Risk-Based Access Control Mechanism for Internet of Vehicles Using Artificial Intelligence

S. Silvia Priscila,1 Abhishek Sharma,2 S. Vanithamani,3 Faiyaz Ahmad,4 R. Mahaveerakannan,5 Ali Jawad Alrubaie,6 Vishal Jagota,7 and Bhupesh Kumar Singh8

1Department of Computer Science, Bharath Institute of Higher Education and Research (BIHER), Chennai, Tamil Nadu, India
2Shri Vaishnav Institute Information Technology, Shri Vaishnav VidyaPeeth Vishwavidyalaya, Indore Ujjain Road, Indore, India
3Department of Computer Applications, M. Kumarasamy College of Engineering (Autonomous), Karur, Tamil Nadu, India
4Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India
5Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India
6Department of Medical Instrumentation Techniques Engineering, Al-Mustaqbal University College, Babylon, Iraq
7Department of Mechanical Engineering, Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh, India
8Arba Minch Institute of Technology, Arba Minch University, Arba Minch, Ethiopia

Correspondence should be addressed to Vishal Jagota; vishaljagota@mits.ac.in and Bhupesh Kumar Singh; dr.bhupeshkumarsingh@amu.edu.et

Received 6 June 2022; Revised 4 July 2022; Accepted 11 July 2022; Published 16 August 2022

1. Introduction to Risk Management Models

Existing access control units are proposed to provide a link among associated data with a user access rule reasoning and an asset to which entry is demanded. A user access model’s execution can be tampered with in several ways, from unanticipated circumstances involving poorly defined password policy to hostile actors acquiring access to a set of current accounts [1]. Consequently, existing access control methods compared to static and established regulations cannot deal with unpredictable events and situations. Consequently, they cannot work with a flexible, decentralized system like the Internet of Things.

The Internet of Vehicles (IoV) is a tending hotspot and is a dispersed network that allows the use of data generated by linked autos and vehicular ad hoc networks (VANETs). A
fundamental goal of the Internet of Vehicles is to enable real-time communication between automobiles and their motor traffic, pedestrians, other vehicles, roadside infrastructure, and fleet management systems (IoV). The deployment of blockchain in the Internet of Vehicles (IoV) analyses its feasibility as a security solution in VANETs. It recommends employing blockchain for data verification for vehicle identification in particular. Blockchain holds data in the form of blocks, which are generated and sent by the system. As a consequence, the procedure strengthens the validity and security of the data. On the other hand, the IoV device needs a risk-based access control paradigm [2]. As per the report, the entertainment system is linked to the Internet through a cellular connection, similar to the vehicle’s CAN (Controller Area Network) buses [3, 4]. According to experts, connecting defence components to the Internet via a sophisticated information and entertainment device is a security risk. This design enables hackers to remotely manipulate and take over the operation of a vehicle [5, 6]. Automotive cyber security is becoming a must-have element as internet connectivity affects every part of our life. Many individuals are surprised to hear that cyber security in the vehicle sector differs significantly from what we are used to seeing in the IT industry, posing challenges in terms of preparation and prevention [7, 8]. An expanded vehicle attack surface, for example, may generate vulnerabilities that attackers may exploit to seize control of and hijack the moving vehicle. This poses substantial security and safety concerns that should fundamentally modify how existing automobiles are manufactured. When it comes to autos, cybersecurity is even more important since the systems and components that manage safety must be protected against destructive assaults, unauthorized access, damage, or any other potential interruptions. Dynamic access points work because they generate access choices based on access regulations and situational variables that are assessed at the moment of the access token. This gives greater flexibility to make fully informed decisions since it can adjust to different scenarios and settings [9].

Moreover, the application of VANETs (vehicular ad hoc networks) simulation to numerous large-scale scenarios should take into consideration the automotive environment’s particular characteristics. As a result, testing and building vehicular networks in practise is expensive and time-consuming. Furthermore, analysing VANETs in such complex environments would yield inaccurate results. Simulation tools, as an alternative to true test platforms, may be used to simulate complex scenarios with more realistic consequences. Due to the limitations of real-world inter-vehicular communication (IVC) experiments on VANETs, realistic simulation is recognised as a pillar in the validation and performance assessment of IVC protocols. In contrast to static rules, access control approaches make knowledge accessible based on factual and contextual factors. Real-time elements include confidence, danger, information, experience, and requirements [10]. A risk-based authentication scheme is among the models that do a risk assessment on every access token before dynamically allowing or denying access. To successfully minimize the risk of a crash, road accident control organizations in nations all over the globe have developed not just regulations and operational procedures for highway inspections but also disaster risk assessment and prediction methodologies in the latest days [11]. Longitudinal incident data were hoped to use to detect and classify high-risk crossings, enabling for effective prioritization of limited resources to reduce road accident incidence and magnitude. The risk estimate process is crucial in implementing a risk-based user, and the chance of information leaks and the worth of that information are calculated in this procedure [2].

The driving-related characteristics, antenna-related parameters for sending and receiving signals, path-related parameters for informal communication, and noise-related parameters when utilising a fading channel make up the majority of the vehicle secrecy parameters. To mimic complicated scenarios with more realistic outcomes, simulation tools may be employed instead of genuine test platforms. Realistic simulation is acknowledged as a pillar in the validation and performance assessment of IVC protocols due to the constraints of real-world intervehicular communication (IVC) studies on VANETs. Communication in autos will be a critical component of autonomous driving technologies. They can learn from the experiences of other cars through the cloud, download data obtained in real time to publicly available maps, and send hazard alerts within their immediate surroundings via WLAN. For AVs, numerous communication technologies are available that enable vehicle-to-everything (V2X) connectivity. These technologies are classified as long-range, medium-range or short-range based on their transmission range. The short-range group talks about how AV communication technology like Bluetooth, ZigBee, and ultra-wide band are evolving. The major purpose of the risk assessment process is to provide a system for rating hazards in order of importance and make knowledge accessible in a particular circumstance using risk integer data [12]. Several studies employed various evaluation and management techniques, although the bulk of them focused on qualitative indications. Quantifying potential threats, especially in network access, is exceedingly difficult access strategy without adequate data to characterize its probability and effect [13]. The healthcare cloud shifts private information from the server to fog nodes on edge nodes to minimize transmission delay and increase user privacy. Following are some of the challenges that arise in such a situation.

