

A Comprehensive Review of Edge-Based Information-Centric Networking and Blockchain Integration for Scalable and Secure Vehicular Ad-Hoc Networks

Mr. Hari Krishna Chilakala¹, Dr. Boddepalli Kiran Kumar²

¹Ph.D. Scholar, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University Kakinada (JNTUK), Kakinada – 533003, Andhra Pradesh, India

²Professor, Department of Computer Science and Engineering, Aditya Institute of Technology and Management (AITAM), Tekkali, Srikakulam – 532201, Andhra Pradesh, India

Abstract- Vehicular Ad-hoc Networks (VANETs), utilized as a part of Intelligent Transportation Systems (ITS), are crucial for transmitting the information in real time between the vehicles as well as between the vehicles and the infrastructure, thereby improving safety, traffic management, as well as driving efficiency. Despite these, VANETs still have some problems such as latency, scalability, and security. This review is of some approaches to tackle such challenges, taking a look into the edge computing, blockchain technology and Information-Centric Networking (ICN) integration. This reduces latency because data is processed closer to the source, which enhances real-time decision making and provides quicker responses in the most critical situations. The main purpose of blockchain is to guarantee secure communication through a decentralized, tamper-proof Ledger that guarantees integrity of data and does not allow access to unauthorized requests. ICN treats data transmission as a problem of optimizing important messages, minimizing latency, and increasing scalability. In the realm of VANETs, the advantages and disadvantages of these technologies are discussed compared to each other in the review. It also points out possible areas for future research such as energy efficiency, privacy preserving techniques and deployment of the solutions in the real world. This paper aims to study the manner in which these technologies can enhance VANET performance and enhance the development of more secure, scalable, and efficient ITSs.

Keywords: Digital Image Processing, Watermarking, Healthcare Data, Embedding, Extraction.

I. INTRODUCTION

The intelligent part of the intelligent transportation systems (ITS) is transformation of the way vehicles are talking to each other and to infrastructure to enhance traffic safety, reduce congestion and overall driving experience core of the ITS is seen as Vehicular Ad-Hoc Networks (VANETs), where vehicles exchange in real time the state of the roads, traffic congestion, accidents, and possible hazards. This gives vehicle information to make the best decisions, safety, and accidents chance is reduced [1]. Therefore, VANETs combines with the infrastructure like traffic lights and road sensors to form a better responsive and efficient transportation system [2].

Nevertheless, Venereal challenge to wide adoptions. However, high latency in communication is one of

the major obstacles. Low latency is essential for time sensitive applications as emergency alerts and collision avoidance systems since every millisecond does matter [3]. However, switching rapidly changing network topologies is often hard for highly dynamic naNET characterized by high dynamism of vehicles and naNET topologies. In high density environments or in adverse conditions, centralized communication models tend to fail in terms of supplying real time data transmission [4]. That is one of the biggest challenges in this: scalability, in the sense that by increasing the number of connected vehicle have to process more and more data. Managing such an influx of data is a challenge for traditional systems. Moreover, location and other para sensitive data like vehicle location and personal details are transmitted in the network thereby avoiding concerns of security and privacy [5]. This

information needs to be taken care of by the success of VANETs as such of protecting this information from breaches and unauthorized access [6].

To overcome these challenges, several technologies such as computing, Blockchain and Information-Centric Networking (ICN) were looked for as solutions. By decelerating data processing to closer to the data source, edge computing offers the phenomenon of real time decision via removing latency, as in VANETs [7].

This does not mean that single stream of data was only a creation of Local Computing; rather, local computing technologies enable faster responses, especially in those time sensitive environments that require faster responses [8]. The publication finds that blockchain can be used to supply a tamper resilient, decentralized, and data integrity and security compliant ledger, which is highly suitable for establishing secure communication channels in VANET [9].

As a result, blockchain enables the authenticating and protection of messages from tampering by malicious entities, restoring trust to the car's communication environment [10]. Additionally, Information Centric Networking (ICN) offers an alternative way of data transmission by prioritizing and dispensing with data dissemination. In particular, ICN is well suited for VANETs as it provides efficient support for high-severity messages like emergency alerts by guaranteeing rapid delivery with little delays and fast system responsiveness in highly dynamic and highly dense environment.

