International Journal of Advanced Technology and Engineering Exploration, Vol 11(114)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2023.10101612

Research Article

Vehicle functionality and security optimization of autonomous vehicles utilizing EHO: a blockchain-based concept

Arunkumar. M[1*], Gomathy. B[2], Venkadesh. C[3], Sreedhar M[4] and Renugadevi S[5]
Assistant Professor, Department of Electronics and Communication Engineering, Sengunthar Engineering College, Tiruchengode, Tamilnadu, India[1]
Professor, Department of Computer Science and Engineering, Dr.N.G. P Institute of Technology, Coimbatore, Tamilnadu, India[2]
Professor, Department of Electronics and Communication Engineering, Builders Engineering College, Kangeyam, Tamilnadu, India[3]
Professor, Department of Electrical and Electronics Engineering, Velalar College of Engineering and Technology, Erode, Tamilnadu, Erode[4]
Associate Professor, Department of Electronics and Communication Engineering, Vellore Institute of Technology, Vellore, Tamilnadu, India[5]

Received: 19-May-2023; Revised: 23-May-2024; Accepted: 24-May-2024

Abstract

The automobile sector is all set to be completely transformed by autonomous cars, which are attracting a lot of interest from both academic and business enterprises. The interconnectivity of separate elements in autonomous vehicle (AV) systems, nevertheless, introduces weaknesses into the network in general. Conventional security techniques may not have been able to resolve these problems. A potent instrument that can help increase the trust and dependability in these kinds of networks is blockchain technology. The two main blockchain ecosystems are Ethereum and bitcoin. Research on how blockchain improves both security and other elements of AV systems was presented in this article. It was demonstrated how blockchain technology assists with a variety of AV-related use cases, including shared storage, improved security, enhanced vehicle functionality, and enhancement of connected sectors. Both the security and vehicle functionality were improved using nature-inspired heuristic algorithm referred to as elephant herd optimization (EHO). The optimization of parameters helped in enhancing the vehicle functionality as well as security in a more efficient manner. Results indicated that, compared with existing methods, the proposed EHO-based blockchain achieved less delay, lower reputation score, higher precision, and lower miss rate with percentages of 83.33%, 56.52%, 38.46%, and 22.22%, respectively. This offers possibilities for development in the field of AV, which may be attained by integrating blockchain technology into intelligent transport systems (ITS) or specific vehicular units.

Keywords

Autonomous vehicles, Vehicle functionality, Security, Elephant herd optimization, Blockchain.

1.Introduction

Autonomous vehicles (AVs), sometimes referred to as self-driving cars, are capable of driving themselves [1]. AVs utilize a range of sensor techniques (like camera, light detection and ranging (LiDAR), and ultrasonic sensor) to detect their environment to enable self-driving. They then employ a control scheme to perceive this sensory data in order to calculate navigation paths, obstacle avoidance, and pursue traffic signs [2].

Nevertheless, responsibility also lies with independence. How could incidents involving autonomous cars (collisions among them, or collisions with remaining vehicles, people, or various objects) be routinely and accurately documented for forensic reasons to establish responsibility? [3] Furthermore, how could the accuracy, validity, and integrity of these recorded occurrences be guaranteed? When there are motivations for the many persons engaged to interfere with the historical accounts to escape punishment, these difficulties become crucial [4]. The rapid advancement of cutting-edge technologies such as artificial intelligence (AI) and pattern recognition has caused

[*] Author for correspondence

substantial disruption in the automobile industry [5]. Modern automobiles are more than simply mechanical tools [6]. The existing performance and security of the vehicle are improved by the usage of a range of scientific investigations. These advancements are causing vehicles to become increasingly sophisticated [7]. Autonomous driving, which is the cornerstone of smart automobiles, has come to be recognized as the field that requires the most emphasis [8] due to the fact that certain features, including route planning, autonomous road identification, and vehicle body condition adjustment, drivers free from tedious driving processes and improved driving safety and simplicity playing a crucial role [9].

The goal of next-generation wireless networks is to provide low-latency, ultra-high reliability connection at all times and locations [10]. The proper communication requirements for the next driverless cars will be met by this. Autonomous cars have indeed benefited from the application of machine learning (ML) methods in a variety of ways, including computer vision for assessing impediments and ML for adjusting speed to the surroundings [11]. (e.g., bumpiness of the road). Existing cloud approaches create safety hazards because of the possible huge count of self-driving cars and the requirement of cloud models to react fast to problems in the real world [12]. Reducing the amount of information transferred and expediting the learning processes for autonomous cars may both be accomplished through optimization [13]. The desired result represents a methodical technique to this design that turns the current cars into mobile data centers, conducts optimization, and responds promptly to their demands [14]. For these networked autonomous cars, the advantages involve improved availability of smooth message transmission and minimal latency internet services while in motion [15].

Blockchain technology is still in charge of helping the automobile industry move forward. When it comes to driver data management, identity authorization, e-transactions, etc., the security that blockchain provides seems too good to be true. When it comes to cars, blockchain opens up new opportunities for things like peer-to-peer (P2P) payments for self-driving cars, vehicle sovereignty, linked mobility, and many more. Another important area where blockchain technology can help is with sharing and managing data. Even though self-driving cars create a lot of data related to driving behaviour, navigation, vehicle use, traffic, and other things, this data needs to be kept, shared, and analysed without putting security at risk. With its distributed ledger and cryptography, blockchain technology makes it faster and safer to handle data. This efficient data management with blockchain lets self-driving cars analyze and judge traffic in real time, reduce accidents, find the best routes, and cut down on journey time.

Connected transportation is another important use of blockchain technology. Blockchain technology lets cars and other facilities in the city and on the roads communicate to each other quickly and easily. It can make a reliable network and let people do business with each other in a safe way. According to a study by Frost and Sullivan, between 10% - 15% of connected vehicle transactions are likely to be done via blockchain by 2025. Blockchain makes autonomous and networked vehicles safer because it can bring together manufacturers under a single drive and test database that saves information about simulations, experiments, and problems. With blockchain technology, smart contracts can make it easier to pay for car insurance, fixes, and tolls etc. Automated payments made possible by smart contracts on a blockchain network save time and paper while increasing security and openness. The process can also go faster and be safer if passengers and cars can be checked using blockchain.

1.1Challenges

In Big data analysis, legal rights of users to delete/modify their own records, and the trade-off between privacy, transparency, and usability are just a few of the challenges that must be considered when deciding whether or not to integrate blockchain with AV despite the impressive opportunities it presents. Some of the most significant obstacles are discussed here.

i. Since blockchain is a distributed ledger, all user information and transactions are permanently recorded and available on all nodes without the possibility of erasure. A difficulty remains in explaining to the data subject where their information is maintained and for how long, even if all such data is encrypted and/or anonymized [16].

ii. Depending on the circumstances, passengers riding in a shared AV may be asked to adjust their own privacy settings. Providing such privacy preference selection, however, becomes difficult if such data is to be stored on the blockchain [17].

iii. It is unclear how the danger of re-identification may be quantified, given that data of users is saved on the blockchain and replicated on numerous nodes. Furthermore, to the best of our knowledge, there is still no well-established solution for the lack of robust privacy-preserving technology for streaming data [18].

iv. As time goes on and more people use a blockchain, the number of blocks grows. Adopting blockchain in vehicle networks could improve privacy and openness in some ways, but it would also increase the amount of work that needs to be done. The main problems with using blockchain in connected autonomous vehicle (CAV) are scalability and overhead. This is because AVs produce a lot of data and need to handle it in real time [19].

v. Researchers think that using blockchain is a good way to figure out liability in CAV, but it has been said that using blockchain could bring up some legal problems that need to be dealt with. Liability for failures or other technical mistakes will be a big legal issue, especially for forensic analysis and insurance [20].

The internet of things (IoT), AI, ML, and blockchain all offer great promise for improving efficiency, utility, and transparency across a wide range of present applications. However, there has been limited research into the feasibility of blockchain technology in fully AVs. Therefore, research on the characteristics and categories of AVs is required. It is also crucial to understand the role that blockchain technology plays in cyberspace and the system of AVs. The role of the smart contract based on blockchain technology in such circumstances is crucial. Vehicles that can operate without human input include autonomous guided vehicles (AGVs), autonomous electric vehicles (AEVs), autonomous aerial vehicles (AAeVs), and autonomous underwater vehicles (AUVs) etc. Each of these AVs belongs to one of several distinct vehicle classes. As a result, it would be instructive to investigate the many types of AVs and the role that blockchain plays in each. Blockchain technology is useful in many ways for AVs including subsystem or system integration. Supply chain management (SCM) is just one application of AGVs in warehouses all around the world.