1. Even though the scheme has identified and permitted virtual servers, they fraudulently read, edit, or destroy users’ private data in a typical security solution [14]

2. If the insurance provider learns about human medical private information or diagnosis findings, the insurance provider raises the premium, resulting in financial losses for the patient [15]

As a result, it is hard for a role-based or attribute-based accessibility point to prevent malevolent fog nodes from entering the region in a cloud-based situation. However, a risk-based authorization can dynamically assess the danger
of fog nodes to provide confidentiality and data security. This article’s contribution is summarised as follows:

(i) Introducing the paradigm to address the concerns of adaptability and sustainability with the fuzzy inference system for risk estimate in the risk-based authentication mechanism

(ii) The research built a SmartDrive suggestion method for drivers’ operating specialists and forecasting using the deep learning approach

(iii) A blockchain-based model enhances the security, and an artificial intelligence model enhances the system’s efficiency

The remainder of the article is as follows: Section 2 indicates the literature survey of the risk-based evaluation models. The suggested artificial intelligence-enabled access control mechanism (AI-ACM) is designed and developed in Section 3. The software analysis and performance evaluations of the proposed system are illustrated in Section 4. Section 5 enumerates the conclusion and future scope of the system.

2. Background to the Risk-Based Evaluation Models

Previous research has used a variety of methodologies to examine and forecast road accident probability, including standard analytics, deep learning, and intelligent systems. Predicting the likelihood of a traffic collision necessitates the accurate identification of key independent variables or key variables [16]. The traditional method exhibits a poor average risk score, lower central processing unit (CPU) utilization ratio, and higher latency.

Ghazal et al. suggested a study methodology based on vehicle motion database key feature extraction and lane-changing (LC) behavior prediction models on expressways [17]. This study used attack tree modeling and K-means grouping systems to estimate the danger level of automobile lane shifts and rely on the Collision Potential Index (CPI). The interaction among the vehicle changing lanes and modifications in vehicle performance among the neighboring automobiles in the middle lane was found to be a major component in the risk analysis of lane-changing behavior, according to the outcomes of key selecting features [18].

Makarfi et al. developed collision propensity forecasting models regarding vehicle social categories acquired using the floating car approach on a Shanghai expressway [19]. The binary logistical regression framework and the support vector machine (SVM) were utilized to create prediction models that had an efficiency of 75%, compared to the 58 percent of total for the unconditional logistic regression.

Hu et al. investigated real-time accident prediction difficulties, which included effects of cultural, demographic information, and trip-generating characteristics on instant accident rate and traffic and weather forecasting elements [20]. The system produces a lower throughput, higher travel distance, and lower accuracy rate. They analysed the imminent accident risk of motorway ramps using traffic, geometry, sociodemographic, and trip-generating factors. Two Bayesian logistic regressions were utilized to detect collision antecedents and their influence on the ramp accident rate [21]. Four SVM algorithms were utilized simultaneously to forecast collisions. According to the findings, socio-demographic and travel-generating factors increased predictive accuracy. Based on three indexes, overall traffic, sonic boom area, and platoon proportion, Chen et al. devised a generalized extreme value (GEV) approach Bayesian network hierarchical system to estimate accident risk [22]. Four signalized junctions in Surrey, British Columbia, were used to test the suggested system. Ning et al. used a GAN method to balance uneven traffic information in conflict and non-collision instances, rebalancing the information using the artificial minority oversampling method and randomized undersampling approach [23]. To compensate for the lack of driver reaction abilities, the intelligent driving system, which is part of ITS, uses cutting-edge information technology to provide the driver with road driving assistance. Vehicle detection is the most fundamental component of ITS and is critical for resolving traffic concerns. GAN is used to enhance the features of cars in night-time images. Twelve quality assessment systems were proposed using the logit model, SVM, and neuronal networks in the research setup. The method has the highest predictive performance, according to the findings.

Many studies have offered a broad range of ideas to enhance intelligent transport systems (ITS) and upcoming vehicle risk indices, in which automobile crashes, head-on collisions, burns, and roll-on occurrences effectively identified with onboard sensors mounted in intelligent cars [24]. Because of technology improvements, road administrations throughout the world now have the opportunity to modify how they manage and administer their roadway networks [25, 26]. Intelligent transportation systems (ITSs) integrate cutting-edge information and communication technology to improve the security, efficacy, and sustainability of transportation networks, reduce traffic congestion, and improve driving experiences. There are several methods to enhance the system [27, 28]. The intelligent transportation system becomes the most significant component of all with the concept of a smart city changing cities into digital societies and bettering the lives of its citizens simpler in every manner [29, 30]. Mobility is a crucial issue in any city; whether residents are going to school, university, or the office, or for any other purpose, they rely on the city’s transportation infrastructure [31, 32]. By utilising an intelligent transportation system, citizens may save time and make their city smarter. It offers comprehensive traffic intelligence, local convenience data, real-time running information, seat availability, and other services that save passengers time while also increasing their security and wellbeing [33, 34]. Driver behavior analysis receives the greatest attention in preventing injuries and traffic safety since drowsy drivers cause a substantial proportion of accidents. To attain better precision in the study of driving behavior, it is also required to incorporate
traffic and junction features. In addition, today’s smart systems employ alert-generating components in surveillance systems to deliver quick notifications to the appropriate vehicles [35].

Steering orientation, vehicle location, driver’s retina, and physiological assessment play important roles in behavior detection. On the other side, path prediction based on previous sequences and present car and driver behavior attracts a lot of interest [36]. The multi-modal Kalman filter is utilized for trajectory tracking based on the enlarged Kalman filter. The suggested Kalman filter effectively controls the input sequence matrix primarily using three variables: vehicle velocity, location, and range from the junction [37]. Long-short-term-memory (LSTM)-based path prediction is ineffective in the case of traffic safety since the path should be anticipated as soon as possible to prevent crashes and disasters. The system exhibits a lower CPU utilization ratio, higher travel distance, and lower accuracy rate.

Risk-based authorization methods are largely utilized to give the authorization system the versatility required. Some scholars considered developing a risk-based authorization paradigm to combat adaptability and the capacity to handle unanticipated scenarios. Nkenyereye et al. established the Risk-Adaptable Authorization (RAA) approach for granting or refusing access based on analysing security threats and operational demands [38]. The risk that comes with authorization is calculated using this model compared to the authentication and authorization. The software then double-checks the operating requirements. Access is provided if the necessary operational requirements and policies are satisfied. However, this approach does not include information on quantifying risk and requirements objectively. To prevent attackers from harming the ITS vital infrastructure, the system should include preventive techniques in addition to detection and recovery strategies. Such preventative techniques must be incorporated into the design from the beginning. Design phase is the most effective stage to prevent exposure, initial security consideration will prune research initiatives that are expensive to secure once implemented, blind eye to attackers will endanger the system robustness, and security is crucial to government and customers are some reasons to secure the in-vehicle network prior to implementation [39, 40].