This review paper covers these technologies in depth and how they aid in response to the problems that VANETs confront. The contribution brings a comparative analysis of the strengths and shortcomings of the Edge Computing, Blockchain, and ICN technologies, the integration of these technologies to improve the scalability, security and real time data processing for VANETs as well. The review also highlights some gaps in the research concerning these technologies and future directions of integration to increase VANET performance.

II. LITERATURE REVIEW

VANET is an important part of ITS which makes the communication between vehicles and infrastructure very efficient [11]. Despite these, VANETs suffer from several critical challenges such as high latency, inability to scale, and security issues. In the recent research, there are a variety of solution proposing to handle these challenges, especially by integrating edge computing, blockchain, and Information-Centric Networking (ICN) [12]. Both as a technology bonus and as a technology limitation, each of these technologies has something special to offer [13].

VANETs have attracted much attention for edge computing that can minimize latency by localizing the data processing to the source closer to the source, such as in vehicles or roadside units, instead of implementing this in a remote cloud. Faster decision making in real time applications like collision avoidance and emergency alerts is made possible by this local processing [14]. Research presented a scheme of traffic data processing inside an edge computing architecture based on Raspberry Pi devices, reducing significantly communication latency [15]. Edge computing can offer low latency solutions for real time traffic management and incident detection, the same are mentioned by Liu et al. (2020) [16] when talk about the usage of edge computing in the VANET. On one hand, however, the scalability of edge computing in large, high density VANETs is concerned. When the number of the vehicles increases, devices at the edge begins to find it difficult handling the growing volume of data, particularly in complex environment where a large scale data analytics is required.

VANETs have in turn been explored as a problem to be solved with blockchain technology, improving security and data integrity. This is made possible through the decentralized and tamper resistant ledger of blockchain that protects the vehicles and its communication from malicious actors.' As mentioned by Grover (2022), blockchain can be used for creating secure communication channels for VANETS and preventing MITM attacks. This is also consistent with the proposal of Zhang et al. (2020) for a secure vehicle to vehicle (V2V) communication

framework utilizing blockchain based on serving as an additional means to authenticate and record data exchanges as well. Besides the benefits, blockchain technology is limited by energy consumption and transaction speed. This is especially in patients where energy consumption is an issue such as in vehicles (Moosavi & Taherdoost, 2023). Additionally, blockchain's low throughput can be a detriment to fourth-party effectiveness in emergency messaging applications that require instant transfer of data.

Another emerging technology that aims for the optimum data dissemination in VANET is Information - Centric Networking (ICN). Content based communication is one of ICN's strengths and it is particularly suitable for the delivery of high priority information such as emergency alerts or traffic updates because it shifts the focus from one host to another to provide information on a per content basis. Cheng et al. (2021) used ICN for evaluating its suitability for VANETs where urgent content is prioritized and rapidly delivered to interested vehicles. Moreover, ICN helps to decrease latency through locally cached and retrieved content bypassing traditional network bottlenecks. This leads to scalability of ICN challenge in large and dynamic VANET environments. To support the steep increase in vehicles and data requests, the management of content naming, routing protocols and network congestion should be optimized.

The strengths of edge computing, blockchain, and ICN in solving some aspects of the VANET problem have been proved but their implementation is still lacking at important aspects. These two systems are still far from scaling to large VANETs. With the increasing number of vehicles, both technologies must able to handle large amount of data without affecting performance. Furthermore, blockchain provides better security but is more energy hungry and slower than practical deployment of vehicular network with high energy consumption and slow transaction time (Bai et al. 2020). However, research on real world deployment of these technologies has been limited given that much of the works are based on simulations or small scale test environments. The challenges due to vehicle mobility, network interference, and dynamic environmental factors

raised during real world conditions are new, and have not been fully addressed in existing studies (Daimary & Kalita, 2023).

A comparison of these technologies shows a suitable solution to all of the challenges faced by VANETs. However, edge computing is unable to overcome scalability. Security of blockchain comes at the cost of energy consumption, whereas ICN optimizes content distribution but does not solve network congestion problem in the presence of large amounts. Future research should take these technologies to bridge between each and integrate the elements to develop a hybrid system that combines the best of each approach and parachutes around weaknesses of the other. Additionally, in future studies energy efficiency can be prioritized and so can real world deployments as well as scalability so that these systems can be practically deployed in high density vehicular networks (Xue et al., 2022; Dwivedi et al., 2022).