1.2Objectives and contribution of the work

a. To utilize a nature-inspired heuristic algorithm, elephant herd optimization (EHO), to enhance both security and vehicle functionality.

b. To transform the automobile industry through the adoption of AV: This objective explores the potential industry-wide revolution due to the rise of autonomous cars, focusing on both the opportunities and the vulnerabilities introduced by their interconnected systems.

c. To enhance AV system capabilities using blockchain technology: The research demonstrates how blockchain can improve various aspects of AV systems, including security, functionality, and sector connectivity.

d. To optimize both security and vehicle functionality using EHO: By employing the EHO algorithm, this objective seeks to significantly improve the performance and security measures of AV systems.

The organization of the paper is as follows: Section 2 presents a literature survey. Section 3 provides insights into terminologies, technologies, and concepts in AVs, including detailed discussions on the use of blockchain in AVs. Section 4 discusses the results. Section 5 elaborates on the discussion. The paper concludes in Section 6.

2.Literature survey

2.1Related works

In 2021, Jain et al. [21] have sought to determine the role that blockchain technology plays in AVs, such as AEV, AUV, AGV, AAeV, and autonomous driving. In order to understand the current situation and potential problems in the future, a comparative study of blockchain-combined AV systems was investigated. The applications and significance of architectures, sensors, and infrastructure needs, vehicle kinds, vehicle target, driving modes, and tracking methodologies, intelligent data processing, intelligent contracts, and industry-specific use cases were all examined in relation to blockchain technology. The investigation of contemporary technology and activities formed the basis of this work. This paper examined current developments in autonomous cars and networks as they were anticipated to be the direction of intelligent vehicles, as well as how blockchain may serve to enhance customer experiences and industry standards. Furthermore, the limitations, potential research areas, and difficulties related to various AVs and technologies were discussed.

In 2020, Guo et al. [22] suggested a method for tracking AV events that was motivated by the blockchain. With a flexible arbitration consensus, they created the "Proof-of-Event" technique to provide reliable and observable event data in order to accomplish unquestionable accident investigations. To efficiently validate and certify the novel block of event data without the use of a central authority, they suggested a dynamic federation consensus technique. On the basis of the suggested quick leader election process and the Hyperledger fabric blockchain network, they did numerical studies and experimental prototypes. The findings demonstrated the viability and efficiency of the approach for creating and archiving accident data in blockchain-oriented vehicle networks. The suggested system's security against various threats as well as attack situations was also explored.

In 2022, Biswas et al. [23] investigated the cloud-controlled wireless network-oriented concept of the AV's cyber physical component, which was joined to UAVs. Furthermore, this approach has a blockchain-oriented security mechanism which is IoT-managed and AI-oriented. In particular, we would emphasize lateral control in autonomous driving, especially the lane change movement, while keeping in mind social behavior. Here, the authors discussed vehicle-to-everything (V2X) communication in a quick manner. V2X interaction was performed out by on-board devices and linked wireless media that improved lane departure procedures while maintaining human driver behaviour that relied on obstacle avoidance.

In 2021, He et al. [24] suggested Bift: 1) a completely decentralized ML platform paired with federated learning (FL) nd 2) blockchain to offer an ML method for CAVs that maintained anonymity. By utilizing their personal driving data to train ML techniques regionally, dispersed CAVs might now use Bift to improve the global method. In order to fend off potential attackers, Bift offered a consensus mechanism called Proof of FL. Bift's effectiveness was assessed, and it was shown to be extensible, reliable, and capable of resisting harmful attacks.

In 2022, Riyal et al. [25] have put out a concept for further developing blockchain technology so that it might be integrated with a decentralized but semi-centralized data storage system. The suggested block chain tree (BCT) strategy combined a tree structure system made up of blockchains with a time-oriented upward data propagation mechanism that optimized the design to lower communication latency, lower its high-power usage values, and guaranteed durability over time. This blockchain-oriented network topology provided significant gains with respect to energy efficiency, speed, storage, and processing, as shown in the comparison research. The suggested methodology decreased the blockchain's need for memory by a ratio of 0.17. In the initial phases of optimization, the energy needed as well as time complexity have been reduced by almost 195%. With additional transactions as well as customers, all the variables were further optimized by orders of magnitude.

In 2022, Cheng et al. [26] implemented a decentralized AV group creation mechanism on the basis of side chain approval in a highway setting. In order to explain the situations of autonomous cars, initially the consensus was side chained. Next, the authors have provided side chain consensus-based decentralized AV group establishment and management techniques. Furthermore, simulations have been run to assess the quality of side chain agreement and the durability of vehicle sets. The results demonstrated that the technique outperformed previous ones in terms of stability, information symmetry, and the proportion of computing jobs.

In 2020, Jiang et al. [27] have suggested a unique model sharing strategy that used blockchain technology to enhance object detection having cross-domain adaptation for autonomous driving vehicles. A domain adaptive you-only-look-once (YOLOv2) method was trained among nodes using blockchain and mobile-edge computing (MEC) technologies, which might drastically lessen the domain discrepancy for various item classes. Smart contracts were also created to effectively handle model sharing and data storage responsibilities. With blockchain consensus, model sharing dependability was secured. The suggested approach was tested using open data sets. The simulation outcomes showed that the suggested technique was more effective and reliable than the reference method.

In 2021, Fu et al. [28] have created a hybrid autonomous driving guidance framework using vehicle collaboration that not only addressed the "bottleneck" of knowledge acquisition during the development of expert systems (ESs) but also addressed the "black box" occurrence of ML in the decision-making procedure. This system combined the adaptive learning ability of ML and the perception abilities of ESs in a unified architectural style. Initially, a deep reinforcement learning (DRL)-based autonomous driving method for CAVs was suggested in order to help them make judgments and derive relevant laws. The next step was to provide a technique for expanding the ES knowledge base that included rule sharing, rule extraction, and rule testing. For the rule-sharing procedure, vehicular blockchain was used in specific to guarantee data security and user privacy. Thirdly, it was suggested that CAVs used hybrid autonomous driving guidance, which combined ES with ML, to produce precise and effective judgments in various driving scenarios. Once properly trained, the method could efficiently direct CAVs to navigate the challenging traffic situation. Numerous simulations confirmed that the solution performed well with respect to safety, decision-making efficacy, and accuracy.

In 2020, Pokhrel and Choi [29] have put out an autonomous blockchain-based federated learning (BFL) solution for effective and privacy-conscious vehicular communication networking, in which local on-vehicle machine learning (LoVML) method updates were traded and validated in a distributed manner. By employing the blockchain's consensus algorithm, BFL made it possible for oVML to operate without the use of centralized training data or collaboration. A mathematical structure was provided that incorporated the controllable connection and BFL variables (such as the block size, retransmission limit, block arrival rate, and the frame sizes) in order to quantify their influence on the effectiveness. This theory was founded on a renewal reward method. More significantly, the thorough examination of the characteristics of the oVML network defined the end-to-end latency using BFL. This information was crucial for determining the best block arrival rate by taking transmission and consensus delays into account. For the purpose of designing an adaptable BFL, we offered a range of mathematical and simulation outcomes that emphasized numerous non-trivial insights and findings. In addition, based on the basis of analytical outcomes, the authors established that the suggested idea of modifying the block arrival rate was evidentially online and effective at pushing the system behavior to the intended operating point. The system latency was reduced by utilizing the channel characteristics. Additionally, it showed how much less dependent on various blockchain characteristics a particular group of channel requirements, retransmission restrictions, and frame sizes was. To accomplish these improvements, nevertheless, a number of obstacles (knowledge gaps) must be closed. We specifically recognized important bottleneck issues that needed additional research and offered suggested future research options.

In 2021, Ying et al. [30] suggested reputation-based leader election (RLE) framework that consisted of two components: leader election and incentive mechanism. In the first, a reputation-oriented election system was initially created to choose a leader who could be trusted on the basis of reputation value that was stored on the blockchain. The suggested plan incorporated prior knowledge and suggestions from various participants. The second sub-system used an incentive scheme to encourage platoon participants to actively engage in the voting process. This system was dependent on the real-time fuel efficiency data collected from the cars that made up a platoon. The technology was competent to counter possible security risks, according to security research. The effectiveness and viability of the method were demonstrated by experimental findings based on the simulated environment. Some of the pros and cons of existing methods are shown in *Table 1*.