Song et al. also created a risk-based system based on item sensitivity, subject reliability, and the differential between the two [41]. However, the model does not provide a method for quantitatively estimating risk. Moreover, in the initial stages of the risk analysis, this approach necessitates a network administrator with extensive knowledge to offer an acceptable value for every input. Creating a consistent and precise risk assessment approach that can handle challenges connected with existing methods in terms of sustainability and incapacity to adapt is one of the primary issues in developing an efficient and dependable risk-based security model [42]. This paper applies the prototype to the risk prediction method to create an effective and flexible risk-based security model. To the greatest of the researchers’ knowledge, no study uses the paradigm in risk-based authentication protocols. As a result, the risk assessment approach of the risk-based authentication mechanism is implemented in this study using a unique IoV model.

3. The Proposed Artificial Intelligence-Enabled Access Control Mechanism

Because robotics is one of the many sectors in which AI has been used, this is a natural application for the technology that aspires to master autonomy. The concept’s promise is that AI and perceptual technologies will provide safer and more predictable behavior, resulting in benefits such as fuel efficiency, comfort, and ease. Developing AI systems for something as complex as a self-driving automobile involves a number of challenges. The AI must connect with several sensors and utilise data as soon as possible. The proposed AI-ACM system is designed with artificial intelligence and a blockchain model. A fuzzy system simplifies the computation process. The three levels of fog computing’s layered structure are as follows:

(1) Edge layer: This surface is the one that is nearest to the client and the physical environment. It comprises various IoT devices, such as sensors, smart cars, cellular phones, etc. These machines’ computations are capable of processing data and are extensively scattered regionally. They are in charge of sensing actual item or product feature information and providing it to the higher layer for handling and preparation.

(2) Fog layer: This layer is made up of several fog nodes that are positioned at the channel’s edge, such as fog servers, gateways, and ground stations. Among edge sources and the network, cloud resources are widely dispersed. They can calculate, transmit, and hold the detected data.

(3) Cloud layer: This layer comprises several elevated storage devices that provide software services, such as smart city, smart manufacturing, smart neighborhood, etc.

The proposed AI-ACM system architecture and layered architecture are shown in Figures 1(a) and 1(b). Each layer is designated with its role at certain level. It comprises of various sensors to process the given information. These sensors are very sensitive, which help to make the system of IoV efficient and reliable. However, this model enhances the system’s accuracy and produces better results. The IoT architecture has three layers, namely, the perception layer, network layer, and application layer. The respective elements in each layer are shown. The system is designed with the three-tiered model. The system exhibits a lower average risk score, higher CPU utilization ratio, and lower latency. The functions of the AI-ACM system are listed below:

(1) Policy Enforcement Point (PEP): It captures memory utilization access queries and forwards them to the policies decision points (PDP), which makes the optimal choice. PEP is in charge of putting PDP’s access choices into action. It satisfies many requirements that PDP imposes as part of the access
determination. An XML requirement is a directive from the PDP towards the PEP on the actions taken during access is granted.

(2) Policy Decision Point (PDP): It reviews user access and generates access choices given the available characteristics that characterize the request’s components (topic, item, and action), as well as relevant access developing customized.

(3) Policy Information Point (PIP): It provides PDP with the attributes it needs to analyse user access versus GAN. It gathers information about the subject, source of relevance, and context wherein permissions are made and passes this information to the PDP via the contextual handler during access judgment.

(4) Policy Administration Point (PAP): It facilitates policy management by allowing users to establish, remove, and amend password policy. It also keeps track of the policy superintendent’s file permissions.

3.1. Risk-Based Access Control Model. Unauthorized data exposure is among the most pressing issues that must be handled in the IoV device. Existing access control systems cannot address this problem since they are based on static and predetermined rules that always provide the same outcome in diverse conditions. As a result, they are not adaptable enough to deal with changing user behavior, particularly in a live situation like the Internet of Things. The model shows the higher throughput, lower travel distance, and higher accuracy rate. On the other side, dynamic admission control techniques are an efficient option for dynamic settings such as the Internet of Things. They use access regulations and genuine and contextual variables to make entry choices. One of the model parameters that use the vulnerability assessment value attached with every access token as a parameter to decide the optimal choice is the risk-based authorization model. It uses a risk tool to evaluate the vulnerability assessment value of every access token and then decides whether to allow or refuse access based on the projected risk value. The research presented and explored a dynamic risk-based authentication protocol for the Internet of Things. The suggested model comprises four input data: user/agent environment, resource vulnerability, activity intensity, and risk record. The vulnerability assessment value linked with the authorization is estimated using these inputs/risk variables. The calculated risk data are then compared to policy measures to determine the optimal choice. The suggested risk-based model’s ultimate objective is to build a system that encourages information exchange to maximize organizational advantages while strictly being accountable for their actions.

3.2. Fuzzy Risk-Based Decision Method. The fuzzy risk-based selection method is suggested in its first form, and it is described in a concise manner below. Risk is expressed as the product of threat probability and effect, expressed as

\[
\text{Risk} = \text{Threat probability} \times \text{effect} \quad (1)
\]

The possibility of a threat is determined by the vehicle’s environment and the driver’s mindset. On the other hand,
the effect is determined by the vehicular environment. The six aspects of a vehicle environment are lane, route, traffic, climate, velocity, and timing.

The risk estimation model of the AI-ACM system is shown in Figure 2. The content from the user is gathered, resources sensitivity is computed, action severity is analysed, and the risk history is stored in the database. The evaluated risk is assessed, and the final grant and deny results are followed. There are two approaches to assess the impact. One method is to determine it based on the project type. Information, transportation effectiveness, and safety uses, for instance, have minimal (0), moderate (1), and high (2) effects. All three programs operate separately simultaneously, and there is no link between them. The operation is denoted as

\[ I(x) = \begin{cases} 
0, & \text{if } x = \text{infotainment}, \\
1, & \text{if } x = \text{traffic efficiency}, \\
2, & \text{if } x = \text{ safety},
\end{cases} \]  

(2)

The data collected from the IoV device are denoted as \( x \). The alternative method uses the trapezoidal-shaped degree of membership to calculate the effect if the user’s sensitivities value \([0, 10]\) is specified in

\[ I(X_0) = \begin{cases} 
0, & \max\{\min[X_0 + 2, 0, X_0 - 2]\} = 1, \\
1, & \max\{\min[X_0 + 1, 2, X_0 - 3]\} = 1, \\
2, & \max\{\min[X_0 + 5, -2, X_0 - 3]\} = 1, \\
3, & \text{otherwise},
\end{cases} \]  