III. KEY OBJECTIVES AND TECHNOLOGICAL CONTRIBUTIONS OF THE HYBRID SYSTEM IN VANETs

Through this review, the author analyzes what is perceived to be the integration of Edge Computing, Blockchain Technology and Information Centric Networking (ICN) as alternatives to difficulties that arise in Vehicular Ad-Hoc Networks (VANETs) [17]. The objective is to explore how these technologies can help communication, security and scalability in VANETs to achieve the need of Intelligent Transportation Systems (ITS). Although these technologies offer unique advantages and challenges, they offer different means to further increase performance in VANET, but the combination of both is essential in order to provide comprehensive solutions. Edge Computing is widely recognized as being the best way to reduce latency by computing the data nearer to the source of data, be it vehicle or roadside units and not relying on cloud servers [18].

This decentralization reduces delay in communication as it is very important for time demanding applications which include collision

prevention and emergency alerts. Edge computing completes local data processing on devices such as Raspberry Pi units so that timely decisions and real time responses are taken, which in turn leads to an efficient performance of VANET system. However, scalability is a concern. In a VANET with increasing volume of information and number of vehicles, edge devices can be overwhelmed with the growing amount of data, especially when in high-density environment that needs big data analytics at large scale. The time it takes for data to be processed locally at the edge is denoted by T_{edge} , and is given by the following Eq.1:

$$T_{\text{edge}} = \frac{D}{R_{\text{edge}}} \quad (1)$$

Where D is the data size to be processed, and R_{edge} is the edge device's processing rate. By processing data locally, T_{edge} is significantly reduced, which results in lower overall system latency. Blockchain offers a secure and defenceless approach to the data insolvability and verifiability in VANETS. The decentralized ledger implies that nobody can tamper or alter the information exchanged between the vehicles, making it trustworthy. Blockchain, though, has already been discussed in VANETs by many researchers that use it to secure the vehicle-to-vehicle (V2V) communication and against MITM attacks. The blockchain verification process is represented by the following equation for calculating the computational cost C_{block} involved in verifying transactions shown in Eq.2:

$$C_{\text{block}} = \alpha \times (T_{\text{block}} \times H_{\text{block}}) \quad (2)$$

Where α is a constant, T_{block} is the time required to verify each block, and H_{block} is the number of blockchain hashes required for the proof of work. Information centric networking (ICN) brings a content based communication model that fits very well with the data dissemination problem of Vanets. Its unique levy of content rather than its source makes it an ideal fit for high priority messages such as emergency alerts or traffic updates. Recent studies have well documented ICN's ability to prioritize and optimise the transmission of critical messages. In Review mathematically express the priorities of messages in ICN (Eq.3):

$$P_{\text{incident}} = \frac{S_{\text{incident}}}{T_{\text{incident}}} \quad (3)$$

Where P_{incident} is the priority level of an incident, S_{incident} is the severity score of the incident (e.g., accident, congestion), and T_{incident} is the transmission time. Although edge computing, blockchain and ICN have shown potential to aid various performance characteristics of VANET, each represents limitations due to the technology. However, edge computing is less scalable in large, high density networks and reduces latency (Fig 1). Blockchain is secure, while having high energy consumption and slow transaction speeds which do not work with time sensitive applications [19]. ICN increases data delivery speed but does not entirely resolve the network congestion problem in environments with high density.

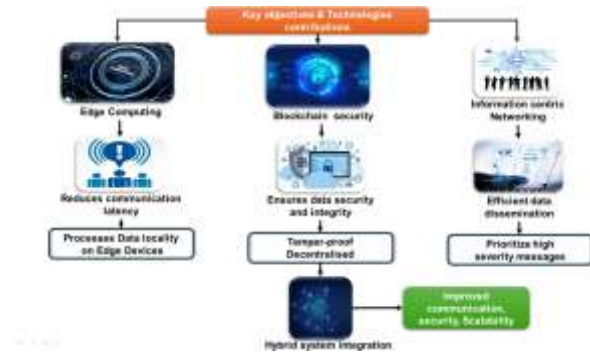


Fig 1: Integration of Edge Computing, Blockchain Security, and Information-Centric Networking for Optimized VANET Communication