Table 1 Pros and Cons of existing methods

Author and year	Title	PROS	CONS
Fu et al. (2022) [31]	Vehicular blockchain-based collective learning for connected and AVs	The framework makes it possible for distributed CAVs to train ML models locally and then upload them to a blockchain network. This allows the entire "collective intelligence" of CAVs to be utilised, and it does so while minimizing the amount of data that is transmitted.	This works lacks in security
Shen et al. (2022) [32]	Secure and efficient blockchain-assisted authentication for edge-integrated internet-of-vehicle (IOV)	It accomplishes mutual authentication across cars, edge nodes, and cloud servers.	It is complex process because it has authentication process
Kumar et al. (2022) [33]	BDEdge: blockchain and deep-learning for secure edge-envisioned green CAVs	This approach has the potential to drastically lower the number of false alarms while simultaneously increasing	Performance analysis of this work is limited

Author and year	Title	PROS	CONS
		accuracy to around 99%.	
Prathiba et al. (2022) [34]	A hybrid deep sensor anomaly detection for AVs in 6th Generation (6G) V2X environment	This method recognises and separates potentially harmful AVs	It is not practically implemented
Tu et al. (2023) [35]	Secure IoV with decentralized consensus blockchain mechanism	It offers excellent performance in terms of authentication.	Time delay process
Bala et al. (2023) [36]	A blockchain-enabled, trust and location dependent -Privacy preserving system in VANET	Improves security and privacy for vehicles in VANET.	Computational and communication costs not fully addressed.
Tyagi et al. (2022) [37]	SecVT: Securing the vehicles of Tomorrow using Blockchain Technology	Addresses multi-level cybersecurity countermeasures against vulnerabilities to hacking.	Adoption barrier due to reliance on a large network of peers.
Alharbi et al. (2023) [38]	Intelligent Transport System (ITS) based Blockchain to preventing routing attacks	Integrates smart contracts to establish trust and verify transactions, ensuring only authorized vehicles participate in the communication network, thereby enhancing the system's integrity.	The effectiveness of the proposed solution is heavily reliant on the underlying blockchain infrastructure, which may limit its applicability in scenarios where such technology is not feasible or is in its infancy.
Chai et al. (2023) [39]	CyberChain: cybertwin empowered blockchain for lightweight and privacy-preserving authentication in Internet of Vehicles	Addresses scalability issues by integrating blockchain, allowing for adaptable, flexible, and scalable data exchange and storage platform suitable for the expanding requirements of IoV	Despite the security enhancements, the system's reliance on blockchain exposes it to risks associated with 51% attacks, where an entity with majority control of the network's hashing power could manipulate or halt transactions, reduce the system's integrity and reliability
Pujol et al. (2024) [40]	Blockchain-based framework for traffic event verification in smart vehicles	The framework's scalability was validated through simulations, indicating potential for real-world integration	The effectiveness of the proposed framework relies heavily on the existing infrastructure for smart vehicles and roadways, which may not be uniformly available in all regions.
Laghari et al. (2023) [41]	Lightweight-BIoV: Blockchain Distributed Ledger Technology (BDLT) for IoVs	Employs a decentralized data management and communication model that eliminates the need for a centralized authority, thereby reducing potential points of failure and enhancing the system's robustness.	The adoption of such a technology requires significant changes in existing IoV infrastructure and protocols, which could be hindered by regulatory, technical, and economic barriers.
Moulahi et al. (2023) [42]	Privacy-preserving FL cyber-threat detection for ITS with blockchain-based security	Employs classification approaches for cyber-threat detection at the vehicle level, improving the ITS's resilience against various cyber-attacks.	The use of blockchain and FL introduces additional computational overhead, potentially impacting the system's efficiency and scalability

Author and year	Title	PROS	CONS
Yadav et al. (2023) [43]	Blockchain-based secure privacy-preserving vehicle accident and insurance registration	Utilizes blockchain to create an immutable record of transactions, fostering trust among all stakeholders by providing a transparent and verifiable ledger of events	The application of blockchain in vehicle insurance and accident reporting may face regulatory hurdles, including compliance with data protection laws and acceptance by legal systems.
Wu et al. (2023) [44]	A decentralized lightweight Blockchain-based authentication mechanism for IoVs	Eliminates the need for centralized control, reducing the risk of single points of failure and enhancing system robustness against various attacks.	Despite efforts to minimize resource usage, the scalability of the proposed system in highly dense vehicular networks remains a concern that may affect performance.

Blockchain technology was studied in connection to the uses and importance of architectures, sensors, and infrastructure requirements, vehicle types, vehicle targets, driving styles, and tracking techniques, intelligent data processing, intelligent contracts, and industry-specific use cases. The results showed that the method for collecting and storing accident data in blockchain-based car networks was viable and effective. The findings showed that in terms of stability, information symmetry, and the percentage of computing jobs, the approach performed better than earlier ones. The results of the simulation demonstrated that the recommended strategy was more dependable and efficient than the standard method. The existing approaches performed well in terms of safety, decision-making effectiveness, and accuracy, according to several simulations. Significant bottleneck concerns were explicitly identified that need deeper study and provided recommendations for potential future research directions.

3.Materials and methods

3.1Terminologies in AVs

Autonomous or "self-driving" vehicles are those that can drive themselves using a combination of hardware sensors and AI software techniques. According to [26] standards, autonomous cars fall into one of the below categories:

Level 0: No automation: This grade only allows manual transmissions.

Level 1: Driving assistance: The car may help with either driving or speeding or stopping, but not at once. The vehicle must be driven by a driver.

Level 2: Partial automation: At this stage, driving, speeding, and stopping may be done concurrently, however the driver still needs to do the other driving tasks while keeping an eye on the road ahead.

Level 3: Conditional automation: At this stage, the vehicle is capable of handling every element of driving, although a driver is still required in the event the system so specifies.

Level 4: High-driving automation: This represents a fully working driving technology that does not require help or much concentration from the driver.

Level 5: Fully autonomous (Unconditional): Human people are only riders in this technology; they are not the drivers. The highest degree of automation is at this point.

For the purposes of this article, only level 3 and above AVs are considered. AVs employ several systems that are interconnected with one another and include a variety of parts. Although each of these parts serves a particular purpose, they all must help the AV achieve the following five key capabilities:

- Estimating the static or dynamic condition of a vehicle.
- Retrieving data regarding the environment (static and moving objects).
- Gathering data on the condition of the driver and passengers (to avoid accidents or notify them).
- Interaction between automobiles and various infrastructure (such as traffic signals or stop lights).
- Opening up a positioning system for use (often global positioning system (GPS)).

3.2Technologies in AVs

Raw data entered by vehicle-to-vehicle (V2V) parts or sensors is how AVs perceive their surroundings. The crucial perceptual job of collision avoidance (to identify both stationery as well as moving objects) is completed. On the basis of perception, AVs react in compliance with topographical circumstances, weather, maps, traffic data, and the locations of nearby cars. Perception is aided by ultrasound (US), LiDAR, radio detection and ranging (RADAR), and cameras. Radar is only utilized for incredibly long-distance monitoring in adaptive cruise control (ACC), while ultrasonic sensors are mostly employed in parking sensors. Cameras are often only utilized to locate road markings and broadcast warnings like speed restrictions on a vehicle's display.

Using electrical connections, images may be captured and sent using RADAR as well as LiDAR. By creating an almost immediate 3-dimensional (3D) map of the environment surrounding the car, the in-vehicle microprocessor can evaluate the data obtained and analyse information to determine driving judgements. The location of an ego vehicle, a crucial element of data needed for autonomous cars, is identified using the produced 3-Dimensional Map (3D map) in conjunction with GPS.

Safe operation of an AV depends on appropriate perception. For precise, dependable, and affordable mapping, AVs employs a variety of sensors, including GPS, LiDAR, RADAR for ACC, and ultrasonic sensors (employed for parking). Utilizing a camera that sends acquired data to in-vehicle microprocessors, computer vision is used to avoid obstacles, a critical duty. KITTI for the identification of cyclists and pedestrians is one approach that has been considered in existing works.

3.3ITS, vehicular ad-hoc networks(VANETS), and CAVs

A collection of both stationery as well as moving cars linked by a wireless network is known as a "VANET". Smart devices are used to link cars to one another in an environment known as an "ITS". A category of autonomous cars known as "CAVs" could be able to link to the network and offer enhanced data exchange in the type of danger information, sensory as well as location information, and environmental awareness.

Internet users may obtain and utilise deployed applications as shown in *Figure 1*. Every participant does have an address and is listed on the Ethereum blockchain (Ethereum address). Due to a fee being paid for every transaction in the shape of Ethereum gas, the expense of keeping the chain is self-regulating. As a result, every vehicle is charged a price for every transaction. The most devoted customers (those who utilize the charging station more often) incur a greater penalty, which defines a restriction of the idea of having automobiles pay for the infrastructure and processing. The charge is paid to miners as well as computational facilities for mining operations and mining-pools, which implies that there exists a strong motivation to provide various necessary tools.