(3)

The IoV data collected from the user is denoted as \( X_0 \). After defining the parameters for vehicle environment, driver mood, and application sensitivity level, the risk is calculated. The risk is expressed as

\[
\text{Risk} = r_s(\max \left[ \frac{b_1}{W_1}, \frac{b_2}{W_2}, \frac{b_3}{W_3}, \frac{b_4}{W_4}, \frac{b_5}{W_5}, \frac{b_6}{W_6} \right] + r_a(\max \left[ k_1, k_2 \right]) )
\]  

(4)

The output weights of the six elements utilized in determining vehicle environment are represented by \( b_1 \) to \( b_6 \). The factor loadings for the components utilized in determining the driver’s mindset are \( r_1 \) and \( r_2 \). The factor loadings for the variables utilized in threat probability assessment are \( k_1 \) and \( k_2 \). The environmental variable is denoted by \( b_7 \). The risk is estimated based on the relevant data of the transmitter and recipient nodes, and a choice is made appropriately. This approach focuses on vehicle-to-vehicle communication at the application level.

3.3. Implementation of the System. The risk estimate approach of the risk-based authentication scheme was implemented using the hybrid system. The implementation of the hybrid system took place in two stages. After implementing the fuzzy logic technique, the neural network was utilized to educate it. The risk criteria considered were user setting, resource vulnerability, action seriousness, and danger history. The fuzzy inference system was then constructed to produce a quantitative risk estimate for each input factor based on the information of IoV security researchers. The result of the fuzzy inference machine with input was utilized to create a dataset for training the system and choosing the most suitable learning method that delivered the best results for the task. The system exhibits a higher CPU utilization ratio, lower travel distance, and higher accuracy rate.

This resulted in a precise output risk rating, which was utilized to determine whether to allow or reject access to every authorization as soon as possible. The input layer represents the risk factors, including the user environment, resource vulnerability, activity intensity, and risk histories. The output layer reflects the risk value calculated as a result of the risk estimate procedure. The risk estimate technique uses the intermediate layer as a concealed layer. The intermediate layer is a hidden layer that performs calculations and updates weights among distinct connections. Identifying the correct hidden layers and cells for every hidden unit was one issue connected with developing the paradigm.

The intricacy of the connection among the input and goal parameters determines the hidden layer required, and it has a significant influence on the education process. A Feed-Forward Back Propagation (FFBP) system with more than one buried layer. An FFBP system with one hidden state is sufficient for most issues in various applications. In addition, choosing the correct amount of neurons in the concealed layer is critical to the designer’s execution. If there are not enough neurons in the simulation, it won’t be able to simulate intricate data, and the fitting would be poor.

Using a massive amount of hidden units influences the results on fresh input, and its capacity to generate a generic model is harmed. Although expanding the number of neurons provides proper training, it affects performance. As a result, a balance must be struck between several with too few hidden units.

3.3.1. Weight Computation for the Environmental Variable. \( b_1 \) to \( b_6 \) are the weighted numbers of the six elements utilized in determining vehicle context, does not provide the method for calculating the weights’ amounts. This study proposes new weight measuring instruments. It guarantees that the
total of all weighting factors equals one. The following equation is used to determine the normalized $b_1$:

$$b_1 = \frac{s_1(W_r)}{|W_r|} \sum_{x=1}^{6} s_1(f_x)$$

The IoV environmental parameter is denoted by $s_1(W_r)$, and the scaling function is denoted by $W_r$. The vehicular factor is denoted by $f_x$, and the solution is denoted by $s_1(f_x)$. The normalized $b_2$ is computed using the following equation:

$$b_2 = \frac{s_2(W_r)}{|W_r|} \sum_{x=1}^{6} s_2(f_x)$$

The IoV road parameter is denoted by $s_2(W_r)$, and the scaling function of the road is denoted by $W_r$. The vehicular factor is denoted by $f_x$, and the solution is denoted by $s_2(f_x)$. The following equation is used to determine the normalized $b_3$:

$$b_3 = \frac{s_3(W_q)}{|W_q|} \sum_{x=1}^{6} s_3(f_x)$$

It computes $b_3$ by splitting $s_3(W_q)$ with $|W_q|$, just as like $b_1$. The vehicular factor is denoted by $f_x$, and the solution is denoted by $s_3(f_x)$. Factor route has 16 potential values. As a result, $|W_q| = 16$. Five of the 16 have been identified as being at high risk. As a result, $s_3(W_q) = 3$.

The following equation is used to determine the normalized $b_4$:

$$b_4 = \frac{s_4(Q_d)}{|Q_d|} \sum_{x=1}^{6} s_4(f_x)$$

It computes $b_4$ by splitting $s_4(Q_d)$ with $|Q_d|$, just as like $b_1$. Component weather has five potential values. As a result, $|W_q| = 5$. The vehicular factor is denoted by $f_x$, and the solution is denoted by $s_4(f_x)$. Two of the five are marked as high-risk. As a result, $s_4(Q_d) = 4$. The following equation is used to determine the normalized $b_5$:

$$b_5 = \frac{s_5(T_l)}{|T_l|} \sum_{x=1}^{6} s_5(f_x)$$

It computes $b_5$ by splitting $s_5(T_l)$ with $|T_l|$, just as like $b_1$. The vehicular factor is denoted by $f_x$, and the solution is denoted by $s_5(f_x)$. Two of the six are marked as high-level of risk. As a result, $s_5(T_l) = 3$. One of the three values is associated with a significant level of risk. As a result, $s_5(T_l) = 1$. The following equation is used to determine the normalized $b_6$:

$$b_6 = \frac{s_6(G_k)}{|G_k|} \sum_{x=1}^{6} s_6(f_x)$$

It computes $b_6$ by splitting $s_6(G_k)$ with $|G_k|$, just as like $b_1$. The vehicular factor is denoted by $f_x$, and the solution is denoted by $s_6(f_x)$. One of the four values is associated with a high level of risk. As a result, $s_6(G_k) = 1$.

The mathematical model of function $b_6$ is computed and shown in Figure 3. The different environmental and IoV parameters and scaling weights are used to compute the results.

