642, 2019.
[61] K. Sahu and R. K. Srivastava, "Needs and importance of reliability prediction: An industrial perspective," *Information Sciences Letters*, vol. 9, no. 1, pp. 33–37, 2020.
[62] R. Kumar, S. A. Khan and R. A. Khan, "Revisiting software security: Durability perspective," *International Journal of Hybrid Information Technology*, vol. 8, no. 2, pp. 311–322, 2015.
[63] A. Attaallah, H. Alsuhabi, S. Shukla, R. Kumar, B. K. Gupta *et al.,* "Analyzing the big data security through a unified decision-making approach," *Intelligent Automation and Soft Computing*, vol. 32, no. 2, pp. 1071–1088, 2022.
[64] K. Sahu and R. K. Srivastava, "Revisiting software reliability," *Advances in Intelligent Systems and Computing*, vol. 802, pp. 221–235, 2019.
[65] R. Kumar, S. A. Khan and R. A. Khan, "Analytical network process for software security: A design perspective," *CSI Transactions on ICT*, vol. 4, no. 2, pp. 255–258, 2016.
[66] R. Kumar, S. A. Khan, A. Agrawal and R. A. Khan, "Measuring the security attributes through fuzzy analytic hierarchy process: Durability perspective," *ICIC Express Letters*, vol. 12, no. 6, pp. 615–620, 2018.
[67] K. Sahu and R. K. Srivastava, "Predicting software bugs of newly and large datasets through a unified neuro-fuzzy approach: Reliability perspective," *Advances in Mathematics: Scientific Journal*, vol. 10, no. 1, pp. 543–555, 2021.

[68] H. Alyami, M. Nadeem, A. Alharbi, W. Alosaimi, M. T. J. Ansari *et al.,* "The evaluation of software security through quantum computing techniques: A durability perspective," *Applied Sciences*, vol. 11, no. 24, pp. 1–18, 2021.
[69] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.,* "A knowledge-based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security-durability of web applications," *IEEE Access*, vol. 8, no. 8, pp. 48870–48885, 2020.
[70] M. T. J. Ansari, A. Baz, H. Alhakami, W. Alhakami, R. Kumar *et al.,* "P-STORE: Extension of store methodology to elicit privacy requirements," *Arabian Journal for Science and Engineering*, vol. 64, no. 3, pp. 1–25, 2021.
[71] K. Sahu, R. Shree and R. Kumar, "Risk management perspective in SDLC," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 3, pp. 1–14, 2014.
[72] R. Kumar, S. A. Khan and R. A. Khan, "Software durability: Concepts & practices," CRC Press, New York, vol. 1, pp. 1–349, 2023. [Online]. Available at: https://www.taylorfrancis.com/books/mono/10.1201/9781003322351/software-durability-rajeev-kumar-suhel-ahmad-khan-raees-ahmad-khan
[73] R. Kumar, V. Manickam and K. Palaparty, "The role of email spam in 2023 for cybercrime," DataQuest Magazine, 2023. [Online]. Available at: https://www.dqindia.com/the-role-of-email-spam-in-2023-for-cybercrime/