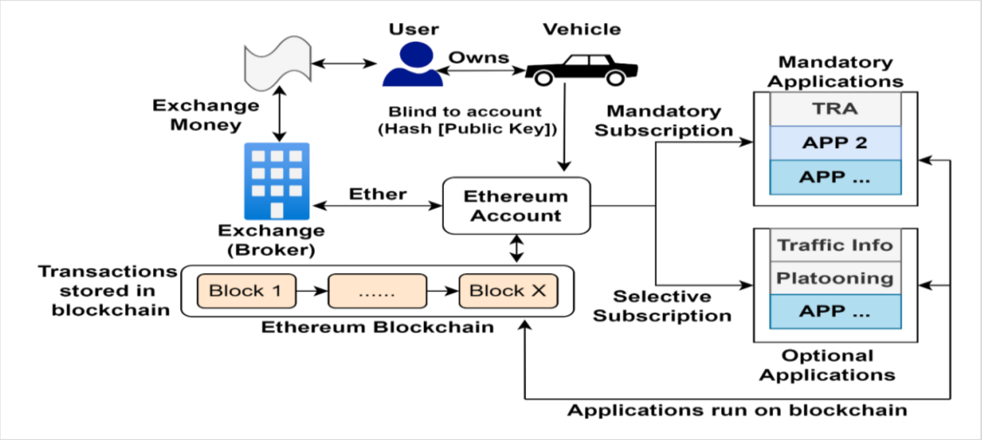

Figure 1 Ethereum oriented rule enforcement and service provision in self-managed VANETs

3.4 Blockchain

A growing set of documents, known as blocks, which are connected via cryptography is referred to as a blockchain [27]. Every block includes transaction data (often expressed as a Merkle tree), a timestamp, as well as a cryptographic hash of the preceding block [28, 29]. Blockchains could be private (controlled by a single entity), consortium (semi-private, distributed among several organizations having restricted access), public (everybody can examine and check the data), or hybrid (has aspects of both private as well as public blockchains). The Ethereum blockchain as well as the Bitcoin network represents the two majors widely used blockchains. Blockchain's main characteristics are:

Decentralized: Since no single entity owns the blockchain, there exists no centralised authority.
Secure: Hash functions are used to encrypt the data before it is saved, ensuring its security.
Immutable: Owing to the blockchain's architecture, data placed into it cannot be modified, rendering it tamper-resistant.
Transparent: Because the blockchain defines a distributed ledger, anybody may view the data.
A blockchain's constituent parts are:
Node: Any machine or user connected to a blockchain network
Transaction: the tiniest component of a blockchain network
Block: A data structure that is employed to store a collection of operations that are dispersed to entire network nodes
Chain: A group of blocks arranged in a specific order
Miners: Particular nodes that include nodes to the chain and do out block validation
Consensus: A group of guidelines and standards that have been unanimously agreed on by each of the blockchain's networks
A "state channel" represents an off-chain channel that enables two or more blockchain users to share data that will eventually be included to the chain when the channel is closed. Upon successful or unsuccessful execution of these atomic transactions, the channel is terminated (exchange or transfer). The blockchain structure is displayed in *Figure 2*.

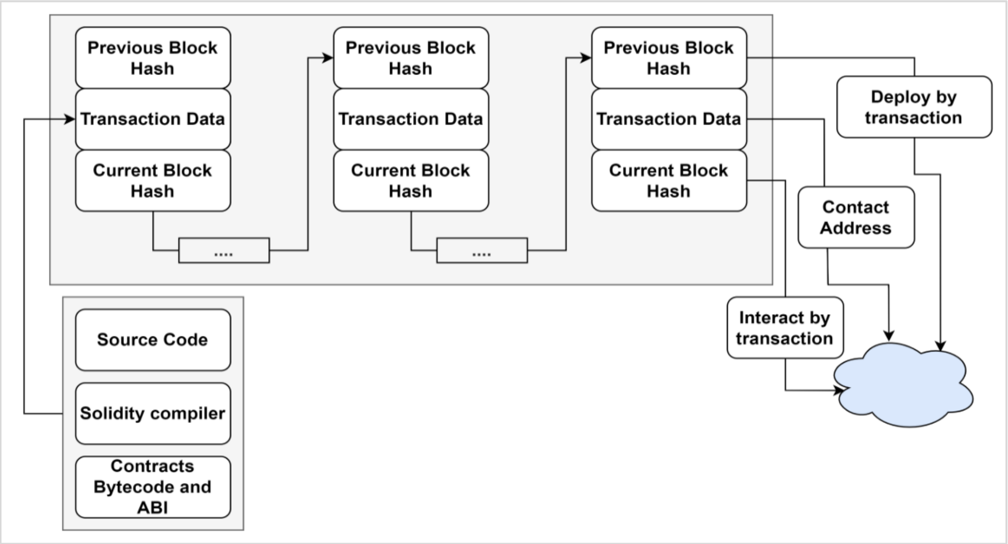

Figure 2 Blockchain structure

3.5 Scalability with blockchains

Scalability represents another issue with today's IoT networks. Present centralized solutions to authorize, authenticate, and link diverse nodes in a system would become a bottleneck when the count of devices linked via an IoT network rises [30]. The complete system might crash if the server goes down, which would need significant expenditures in servers that could manage a lot of information sharing.
Very labor- and resource-intensive mining-oriented consensus procedures are frequently utilised in public blockchains like Bitcoin to build confidence amongst completely anonymous participants. As a result, there are lengthy transaction times, which have a negative impact on both efficiency and scalability. As a result, side chains are developed to take the transaction management strain off the main chain.

The usage of private as well as permissioned blockchain is preferable in situations where there is business to business (B2B) and business to consumer (B2C) transactions. Private blockchains feature fewer nodes, which speeds up the consensus process and enhances performance and scalability overall.

Novel blockchains, termed blockchain 3.0, are presently emerging and are built on the distributed ledger technology (DLT) concepts. These blockchains employ directed acyclic graph (DAG) and a cutting-edge polling and verification technique to increase performance and scalability.

3.6 Consensus mechanism

Fault-tolerance is addressed using a consensus process. It is employed to reach a collective understanding of the channel's current status or the information that needs to be included in it. The well-known consensus algorithms include proof of work (utilized by Litecoin, Bitcoin, and Monero), proof of stake (employed by Dash as well as Ethereum 2.0), proof of vote, and proof of burn.

An autonomous element in the program known as an agent has the ability to foresee potentially hazardous circumstances and initiate a procedure for dealing with or preventing them. Suboptimal solutions could result from parallel solutions developed concurrently. Priority is assigned in these situations depending on a criterion unique to the circumstance. For instance, rather than both cars stopping, the AV approaching the location initially should slow down and the other should stop in order to prevent an accident. The factor used to establish priority ranking might alternatively be a quality that every party separately decides upon and is simple for them to learn about. The protocol should produce solutions that are consistent. This lowers the cost for transmission above a system and the necessary hardware requirements, ensuring that the agreement may be reached even without contact among the parties.

3.7Usage of blockchain for ensuring security

The heavy reliance on IoT gadgets in driverless cars defines a serious concern. Distributed denial of service (DDoS) attacks can frequently target these IoT devices. In this regard, blockchain technology has the potential to be quite beneficial. Blockchain offers a platform for fully transparent and verifiable updates and avoids single point of failure threats due to its decentralized nature. Additionally, blockchains support device authentication and verification using a distributed system.

3.8Issues and enhancements linked with AVs

The count of AVs on the road would continue to rise since it is anticipated that they will become the normalized standard. Self-driving cars have more sensors and network access when compared with non-autonomous cars, which surely increases the amount of security flaws and, consequently, the attack vector of an AV. Today's opponents are getting more and more sophisticated. With these abilities and practical low-cost aggressive tools, they may be able to quickly breach automotive security measures and, in the worst event, grant unauthorized individuals' full ownership of the vehicle or access to its data. Owing to the combination of car sensors with blockchain, the anticipated functionality of AVs may be improved. The adoption of autonomous cars and blockchain network may have a ripple effect on businesses that are directly linked. For example, the incorporation of blockchain in these AVs may eliminate the requirement for intermediaries, such as dealers in fleet management software or ride-hailing services such as Uber.

3.9Blockchain in enhancing AV functionalities

The following are some ways that blockchain might enhance the operation of an AV.

Vehicle lifecycle verification: The automotive supply chain business may be fairly complicated, including everything from suppliers, manufacturers, and vendors to providers of replacement parts as well as government regulatory bodies.

Payments and insurance: All facets of insurance transactions may fall under this. The usage of these state channels is intended to enable rapid and trustworthy exchange of data, products, and money.

Power needs and charging stations: The employment of state channels is intended to enable rapid and trustworthy trade of data, products, and money. A blockchain is used to hold the bids submitted by several charging stations, ensuring verifiability and transparency. The "start charging is triggered" event occurs as soon as the charger is plugged in. The charging system maintains its reliability by recording and saving different vehicles data in a hash that is upgraded as needed, however user data is maintained off-chain because of respect for security. The charge condition is saved on the Ethereum blockchain via a signed transaction. When a specific billing threshold is met, a payment request is sent (any method of payment can be utilized).

Parking for AVs: For the variety of AV technologies, there exist intelligent parking control designs that are suitable. This technology could be put into place for conventional automobiles and expanded to AVs in the future. Certain decision-making duties, like including automobiles in parking pools, may potentially be performed by AVs rather than people as automation levels go up.