### 3.3.2. Weight Computation for Threat Likelihood Variable

The vehicle environment calculates the threat probability ($V_{att}$) and the driver’s attitudes ($D_{att}$) as previously stated. The threat probability is defined as stated in

$$\text{Threat probability} = k_1 V_{att} - k_2 D_{att}.$$  

The factor loadings for the automobile context and motorist’s attitude variables, correspondingly, are $k_1$ and $k_2$. The technique for calculating these weights’ values is unknown. The following technique for measurement methods is proposed in this study. Suppose that $|V_{att}|$ is the total variety of features used in the automobile context computation, and $|D_{att}|$ is the number of variables used in the
motorist’s attitude computation. The value obtained of the automobile context must be larger than the weighting factor of the driver’s attitudes since the computational complexity used in car context computation is more than the set of elements used in driver’s attitude computation. The following equation is used to compute the IoV variable:

$$k_1 = \frac{|V_{ct}| \pm |D_{att}|}{|V_{ct}| - |D_{att}|}$$  \hspace{1cm} (15)

The vehicle environment calculates the threat probability ($V_{ct}$) and the driver’s attitude ($D_{att}$). Subtracting $k_1$ from 1 yields the weighted sum ($k_2$) of the driver’s mindset and is expressed in

$$k_2 = \frac{|V_{ct}|}{|V_{ct}| + |D_{att}|} + \frac{|D_{att}|}{|V_{ct}| - |D_{att}|}$$  \hspace{1cm} (16)

The vehicle environment calculates the threat probability ($V_{ct}$) and the driver’s attitude ($D_{att}$).

### 3.3.3. Weight Computation for Driver Parameters

The driver’s attitude is determined in the following way, as stated in the following equation:

$$D_{att} = \max(d_1 \times S, d_2 \times T).$$  \hspace{1cm} (17)

It is determined by two factors: age ($S$) and expertise ($T$). Three risk levels are connected with every variable: low, moderate, and extreme. The output weights ($d_1$ and $d_2$) are modified at execution depending on the methods. The output weight is expressed as

$$d_1 = \frac{G_c(S)}{G_c(S) + G_c(T)}$$  \hspace{1cm} (18)

$G_c(S)$ and $G_c(T)$ are the edge values of the maturity and experience factors.

The mathematical model of function $d_1$ is depicted in Figure 4. The edges of age and experience factors of the drivers are used to compute the final result. $G_c(S)$ and $G_c(T)$ are the edge values of the maturity and experience factors, correspondingly. The value of $d_2$ is found by subtracting $d_1$ from 1 and expressed as

$$d_2 = \frac{G_c(T)}{G_c(S) - G_c(T)}$$  \hspace{1cm} (19)

$G_c(S)$ and $G_c(T)$ are the edge values of the maturity and experience factors. When the relative risks for the variables maturity and experience are small and great, correspondingly, the factors of $G_c(S)$ and $G_c(T)$ are 5 and 11, respectively.

### 3.4. Intelligent Edge Computing

Edge computing is largely responsible for the evolution of the environment surrounding the vehicle sector. The exponential data rise in connected and autonomous automobiles, real-time data handling, and novel technologies are driving the edge computing business. Rather than doing it centrally, it puts processing and data closer to the edge, where people or devices may access it. This preserves real-time findings while minimising application performance and latency problems. Users’ availability of Internet material has steadily grown as the IoV has progressed. More networking is essential to accommodate the massive data flow, resulting in server overload and greater network traffic. The edge caching technique offers great ability to alleviate the traffic load issue.

The traffic burden in the system can be lowered by boosting the precached information of end consumers in edge nodes. In peripheral cache technologies, it is frequently essential to estimate the cache contents and store time that relies on the prior forecast of user demands, content attractiveness, and other material. GAN is used to make accurate predictions. The model exhibits a lower average risk score, lower latency, higher throughput, and lower travel distance. Among the AI techniques, supervised learning can engage with and pass judgment based on student engagement with the surroundings. Mobile cloud technology also allows for edge node processing and storage, allowing AI systems to be used in computing design. As each edge device can sense its data center, the users can comprehend by mining the electronic information signals of IoV participants in the system and combining them with evolutionary programming technology. Cache efficiency is enhanced by the intelligent choice of cached items in a restricted storage area.

In addition to its cache purpose in edge devices, automation also serves as a task-lightening optimization tool. The endpoint can offload computational activities to adjacent edge devices or the Internet for execution and get the aspect of development in a computing system. However, in light of changes in networking circumstances and resource limits, activities cannot even accomplish offloading at a
minimal price in the real world. Template matching technology is applied to learn dumping techniques and implementation costs throughout task unloading. GAN continually directs the maximum of the incentives functional in the template matching network during the learning phase. Eventually, it realizes the decision-making capacity of the smart offload of computational jobs, maximizing the computational task application performance. The convergence of technology frequently results in innovative solutions. The IoV combines cloud technology and intelligent systems to create smart cloud technology, which promotes and relies on one another. It paves the way for today’s fast growth of automated driving.

3.5. Performance Improvement Mechanism. Traditional geographic crowdsourcing job allocation depends too heavily on centralized crowdsourced servers, which, if attacked, will result in the site’s data loss, causing all of the provider’s private data to be destroyed and the entire network to break. It uses blockchain technology to address this issue, which has the decentralized characteristic of ensuring that each employee has a full duplicate of the whole blockchain state, so even if one worker is targeted and unable to operate, other workers keep working. Nevertheless, the blockchain’s transaction computing power is insufficient to match the practical demands of geographical crowdsourcing work distribution. The performance improvement algorithm is shown in Algorithm 1.

A blockchain efficiency optimization technique is developed to increase the transactions processing capability by dynamically choosing the blockchain consensus method, frame size, and block production rules to optimize the capacity of blockchain. The following are the stages, activities, and reward components. This study defines the subspace $SS(x)$ of every epoch $t$ in the perspective of blockchain improving performance as the combination of transaction volume $TS(x)$ and node computational power $NP_c$, which can be stated explicitly in

$$SS^x = [TS(x),]NP_c^x.$$  

The transaction volume is denoted by $TS(x)$, and the node computational power is denoted by $NP_c$.

Action: Modify the block-generating node $BG_n$, the consensus method $B_c$, the block length $BG_l$, and the block creation time $BG_t$ to enhance the throughput. As a result, the activity space $Q^x$ is defined in

$$Q^x = [BG_n, BG_l, BG_t, B_c]^x.$$  

The packet generation node $BG_n \in (T_1, T_2, T_3, T_4)$ is represented by $BG_n$, where $BG_n \in [0, 1]$ represents the Kafka consensus protocol and $BG_l$ represents the Solo consensus protocol, correspondingly. $BG_l$ represents the block size, with $BG_l \in [0.2, 0.4, 0.6, \ldots, BG_l^{max}]$ representing the greatest block size. $BG_t$ is the time it takes to produce a new element, $BG_n \in [0.5, 1, \ldots, BG_n^{max}]$ is the longest block generation time, and $BG_{nmax}$ is the smallest packet generation time.