3.10Optimizing associated industries

The AV sector has an impact on several connected sectors, including transportation and commerce, with respect to consumer participation, inter-sector reliance, and industrial relationships. Blockchain incorporation developments in the AV industry would thus have an impact on these areas. It may also be applied to address comparable advancements.

3.11Proposed workflow

The proposed methodology explains how blockchain could enhance AV systems' various components, including security. This methodology has demonstrated how blockchain technology may be applied to several applications linked to AVs, such as shared storage, enhanced security, and better vehicle functioning, and connected sector improvement. Here, a very effective nature-inspired heuristic algorithm known as EHO is used to enhance both the security and the functionality of the vehicle. In a more effective way, parameter optimisation contributes to improved vehicle security and functioning. The potential directions are presented for AV development that may be realised by incorporating blockchain technology with ITS or particular vehicle units. A detailed workflow description is given below.

- Data Collection: The system collects real-time data from various AV sensors (e.g., LiDAR, cameras, GPS).
- Data Preprocessing: Raw data are pre-processed to filter noise and prepare for analysis. This includes data normalization and feature extraction.
- Security Checks: Data are then passed through blockchain-based security protocols. This step ensures data integrity and authentication using cryptographic techniques.
- EHO Application: The pre-processed and secured data are input into the EHO algorithm. Here, the algorithm optimizes vehicle functionalities such as routing and obstacle avoidance based on current traffic conditions and environmental data.
- Decision making: The optimized results from EHO are used to make real-time driving decisions. This includes path planning, speed adjustments, and other autonomous driving actions.
- Action implementation: Commands generated from the decision-making process are sent to the vehicle's operational system to execute driving actions.
- Feedback loop: The outcomes of the actions are monitored, and feedback is sent back to the data collection phase to refine sensor inputs and optimization parameters continually.
- Data storage: All transactional data, including decision logs and action records, are stored in a blockchain. This ensures that all operations are recorded in an immutable ledger, facilitating accountability and auditability.

The EHO utilized for optimizing the functional parameters in elaborated in the next section.

3.12EHO

The EHO is used for optimizing the security as well as the vehicle functionality of the AVs. We preferred to condense the elephant herding behaviour into the below idealised principles in order to have it answer entire sorts of global optimisation issues.

- There are several clans in the elephant population, and every clan includes a certain count of elephants.
- Every generation, a certain count of male elephants would split off from their family group and live separately in an area apart from the major elephant herd.
- Every clan of elephants is headed by a matriarch and coexists as a group.

Clan updating operator: As previously indicated, a matriarch from every clan serves as the head of the whole elephant population. Thus, matriarch djhas an impact on the subsequent status of every elephant in clandj. It may be modified as with the clan dj's elephant k as in Equation 1.

$$y_{new,dj,k} = y_{dj,k} + \alpha \times \left(y_{best,dj} - y_{dj,k}\right) \times s \ (1)$$

Here, elephant k's current position in clan $dj$is indicated by the variables $y_{new,dj,k}$ and $y_{dj,k}$, correspondingly. $\alpha \epsilon [0, 1]$ represents a scale factor that assesses the impact of matriarch djon $y_{dj,k}$. $y_{best,dj}$ stands in for matriarchdj, the fittest elephant member of clandj. $s\epsilon[0,1]$. In this case, transmission is uniform.

Equation (1), i.e., $y_{dj,k} = y_{best,dj}$, cannot be used to upgrade the fittest elephant in every clan. The fit one can change it as in Equation 2.

$$y_{new,dj,k} = \beta \times y_{center,dj} \qquad (2)$$

Here, $\beta\epsilon[0,1]$ represents a parameter that governs how the $y_{center,dj}$affects the $y_{new,dj,k}$. We recognize that the knowledge gathered by every elephant in clan $dj$is what creates the novel individual $y_{new,dj,k}$in equation 2. The centre of clandj, $y_{center,dj}$, may be computed using the e^{th}dimension as in Equation 3:

$$y_{center,dj,e} = \frac{1}{o_{dj}} \times \sum_{k=1}^{o_{dj}} y_{dj,k,e} \qquad (3)$$

Here, $1 \leq e \leq E$ denotes the dimension in the e^{th}position and E denotes the overall dimension. The count of elephants in clan $dj$is known aso_{dj}. The $e^{th}$of the elephant individual $y_{dj,k}$is$y_{dj,k,e}$. By using E calculations and Equation 3, one may determine the location of clan dj's centre,$y_{center,dj}$.

Separating operator: When they reach adolescence, male elephants in the elephant group may depart their family group and live independently. When attempting to solve optimisation issues, this separating procedure may be described as a separating operator. Let's consider that the elephant individuals having the weakest fitness may utilize the separation operator at every generation as described in Equation 4 in order to further enhance the search efficiency of the EHO technique.

$$y_{worst,dj} = y_{min} + (y_{max} - y_{min} + 1) \times rand \quad (4)$$

Here, the elephant individual's position's maximum and lower bounds are, correspondingly, denoted by y_{max}andy_{min}. The worst elephant in clan $dj$is identified as$y_{worst,dj}$. $rand\epsilon[0,1]$represents a type of stochastic distribution as well as uniform distribution in the [0, 1] range. The EHO technique is created on the basis of the descriptions of the clan updating operator as well as separation operator, and its basis may be described as seen in Algorithm 1.

Algorithm 1: EHO Algorithm

```
Step 1: Initialization. Place generation counter $u = 1$; population initialization; maximum generation as $maxgen$
Step 2: while $u < MaxGen$ do
    Arrange the entire elephants as per their fitness
    Clan updating operator implementation
        $y_{new,dj,k} = y_{dj,k} + \alpha \times (y_{best,dj} - y_{dj,k}) \times s$
        $y_{new,dj,k} = \beta \times y_{center,dj}$
    Separating operator implementation
        $y_{worst,dj} = y_{min} + (y_{max} - y_{min} + 1) \times rand$
    Population evaluation using the newly updated positions
        $u = u + 1$
Step 3: end while
Stop
```

3.13Blockchain relevance

Blockchain vs DLTs: Despite the fact that a lot of AV use cases legitimately call for blockchain, there has been a tendency to abuse blockchain technology, which entails employing it without the required consensus protocol. Various use cases just need storage preservation, which permissioned DLT may readily offer; a blockchain is not always necessary in these situations.

Resistant to tamper: Some studies emphasise "tamper-free" ledgers to guarantee data integrity during AV transmission. Recognizing what the innovation delivers depends on how the phrases "tamper tolerant," "tamper-free and "tamper-resistant" are distinguished. A blockchain is impervious to tampering: It was made with the intention of resisting modification. Its protocols are strong enough to withstand manipulation even if there exists a chance of alteration. According to the research, the words "tamper-free" and "tamper-tolerant" refer to things that might be interfered with but whose consequences may be undone later by late control, rollback, or implementation changes.

Absence of relevant consensus mechanisms: Only few research papers criticise the common proof of work, blockchain consensus mechanisms, Stake, and Authority, for failing to preserve the decentralisation of regulation in the blockchain, ultimately leading to the distribution of power in the areas having more resources and computational power, respectively. Nevertheless, as noted in various articles, the recommended replacements to these fail incentives. Every link in the chain must be able to independently validate the on-chain data for public records of AV lifetime and logs for vehicle sharing. The data source should also be on-chain because the validation defines a byproduct of the consensus method, which only works with on-chain information.

In order for validation to take place as a component of the functioning, these data sources should be integral to the blockchain. Most presently suggested solutions include external verification, which makes the consensus process useless on its own unless it is made able to integrate certain sort of metadata in the AV records that serve as its source on-chain. We believe that in these use cases, blockchain technology is still underutilised given its potential as an environment.

3.14Conflicts with the usage of Blockchain in AVs

The various conflicts arising with the usage of blockchain in AVs is listed below.

Scalability: Because every node in the blockchain retains a distinct copy of all the data available on the blockchain, the idea of visibility in blockchain technology is founded on this. Because of the quick creation of significant volumes of data, this is not practical for AVs. This data would grow as there are more cars (nodes), which will make the system less effective. Keeping only the essential data on the blockchain and the other information on a shared storage device is one potential approach.

Computational feasibility: The consensus algorithm used by blockchains needs a lot of processing power. These calculations could not be made possible on AVs, which could lead to a device with limited throughput by adding to delay.

3.15 Future of associated industries

Examining the existing suggestions and evaluated options, developments in the AV industry utilizing DLTs or blockchain would enhance the experience surrounding coverage provision, with expanded services surrounding the provision of a spotless driving history, or for car loan or cooperation. Due to its ability to schedule and arrange trips without the use of a middleman, DLTs would help car sharing become more widely used. By making vehicle availability data public, DLTs enable users and automobile owners to seamlessly coordinate travel plans. Efficient SCM in the transportation sector may benefit from the use of blockchain. Nevertheless, employing blockchain technology alone does not guarantee timely processing and transportation of products. Smuggling incidents and radio frequency identification (RFID) tag manipulation might result in inaccurate data being recorded on the blockchain, rendering the technology useless overall.

3.16Cryptocurrency usage

The problem of finance could be solved when more cars become autonomous by offering a form of payment that is built into or supported by the blockchain network. This might imply that cryptocurrency might be used to cover parking and tolls. Nevertheless, in the event of a 51% miner attack, cryptocurrency usage will not be advantageous. Nevertheless, to carry off this type of attack, Ethereum as well as Bitcoin must do enormous amounts of computing.

Lesser blockchains are particularly vulnerable to these attacks since it is simple to gather the necessary computing power.
As a result, autonomous cars should choose their preferred blockchain for transactions with great caution.

Furthermore, if blockchain-oriented payments are to be used as a long-term option with AVs, the instability of cryptocurrencies defines a big barrier to their acceptance. This instability represents a result of state-specific fiscal regulations and policies rather than a feature of cryptocurrencies. An unduly pessimistic viewpoint would assert that fiat currencies will eventually be assessed with respect to cryptocurrencies, while an optimistic viewpoint would forecast that this consistency will rise. Analyzing how the market reacts to exchanges and implementations between fiat-crypto exchanges seems to be a useful strategy for determining how single platform might be utilised to solve the flaws of another.

4.Results

4.1Experimental setup

The proposed blockchain-based AVs was implemented in MATLAB simulation environment and the findings were analyzed. The hardware used is Intel core i7 processor with chipset 2600, 3.40 GHZ central purpose unit CPU 2 GB RAM running on the platform Microsoft Windows 7. The proposed EHO-oriented blockchain-based AVs was compared with existing methods such as particle swarm optimization (PSO), Gray wolf optimization (GWO), and sunflower optimization algorithm (SFO) in terms of various measures such as delay time analysis, reputation score analysis, precision analysis, and miss rate analysis to describe the betterment of the proposed method.

4.2Delay time analysis

The delay time analysis against the number of AVs is displayed in *Figure 3.* Here, a total of 100 AVs is considered. The delay time is minimum with EHO than the considered state-of-the-art methods, thereby revealing the superiority of the proposed method. Therefore, it can be demonstrated clearly that the proposed EHO-oriented blockchain-based AVs is superior to the traditional methods with respect to the delay time analysis.

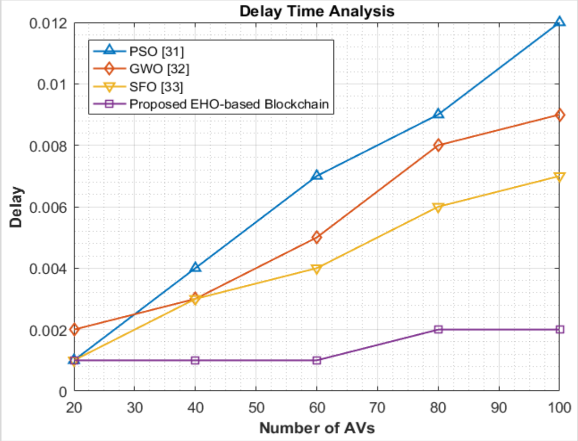

Figure 3 Delay time analysis of the proposed system

4.3Reputation score analysis

The reputation score analysis with respect to the instances of accident for the developed EHO-oriented blockchain-based AVs and the considered state-of-the-art methods as shown in *Figure 4.* The instances of accident considered are 1,2,3,4, and 5. The reputation score is minimum with the considered

EHO-based AVs than the existing methods, thus demonstrating its improvement. The suggested incentive model ensures that the most recent accident conduct will dominantly decide the reputation score.

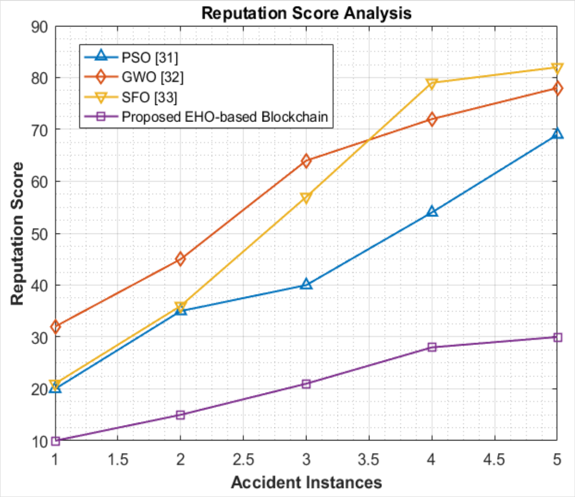

Figure 4 Reputation core analysis of the proposed system

4.4Precision analysis

The precision analysis in terms of various components for the proposed EHO-oriented blockchain-based AV and the conventional methods is shown in *Figure 5*. Here, the considered components are the bus, car, bike, person, and truck. The findings show that the suggested strategy can raise the average accuracy across a range of categories. Furthermore, when compared to current approaches, the suggested strategy can improve performance. The suggested approach can greatly lessen the domain deviation and produce better results.

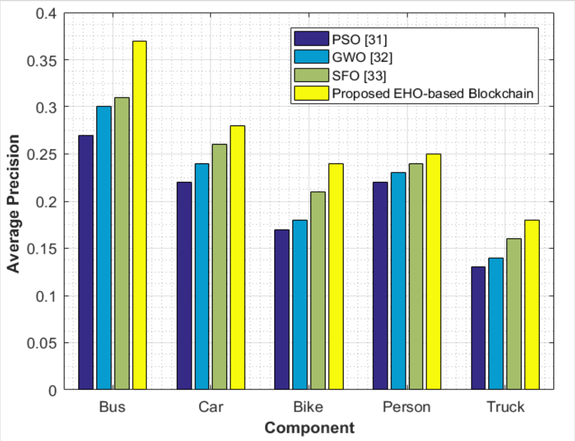

Figure 5 Precision analysis of the proposed system

4.5Miss rate analysis

The miss rate analysis of the introduced EHO-oriented blockchain-based AVs against the state-of-the-art methods as shown in *Figure 6*. In this context, the assumed components are the bus, car, bike, person, and truck. The suggested technique's miss rate is lower than the miss rates of the existing approaches. Therefore, the domain disparity between several object components may be greatly reduced using the current strategy.

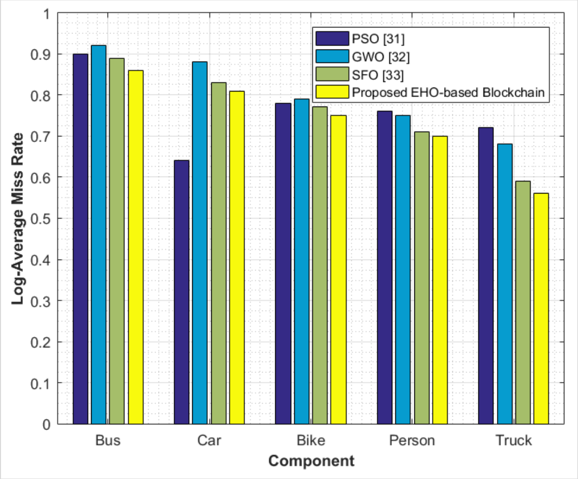

Figure 6 Miss rate analysis of the proposed system

4.6Attack possibility analysis

The attack possibility analysis of the proposed EHO-oriented blockchain-based AVs against the conventional methods is displayed in *Table 2*. It can be dmonstrated clearly from the table that the developed model achieves less attack score when compared with the other considered existing methods in various devices. Thus, it can be concluded that the possibility of attack is lower with the suggested model than the different conventional methods respectively.

Table 2 Attack possibility analysis of the proposed system

Methods	**Devices**				
	Bus	**Car**	**Bike**	**Person**	**Truck**
PSO [45]	3.5	4.9	2.7	5.3	6.8
GWO [46]	2.8	3.1	4.6	5.2	5.7
SFO [47]	4.2	5.3	6.1	7.2	4.8
Proposed EHO-based blockchain	2.5	2.9	3.8	4.7	2

5.Discussion

When compared to various state-of-the-art techniques, EHO demonstrated the shortest delay time, indicating its superiority. The reputation score for EHO-oriented AVs was lower than that of current methods, suggesting an improvement. The outcomes showed that the suggested method could increase average accuracy across several different contexts. The suggested approach was able to produce better results and significantly minimize domain disparity. Compared to existing approaches, the miss rate of the suggested method was reduced. It isevident that the suggested model had a lower attack risk compared to various conventional methods.