Reward: Every epoch $t$ must meet the following requirements to enhance the blockchain bandwidth. The reward is expressed as

$$R = \max \{F(T, Q)\}.$$  

$F(T, Q)$ is an action-value product with a discount factor of $\alpha \in [0, 1]$ and an instantaneous reward $R^x$. The final evaluated risk and its reward are expressed as

$$R^x(T^x, Q^x) = \frac{W_t \times TS(x)}{W_n}.$$  

The IoV environmental variable is denoted by $W_t$, the vehicular risk factor is denoted by $W_n$, and the transaction cost is expressed by $TS(x)$.

The AI-ACM system is designed with blockchain and artificial intelligence. The system’s security is increased by blockchain, and the accuracy is enhanced by artificial intelligence. The system complexity is reduced by using a fuzzy system. The effectiveness of the AI-ACM system is analysed and evaluated in the next section.

4. Simulation Outcomes and Analysis

To enhance the precision of the output hazard, several tests were conducted to train the suggested framework of the risk estimate approach. Moreover, multiple tests were carried out using different learning methods to identify the number of hidden units. The MATLAB program was used to write and run all learning and tests. On an Intel(R) Core (TM) i5, 2.40 GHz CPU, with 8 GB RAM, running Windows 8, all tests and observations were programmed in MATLAB. The simulation outcomes such as average risk score, central processing unit (CPU) utilization ratio, latency, throughput, travel distance, and accuracy rate regarding IoV vehicles and credit are analysed.

The average risk analysis of the AI-ACM system is computed and shown in Figure 5. The simulation is done by considering the 100 IoV vehicles, and the respective risk of each vehicle is computed and monitored. With the help of artificial intelligence, the AI-ACM system increases the risk computation efficiency and the blockchain model enhances the security; hence, the overall efficiency is increased. The risk evaluation is done using the fuzzy model that simplifies the computation process and produces faster results with higher accuracy.

The simulation analysis of the AI-ACM system is depicted in Table 1. The simulation outcomes such as CPU utilization ratio, latency, and throughput of the AI-ACM system are computed, and the outcomes are tabulated. The AI-ACM system is designed with artificial intelligence and a blockchain model in the vehicular environment. The simulation outcome of the AI-ACM system is analysed continuously, and the outcomes show the effectiveness of the AI-ACM system more than the traditional model. The AI-ACM system has a higher CPU utilization ratio, lower latency, and higher throughput.

The single and multiple blockchain model evaluations of the AI-ACM system are expressed in Figures 6(a) and 6(b),
respectively. The simulation outcomes, namely, CPU utilization ratio, latency, and throughput of the AI-ACM system are evaluated under single and multiple blockchain models. As the number of blocks in the blockchain model increases, the security and system efficiency also increase. The simulation accuracy is further enhanced by artificial intelligence and blockchain models. The variation in the results with respect to time is plotted.

Table 2 indicates the credit evaluation of the AI-ACM system. The credit of IoV vehicles is varied from 10% to 100%, with a step size of 10%. As the credit of the IoV vehicle is increased, the respective travel distance and accuracy rate also increase. The AI-ACM system with artificial intelligence and the blockchain model enhances the computation and produces a lower traveling distance and higher assigning accuracy rate. The AI-ACM system ensures the highest accuracy.

Figures 7(a) and 7(b) show the credit analysis concerning travel distance and assign accuracy rate. The credit of IoV vehicles is varied from 10% to 100%, with a step size of 10%. The credit is indirectly related to the risk of the IoV vehicle. As the credit of the IoV vehicle is increased, the respective travel distance and accuracy rate also increase. The AI-ACM system with artificial intelligence and the blockchain model enhances the computation and produces a lower traveling distance and higher assigning accuracy rate. The AI-ACM system ensures the highest accuracy.

Figures 8(a) and 8(b) indicate the IoV analysis concerning travel distance and the assigned accuracy rate. The number of IoV vehicles for the simulation analysis is varied from 100 vehicles to 1000 vehicles with an incremental size of 100 vehicles. As the number of IoV vehicles increases, the network’s traffic and congestion result in poor performance. The blockchain model with three-tier architecture enhances the security of the AI-ACM system, and the artificial intelligence model enhances the system’s accuracy and produces better results.

The AI-ACM system is analysed, and the outcomes are compared in this section. The simulation outcomes such as average risk score, CPU utilization ratio, latency, throughput, travel distance, and accuracy rate regarding IoV vehicles and credit are analysed. The results indicate the effectiveness of the AI-ACM system with the blockchain and artificial intelligence in a vehicular environment.

\[
\text{Algorithm 1: Performance improvement algorithm.}
\]

For \( t = 0 \) to \( T \) repeat
- Select action with probability \( \epsilon \)
- Execute the action to generate block based on consensus method and block size
- Monitor reward \( R^t \) and move to the next phase
- Store the results \( S^t, Q^t, \) and \( R^t \)
- Sample the outcome of a minibatch by selecting random data
- Upgrade the network policy \( R^t (T^t, Q^t) \)
End for

**Table 1: Simulation analysis of the AI-ACM system.**

| Simulation time (ms) | CPU utilization ratio (%) | Latency (s) | Throughput (tps) |
|----------------------|---------------------------|-------------|-----------------|
| 5                    | 18                        | 24          | 54              |
| 10                   | 27                        | 13          | 58              |
| 15                   | 32                        | 16          | 63              |
| 20                   | 36                        | 23          | 61              |
| 25                   | 26                        | 18          | 59              |
| 30                   | 31                        | 21          | 74              |
| 35                   | 25                        | 25          | 63              |
| 40                   | 29                        | 16          | 59              |
| 45                   | 42                        | 18          | 68              |
| 50                   | 47                        | 31          | 73              |

**Table 2: Credit evaluation of the AI-ACM system.**

| Credit (%) | Travel distance (km) | Assign accuracy rate (%) |
|------------|----------------------|--------------------------|
| 10         | 24                   | 76                       |
| 20         | 27                   | 73                       |
| 30         | 32                   | 79                       |
| 40         | 38                   | 81                       |
| 50         | 25                   | 85                       |
| 60         | 27                   | 78                       |
| 70         | 31                   | 74                       |
| 80         | 35                   | 86                       |
| 90         | 28                   | 89                       |
| 100        | 42                   | 75                       |
Figure 6: (a) Single blockchain model evaluation of the AI-ACM system. (b) Multiple blockchain model evaluation of the AI-ACM system.