EHO-based blockchain has the shortest delay time compared to other methods that are thought to be state-of-the-art, demonstrating its superiority. As a result, it is undeniably proven that the suggested EHO-oriented blockchain-based AVs outperform conventional approaches in terms of delay time analysis. With the considered EHO-based AVs over the present approaches, the reputation score is minimal, proving its improvement. The recommended incentive model guarantees that the reputation score will mostly be determined by the most recent accident behaviour. The results demonstrate that the proposed technique can improve average accuracy in a number of areas. Furthermore, the recommended procedure can boost performance in comparison to current methods. The recommended strategy can significantly reduce domain discrepancy and yield superior outcomes. The miss rate of the proposed method is lower than the miss rates of the current methods. Therefore, the current technique may significantly minimise the domain mismatch between a number of object components. It is evident that the recommended model has a reduced risk of attacks than the other traditional approaches, respectively.

The proposed EHO-based blockchain achieves 83.33%, 56.52%, 38.46%, and 22.22%, respectively, less latency, less reputation score, high precision, and fewer miss rate when compared to the current approaches.

5.1Limitations

The proposed system is an independent system characterized by poor quality of service (QoS). Therefore, it requires improvement to enhance both the system itself and the associated infrastructure. Additionally, the proposed system exhibits high computational complexity.

A complete list of abbreviations is listed in *Appendix I.*

6.Conclusion and future work

This study explores how blockchain technology could enhance various components of AV systems beyond security. It has been demonstrated that blockchain can support numerous AV-related use cases, including shared storage, enhanced connectivity between sectors, increased security, and improved vehicle functionality. In this instance, the nature-inspired heuristic algorithm, EHO, was utilized to boost both security and vehicle functionality.

The EHO-based blockchain exhibits the shortest delay time compared to other methods considered state-of-the-art, demonstrating its superiority. Consequently, it is unequivocally proven that the suggested EHO-based blockchain-based AVs outperform conventional approaches in terms of delay time analysis. With the EHO-based AVs, the reputation score is minimal, signifying its improvement. The proposed EHO-based blockchain achieves 83.33% less latency, a 56.52% lower reputation score, 38.46% higher precision, and a 22.22% lower miss rate when compared to current approaches.

Some of the future works are as under:

1. Future research will expand to include more parameters beyond vehicle functionality and security, utilizing enhanced deep learning models optimized with novel hybrid metaheuristic algorithms.
2. Blockchain technology holds promise for enhancing AV security and functionality, but research into its cryptographic primitives and protocols is still nascent and requires further exploration.
3. Future considerations involve implementing off-chain transactions for specific types of data and applying suitable privacy-preserving algorithms designed for streaming data, as potential strategies to address the re-identification issue.
4. Further research is needed to explore the QoS and ways to enhance it for various AVs.
5. The development of more use-cases leads to a better understanding of the features and implementation challenges of various AVs.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

Data availability

The data considered in this study were gathered from BDD100K to KITTI, which comprise real-time driving data. The data are available in a public repository at the following links:

1. https://github.com/bdd100k/bdd100k
2. https://github.com/topics/dataset
3. https://www.kaggle.com/datasets/klemenko/kitti-dataset

Author's contribution statement

Arunkumar. M: Conceptualization, data collection, validation, draft and final writing, analysis and interpretation of results. **Gomathy. B**: Supervision, conceptualization, results interpretation, writing review and editing. **Venkadesh. C:** Supervision, conceptualization, writing review and editing.

References

[1] Xing S, Jakiela M. Lane change strategy for autonomous vehicle. Mechanical Engineering and Materials Science Independent Study. 2018.

[2] Damaj IW, Serhal DK, Hamandi LA, Zantout RN, Mouftah HT. Connected and autonomous electric vehicles: quality of experience survey and taxonomy. Vehicular Communications. 2021; 28:100312.

[3] Li H, Wu C, Chu D, Lu L, Cheng K. Combined trajectory planning and tracking for autonomous vehicle considering driving styles. IEEE Access. 2021; 9:9453-63.

[4] Hang P, Lv C, Huang C, Cai J, Hu Z, Xing Y. An integrated framework of decision making and motion planning for autonomous vehicles considering social behaviors. IEEE Transactions on Vehicular Technology. 2020; 69(12):14458-69.

[5] Guo J, Luo Y, Li K. Adaptive non-linear trajectory tracking control for lane change of autonomous four-wheel independently drive electric vehicles. IET Intelligent Transport Systems. 2018; 12(7):712-20.

[6] Yu Y, Liu S, Jin PJ, Luo X, Wang M. Multi-player dynamic game-based automatic lane-changing decision model under mixed autonomous vehicle and human-driven vehicle environment. Transportation Research Record. 2020; 2674(11):165-83.

[7] Manoharan S. Image detection classification and recognition for leak detection in automobiles. Journal of Innovative Image Processing (JIIP). 2019; 1(2):61-70.

[8] Li S, Li Z, Yu Z, Zhang B, Zhang N. Dynamic trajectory planning and tracking for autonomous vehicle with obstacle avoidance based on model predictive control. IEEE Access. 2019; 7:132074-86.

[9] Liu L, Lu S, Zhong R, Wu B, Yao Y, Zhang Q, et al. Computing systems for autonomous driving: state of the art and challenges. IEEE Internet of Things Journal. 2020; 8(8):6469-86.

[10] Seif HG, Hu X. Autonomous driving in the icity-HD maps as a key challenge of the automotive industry. Engineering. 2016; 2(2):159-62.

[11] Walling DH. The design of an autonomous vehicle research platform. Doctoral Dissertation, Virginia Tech Carilion School of Medicine Library.

[12] Wang H, Wang B, Liu B, Meng X, Yang G. Pedestrian recognition and tracking using 3D LiDAR for autonomous vehicle. Robotics and Autonomous Systems. 2017; 88:71-8.

[13] Wang W, Qie T, Yang C, Liu W, Xiang C, Huang K. An intelligent lane-changing behavior prediction and decision-making strategy for an autonomous vehicle. IEEE Transactions on Industrial Electronics. 2021; 69(3):2927-37.

[14] Xu X, Zuo L, Li X, Qian L, Ren J, Sun Z. A reinforcement learning approach to autonomous decision making of intelligent vehicles on highways. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2018; 50(10):3884-97.

[15] Dong J, Chen S, Li Y, Du R, Steinfeld A, Labi S. Space-weighted information fusion using deep reinforcement learning: the context of tactical control of lane-changing autonomous vehicles and connectivity range assessment. Transportation Research Part C: Emerging Technologies. 2021; 128:103192.

[16] Riva GM. What happens in blockchain stays in blockchain. a legal solution to conflicts between digital ledgers and privacy rights. Frontiers in Blockchain. 2020; 3:1-18.

[17] Giannaros A, Karras A, Theodorakopoulos L, Karras C, Kranias P, Schizas N, et al. Autonomous vehicles: sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. Journal of Cybersecurity and Privacy. 2023; 3(3):493-543.

[18] Javaid M, Haleem A, Singh RP, Suman R, Khan S. A review of blockchain technology applications for financial services. Bench Council Transactions on Benchmarks, Standards and Evaluations. 2022; 2(3):100073.

[19] Peng C, Wu C, Gao L, Zhang J, Alvin YKL, Ji Y. Blockchain for vehicular internet of things: recent advances and open issues. Sensors. 2020; 20(18):1-37.

[20] De FP, Mannan M, Reijers W. Blockchain as a confidence machine: the problem of trust & challenges of governance. Technology in Society. 2020; 62:101284.

[21] Jain S, Ahuja NJ, Srikanth P, Bhadane KV, Nagaiah B, Kumar A, et al. Blockchain and autonomous vehicles: recent advances and future directions. IEEE Access. 2021; 9:130264-328.

[22] Guo H, Li W, Nejad M, Shen CC. Proof-of-event recording system for autonomous vehicles: a blockchain-based solution. IEEE Access. 2020; 8:182776-86.

[23] Biswas A, Reon MO, Das P, Tasneem Z, Muyeen SM, Das SK, et al. State-of-the-art review on recent advancements on lateral control of autonomous vehicles. IEEE Access. 2022; 10:114759-86.

[24] He Y, Huang K, Zhang G, Yu FR, Chen J, Li J. Bift: a blockchain-based federated learning system for

connected and autonomous vehicles. IEEE Internet of Things Journal. 2021; 9(14):12311-22.

[25] Riyal A, Kumar G, Sharma DK, Gupta KD, Srivastava G. Blockchain tree powered green communication for efficient and sustainable connected autonomous vehicles. IEEE Transactions on Green Communications and Networking. 2022; 6(3):1428-37.

[26] Cheng J, Xu G, Yuan G, Yang L, Huang Z, Huang C, De AVH. A side chain consensus-based decentralized autonomous vehicle group formation and maintenance method in a highway scene. IEEE Transactions on Industrial Informatics. 2022; 18(12):9250-8.

[27] Jiang X, Yu FR, Song T, Ma Z, Song Y, Zhu D. Blockchain-enabled cross-domain object detection for autonomous driving: a model sharing approach. IEEE Internet of Things Journal. 2020; 7(5):3681-92.