Figure 7: (a) Credit analysis with respect to travel distance. (b) Credit analysis concerning assigning accuracy rate.

Figure 8: (a) IoV analysis concerning travel distance. (b) IoV analysis concerning assigning accuracy rate.
5. Conclusion and Future Study

A risk-based authorization model is one of the model parameters that uses real-time and situational variables to determine access choices. This approach analyses each admin access for danger and dynamically grants or denies access depending on the projected risk rating. One of the most important phases in implementing a risk-based authorization architecture for the Internet is risk quantification. Even though the fuzzy inference system delivers precise and realistic risk estimates for access risk controls, the fuzzy inference system has significant drawbacks. The sustainability of the fuzzy inference system appears to be questionable since estimating potential risks of admission risk controls takes a long time. Moreover, fuzzy logic is incapable of learning or adapting to a new context.

This paper introduces an artificial intelligence-enabled access control mechanism (AI-ACM) with vehicle nodes and roadside units (RSUs) to overcome these issues. Roadside units (RSUs), which are frequently fixed, are essential for V2I deployment in order to collect data on the present situation of local traffic. As a result, V2I necessitates a broad coverage of RSUs in order to increase automobile environmental awareness. However, on the one hand, the deployment of stationary RSU is costly, and on the other side, it takes time to complete. While a vehicle is outside the radio coverage area of fixed RSUs, it can communicate with adjacent mobile RSUs to obtain traffic updates. Furthermore, incorporating learning capabilities allow the risk forecasting model to respond to differences in the IoV ecosystem, resulting in more precise and effective risk beliefs. The simulation outcomes such as average risk score, CPU utilization ratio, latency, throughput, travel distance, and accuracy rate regarding IoV vehicles and credit are analysed.

The suggested prototype was also assessed against a public health system (children’s clinic) using blockchain and AI. The findings indicate that the suggested model ensures dynamic, adaptable, and precise access choices using the situational and real characteristics encompassing the timeframe affiliated with each request. Artificial intelligence approaches are researched for the risk estimate process. Blockchains are predicted to deliver improved outcomes in terms of reliability and achievement of the vast dataset used in this study. Furthermore, research on combining risk and user trust factors to make access choices must be carried out.

Data Availability

The data are available on request from the corresponding author.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

[1] S. R. Pokhrel and J. Choi, “Improving tcp performance over WiFi for internet of vehicles: a federated learning approach,” IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 6798–6802, 2020.
[2] L. Song, G. Sun, H. Yu, X. Du, and M. Guizani, “Fbia: a fog-based identity authentication scheme for privacy preservation in internet of vehicles,” IEEE Transactions on Vehicular Technology, vol. 69, no. 5, pp. 5402–5415, 2020.
[3] A. Irshad, M. Usman, S. Ashraf Chaudhry, H. Naeqi, and M. Shaﬁq, “A provably secure and efficient authenticated key agreement scheme for energy internet-based vehicle-to-grid technology framework,” IEEE Transactions on Industry Applications, vol. 56, no. 4, pp. 1–4435, 2020.
[4] X. Zhang, K. P. Rane, I. Kakaravada, and M. Shabaz, “Research on vibration monitoring and fault diagnosis of rotating machinery based on internet of things technology,” In Nonlinear Engineering, vol. 10, no. 1, pp. 245–254, 2021.
[5] C. Li, H. Niu, M. Shabaz, and K. Kajal, “Design and implementation of intelligent monitoring system for platform security gate based on wireless communication technology using ML,” In International Journal of System Assurance Engineering and Management. Springer Science and Business Media LLC, vol. 13, no. 1, pp. 298–304, 2021.
[6] M. K. Loganathan, C. Ming Tan, B. Mishra, T. A. M. Msagati, and L. W. Snyman, “Review and selection of advanced battery technologies for post 2020 era electric vehicles,” In Proceedings of the 2019 IEEE Transportation Electriﬁcation Conference (ITEC-India), pp. 1–5, Bengaluru, India, December 2019.
[7] G. S. Sriram, “Edge computing vs. Cloud computing: an overview of big data challenges and opportunities for large enterprises,” International Research Journal of Modernization in Engineering Technology and Science, vol. 4, no. 1, pp. 1331–1337, 2022.
[8] J. Bhola, S. Soni, and G. K. Cheema, “Recent trends for security applications in wireless sensor networks – a technical review,” 2019 6th international conference on computing for sustainable global development (INDIACom), pp. 707–712, 2019.
[9] M. T. Abbas, A. Muhammad, and W. C. Song, “SD-IoV: SDN enabled routing for internet of vehicles in road-aware approach,” Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 3, pp. 1265–1280, 2020.
[10] M. F. Khan, F. Aadil, M. Maqsood, S. H. R. Bukhari, M. Hussain, and Y. Nam, “Moth ﬂame clustering algorithm for internet of vehicle (MFCA-IoV),” IEEE Access, vol. 7, pp. 11613–11629, 2019.
[11] J. Eze, S. Zhang, E. Liu, and E. Eze, “Cognitive radio-enabled internet of vehicles: a cooperative spectrum sensing and allocation for vehicular communication,” IET Networks, vol. 7, no. 4, pp. 190–199, 2018.
[12] A. K. Sutrula, P. Bagga, A. K. Das, N. Kumar, J. J. P. C. Rodrigues, and P. Lorenz, “On the design of conditional privacy preserving batch veriﬁcation-based authentication scheme for Internet of vehicles deployment,” IEEE Transactions on Vehicular Technology, vol. 69, no. 5, pp. 5535–5548, 2020.
[13] J. Kong, J. Li, B. Jiang, and H. Song, “Short-term trafﬁc ﬂow prediction in smart multimedia system for Internet of Vehicles based on deep belief network,” Future Generation Computer Systems, vol. 93, pp. 460–472, 2019.
[14] A. Sharif, J. P. Li, M. A. Saleem et al., “A dynamic clustering technique based on deep reinforcement learning for Internet of vehicles,” Journal of Intelligent Manufacturing, vol. 32, no. 3, pp. 757–768, 2021.
[15] Y. Zhang, R. Wang, M. S. Hossain, M. F. Alhamid, and M. Guizani, “Heterogeneous information network-based
content caching in the internet of vehicles," IEEE Transactions on Vehicular Technology, vol. 68, no. 10, pp. 10216–10226, 2019.