[28] Fu Y, Li C, Yu FR, Luan TH, Zhang Y. Hybrid autonomous driving guidance strategy combining deep reinforcement learning and expert system. IEEE Transactions on Intelligent Transportation Systems. 2021; 23(8):11273-86.

[29] Pokhrel SR, Choi J. Federated learning with blockchain for autonomous vehicles: analysis and design challenges. IEEE Transactions on Communications. 2020; 68(8):4734-46.

[30] Ying Z, Ma M, Zhao Z, Liu X, Ma J. A reputation-based leader election scheme for opportunistic autonomous vehicle platoon. IEEE Transactions on Vehicular Technology. 2021; 71(4):3519-32.

[31] Fu Y, Yu FR, Li C, Luan TH, Zhang Y. Vehicular blockchain-based collective learning for connected and autonomous vehicles. IEEE Wireless Communications. 2020; 27(2):197-203.

[32] Shen M, Lu H, Wang F, Liu H, Zhu L. Secure and efficient blockchain-assisted authentication for edge-integrated internet-of-vehicles. IEEE Transactions on Vehicular Technology. 2022; 71(11):12250-63.

[33] Kumar P, Kumar R, Gupta GP, Tripathi R. BDEdge: blockchain and deep-learning for secure edge-envisioned green CAVs. IEEE Transactions on Green Communications and Networking. 2022; 6(3):1330-9.

[34] Prathiba SB, Raja G, Anbalagan S, Arikumar KS, Gurumoorthy S, Dev K. A hybrid deep sensor anomaly detection for autonomous vehicles in 6G-V2X environment. IEEE Transactions on Network Science and Engineering. 2022; 10(3):1246-55.

[35] Tu S, Yu H, Badshah A, Waqas M, Halim Z, Ahmad I. Secure internet of vehicles (IoV) with decentralized consensus blockchain mechanism. IEEE Transactions on Vehicular Technology. 2023; 72(9):11227-36.

[36] Bala K, Upadhyay R, Anwar SR, Shrimal G. A blockchain-enabled, trust and location dependent-privacy preserving system in VANET. Measurement: Sensors. 2023; 30:100892.

[37] Tyagi AK, Agarwal D, Sreenath N. SecVT: securing the vehicles of tomorrow using blockchain technology. In international conference on computer communication and informatics (ICCCI) 2022 (pp. 1-6). IEEE.

[38] Alharbi M, Alabdulatif A. Intelligent transport system based blockchain to preventing routing attacks. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). 2023:126-43.

[39] Chai H, Leng S, He J, Zhang K, Cheng B. CyberChain: cybertwin empowered blockchain for lightweight and privacy-preserving authentication in internet of vehicles. IEEE Transactions on Vehicular Technology. 2021; 71(5):4620-31.

[40] Pujol FA, Mora H, Ramírez T, Rocamora C, Bedón A. Blockchain-based framework for traffic event verification in smart vehicles. IEEE Access. 2024; 12:9251-66.

[41] Laghari AA, Khan AA, Alkanhel R, Elmannai H, Bourouis S. Lightweight-biov: blockchain distributed ledger technology (bdlt) for internet of vehicles (iovs). Electronics. 2023; 12(3):1-17.

[42] Moulahi T, Jabbar R, Alabdulatif A, Abbas S, El KS, Zidi S, et al. Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security. Expert Systems. 2023; 40(5):e13103.

[43] Yadav AS, Charles V, Pandey DK, Gupta S, Gherman T, Kushwaha DS. Blockchain-based secure privacy-preserving vehicle accident and insurance registration. Expert Systems with Applications. 2023; 230:120651.

[44] Wu A, Guo Y, Guo Y. A decentralized lightweight blockchain-based authentication mechanism for internet of vehicles. Peer-to-Peer Networking and Applications. 2023; 16(3):1340-53.

[45] Pedersen ME, Chipperfield AJ. Simplifying particle swarm optimization. Applied Soft Computing. 2010; 10(2):618-28.

[46] Mirjalili S, Mirjalili SM, Lewis A. Grey wolf optimizer. Advances in Engineering Software. 2014; 69:46-61.

[47] Gomes GF, Da CSS, Ancelotti AC. A sunflower optimization (SFO) algorithm applied to damage identification on laminated composite plates. Engineering with Computers. 2019; 35:619-26.

Arunkumar. M received his Bachelor of Engineering(Electronics and Communication Engineering) from Sengunthar Engineering College – Tiruchengode (Affiliated to Anna University, Chennai) in 2010 and Master of Engineering (VLSI Design) from Sengunthar Engineering College – Tiruchengode (Affiliated to Anna University, Chennai) in 2013.He is working as an assistant professor in Department of Electronics and Communication Engineering at Sengunthar Engineering College (Autonomous) – Tiruchengode from 2013 July with more than 10 years of experience. Presently he is a research scholar of Anna University, Chennai under the faculty of Information and Communication Engineering. His area of interest is Embedded System, Internet of Things and Artificial Intelligence.

Email: arunkumar2909@gmail.com

Dr. Gomathy. B is currently working as professor of Computer Science and Business Systems department at Dr NGP Institute of Technology, Coimbatore, Tamil Nadu, India. She received his Ph.D. degree in computer Science in the year 2014. Her area of interest includes Data Analytics, Security, Image Processing and wireless networks. Presently she is guiding research scholars in the field of Big Data and Wireless networks. She is having a lifetime membership of Indian Society for Technical Education (ISTE) and IAENG.
Email: bgomramesh@gmail.com

Dr. Venkadesh. C graduated with B.E degree in Electronics and Communication Engineering in the year 1988,M.E in Applied Electronics in 1989 and Ph.D.in the year 2007 from Jawaharlal Nehru Technological University. Currently he is working as Chief Executive Officer at Builders engineering college, Kangayam, Tirupur. He has 30 years of teaching experiences and has published more than 145 papers in the leading journals and conferences. His areas of interest are Wireless Networks, Image Processing, and Machine Learning. He is an Active member of IEEE, ISTE, IE and IETE.
Email: prof.c.venkatesh@gmail.com

Dr. Sreedhar M is currently working as professor of Electrical and Electronics Engineering at Velalar College of Engineering and Technology, Erode Tamil Nadu, India. He received his Ph.D. degree in Faculty of Communnication Engineering from Anna University Chennai in the yaer 2013. His area of interest includes are Wireless Networks, Embedded Systems.
Email: callsreedhar@gmail.com

Dr. Renugadevi S is currently working as Associate professor of Electronics and Communication Engineering at School of Electronics Engineering, VIT University, Vellore, Tamil Nadu, India. He received his Ph.D. degree in Faculty of Communnication Engineering from Anna University Chennai. Her area of interest includes are ANN, Machine Learning Wireless Networks, Embedded system.
Email: srenugadevi@vit.ac.in

Appendix I

S. No.	Abbreviation	Description
1	3D Map	3-Dimensional Map
2	AAeV	Autonomous Aerial Vehicles
3	ACC	Adaptive Cruise Control
4	AEV	Autonomous Electric Vehicles
5	AGV	Autonomous Guided Vehicles
6	AI	Artificial Intelligence
7	AUV	Autonomous Underwater Vehicles
8	AV	Autonomous Vehicles
9	B2B	Business to Business
10	B2C	Business to Consumer
11	BCT	Block Chain Tree
12	BFL	Blockchain-based Federated Learning
13	CAVs	Connected Autonomous Vehicles
14	DAG	Directed Acyclic Graph
15	DDOS	Distributed Denial of service
16	DLT	Distributed Ledger Technology
17	DRL	Deep Reinforcement Learning
18	EHO	Elephant Herd Optimization
19	ESs	Expert Systems
20	FL	Federated Learning
21	GPS	Global Positioning System
22	GWO	Grey Wolf Optimizer
23	IoT	Internet of Things
24	ITS	Intelligent Transport System
25	LiDAR	Light Detection And Ranging
26	MEC	Mobile-Edge Computing
27	ML	Machine Learning
28	oVML	on-Vehicle Machine Learning
29	P2P	Peer to Peer
30	PSO	Particle Swarm Optimization
31	QOS	Quality of Service
32	RADAR	RAdio Detection and Ranging
33	RLE	Reputation-based Leader Election
34	SCM	Supply Chain Management
35	UAVs	Unmanned Aerial Vehicles
36	US	Ultra Sound
37	V2V	Vehicle-to-Vehicle
38	V2X	Vehicle-to-Everything
39	VANET	Vehicular Ad-hoc NETwork
40	YOLO	You-Only-Look-Once
41	LoVML	Local On-Vehicle Machine Learning
42	IOV	Internet-of-Vehicle
43	6G	6th Generation
44	ITS	Intelligent Transport System
45	RFID	Radio Frequency Identification
46	CPU	Central Purpose Unit
47	PSO	Particle Swarm Optimization
48	GWO	Gray Wolf Optimization
49	SFO	Sunflower Optimization Algorithm
50	BDLT	Blockchain Distributed Ledger Technology