[16] G. Rathee, F. Ahmad, F. Kurugollu, M. A. Azad, R. Iqbal, and M. Imran, "CRT-BioV: a cognitive radio technique for blockchain-enabled internet of vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 4005–4015, 2021.

[17] T. M. Ghazal, R. A. Said, and N. Taleb, "Internet of vehicles and autonomous systems with AI for medical things," Soft Computing, pp. 1–13, 2021.

[18] S. R. Pokhrel, "Software defined internet of vehicles for automation and orchestration," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 6, pp. 3890–3899, 2021.

[19] A. U. Makarfi, K. M. Rabie, O. Kaiwartya et al., "Toward physical-layer security for Internet of Vehicles: interference-aware modeling," IEEE Internet of Things Journal, vol. 8, no. 1, pp. 443–457, 2021.

[20] C. Hu, W. Fan, E. Zeng et al., "Digital twin-assisted real-time traffic data prediction method for 5G-enabled internet of vehicles," IEEE Transactions on Industrial Informatics, vol. 18, no. 4, pp. 2811–2819, 2022.

[21] U. Chaudhary, A. Patel, A. Patel, and M. Soni, Survey Paper on Automatic Vehicle Accident Detection and Rescue System. Lecture Notes on Data Engineering and Communications Technologies, vol. 52, Springer, Singapore, 2021.

[22] C. Chen, H. Xiang, T. Qiu, C. Wang, Y. Zhou, and V. Chang, "A rear-end collision prediction scheme based on deep learning in the Internet of Vehicles," Journal of Parallel and Distributed Computing, vol. 117, pp. 192–204, 2018.

[23] Z. Ning, P. Dong, X. Wang et al., "Deep reinforcement learning for intelligent internet of vehicles: an energy-efficient computational offloading scheme," IEEE Transactions on Cognitive Communications and Networking, vol. 5, no. 4, pp. 1060–1072, 2019.

[24] M. Soni, B. S. Rajput, T. Patel, and N. Parmar, "Lightweight vehicle-to-infrastructure message verification method for VANET," in Lecture Notes on Data Engineering and Communications Technologies, K. Kotecha, V. Piuri, H. Shah, and R. Patel, Eds., vol. 52, Singapore, Springer, 2021.

[25] K. Jairath, N. Singh, M. Shabaz, V. Jagota, and B. K. Singh, "Performance analysis of metamaterial-inspired structure loaded antennas for narrow range wireless communication", scientific programming, vol., Scientific Programming, vol. 2022, Article ID 7940319, 1 page, 2022.

[26] G. Murugesan, T. I. Ahmed, M. Shabaz et al., "Assessment of mental workload by visual motor activity among control group and patient suffering from depressive disorder," Computational Intelligence and Neuroscience, vol. 2022, Article ID 8558489, 1 page, 2022.

[27] N. Ding, P. Prabhakar, A. Khosla, V. Jagota, E. Ramirez-Asis, and B. K. Singh, "Application of fuzzy immune algorithm and soft computing in the design of 2-DOF PID controller," Discrete Dynamics in Nature and Society, vol. 2022, Article ID 5608054, 1 page, 2022.

[28] X. Zhan, Z. H. Mu, R. Kumar, and M. Shabaz, "Research on speed sensor fusion of urban rail transit train speed ranging based on deep learning," Nonlinear Engineering, vol. 10, no. 1, pp. 363–373, 2021.

[29] A. Irshad, M. Sher, S. A. Chaudhry, Q. Xie, S. Kumari, and F. Wu, "An improved and secure chaotic map based authenticated key agreement in multi-server architecture," Multimedia Tools and Applications, vol. 77, no. 1, pp. 1167–1204, 2018.

[30] L. Yan, J. L. Webber, A. Mehboobniya et al., "Distributed optimization of heterogeneous UAV cluster PID controller based on machine learning," Computers & Electrical Engineering, vol. 101, Article ID 1080599, 2022.

[31] E Guo, V. Jagota, M. E. Makithka, and P. Kumar, "Study on fault identification of mechanical dynamic nonlinear transmission system," Nonlinear Engineering, vol. 10, no. 1, pp. 518–525, 2021.

[32] G. S. Saja, W. James, and J. Flores, Deep learning components project managers need to implement to ensure the success of projects in information technology enterprises, University of the Cumberlands, Williamsburg, U S A, 2021.

[33] S. Zhang, K. Srividya, I. Kakaravada et al., "A global optimization algorithm for intelligent electromechanical control system with improved filling function," Scientific Programming, vol. 2022, Article ID 3361027, 1 page, 2022.

[34] J. Bhola and S. Soni, "A study on research issues and challenges in WSAN," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), vol. 2016, pp. 1667–1671, 2016.

[35] S. Yaqoob, A. Ullah, M. Akbar, M. Imran, and M. Shaob, "Congestion avoidance through fog computing in internet of vehicles," Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 10, pp. 3863–3877, 2019.

[36] M. N. Kumar, V. Jagota, and M. Shabaz, "Retrospection of the optimization model for designing the power train of a formula student race car. Scientific programming," Scientific Programming, vol. 2021, Article ID 9465702, 1 page, 2021.

[37] L. Du, L. Zhang, X. Tian, and J. Lei, "Efficient forecasting scheme and optimal delivery approach of energy for the energy Internet," IEEE Access, vol. 6, pp. 15026–15038, 2018.

[38] L. Nkenyereye, C. H. Liu, and J. Song, "Towards secure and privacy preserving collision avoidance system in 5G fog based Internet of Vehicles," Future Generation Computer Systems, vol. 95, pp. 488–499, 2019.

[39] A. Hbaieb, S. Ayed, and L. Chaari, "A survey of trust management in the Internet of Vehicles," Computer Networks, vol. 203, Article ID 108558, 2022.

[40] R. Nouh, M. Singh, and D. Singh, "SafeDrive: hybrid recommendation system architecture for early safety predication using Internet of Vehicles," Sensors, vol. 21, no. 11, p. 3893, 2021.

[41] Y. Song, Y. Fu, F. R. Yu, and L. Zhou, "Blockchain-enabled Internet of Vehicles with cooperative positioning: a deep neural network approach," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3485–3498, 2020.

[42] C. Sonmez, C. Tunca, A. Ozgovde, and C. Ersoy, "Machine learning-based workload orchestrator for vehicular edge computing," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 4, pp. 2239–2251, 2021.