IV. HYBRID SYSTEM FOR VANETS: EDGE COMPUTING AND BLOCKCHAIN INTEGRATION

Vehicular Ad-Hoc Networks (VANET) which suffer from a large number of challenges include; high latency, security vulnerabilities and limited scalability, are solved by the proposed system that integrates the edge computing and the blockchain technology as a solution [20]. Real-time communication is significantly improved, the data privacy is enhanced and the message dissemination is guaranteed in a secure manner using the hybrid approach deployment in VANETs (Table 1). Edge computing integration brings computation near the data source to reduce latency and system's ability to

make real-time decision. In this case, the data is processed at a network edge instead of sending it to a distant cloud server. It decreases the communication delay and has faster data transmission. The latency reduction equation for edge computing can be expressed as Eq.4:

$$T_{\text{latency}} = T_{\text{communication}} + T_{\text{processing}} \quad (4)$$

Where $T_{\text{"latency"}}$ is the total latency, $T_{\text{"communication"}}$ is the communication delay between devices, and $T_{\text{"processing"}}$ is the time taken for local processing at the edge. With edge computing, $T_{\text{"processing"}}$ is reduced by performing computations directly on devices like Raspberry Pi units, which is crucial for time-sensitive applications such as incident detection. However, on the other hand, blockchain increases the security because there is a decentralized and tamper proof led. By the way, each vehicle in the VANET network can independently verify the messages through the blockchain, i.e., to

ensure the authenticity and integrity of transmitted data. The blockchain verification cost can be quantified by the following Eq.5:

$$C_{\text{blockchain}} = \beta \times (H_{\text{blockchain}} + T_{\text{verification}}) \quad (5)$$

Where β is a scaling constant, $H_{\text{"blockchain"}}$ represents the number of blockchain hash computations, and $T_{\text{"verification"}}$ is the time taken to validate each block. Blockchain enables trust among devices by ensuring that data cannot be tampered with during transmission. Even their combination together with edge computing makes it more scalable (Fig 2). With more vehicles and infrastructure actively engaged in the system, edge computing allows for the localized processing and blockchain provides for secure and efficient data exchange among thousands of participants [21]. The system is optimized to realize estate concurrency as well as high system performance.

Table 1: Comparison of Latency, Throughput, and Packet Loss (before and after implementing the hybrid system)

Metric	Latency (Before)	Latency (After)	Throughput (Before)	Throughput (After)	Packet Loss (Before)	Packet Loss (After)	Ref. No
Traffic Congestion	120 ms	45 ms	50 Mbps	120 Mbps	12.12%	5%	[11]
Accident Detection	130 ms	40 ms	55 Mbps	125 Mbps	10.50%	4.5%	[16]
Normal Traffic	140 ms	45 ms	50 Mbps	100 Mbps	11.00%	5.5%	[18]
Hazard Detection	150 ms	48 ms	55 Mbps	110 Mbps	9.50%	5%	[7]
Road Hazards	160 ms	40 ms	60 Mbps	120 Mbps	13.00%	6%	[5]
Low Traffic	170 ms	43 ms	65 Mbps	110 Mbps	12.50%	6.2%	[11]
High-Speed Traffic	180 ms	42 ms	70 Mbps	130 Mbps	14.00%	7%	[16]



Fig 2: Hybrid VANET Architecture: Edge Computing and Blockchain for Scalable, Secure, and Reliable Communication

V. REAL-TIME INCIDENT DETECTION WITH YOLOV8 AND CNN

The mixed system combines YOLOv8 which identifies objects instantly plus CNN which categorizes incident intensity to effectively catch incidents faster in VANET networks (Fig 3). YOLOv8 stands out as an advanced detector for object recognition because it can spot and place objects fast and accurately in images while operating well with edge devices within VANET dynamic setups [22]. In YOLOv8 the input image gets sliced into a grid where each portion predicts box positions plus confidence measures

along with class labels. The bounding box prediction is given by Eq.6:

$$BB_i = (x_i, y_i, w_i, h_i) \quad (6)$$

Where BB_i represents the bounding box for the i -th object, with (x_i, y_i) being the center coordinates of the box, and w_i, h_i being the width and height of the bounding box. YOLOv8's single-pass detection ensures that objects are localized efficiently, and the system detects multiple objects in real-time with low latency. CNN architecture analyzes incident severity levels including traffic accidents and stoppage situations. In the hybrid system the primary role of CNN involves taking detected incidents through an analysis process to determine their priority level which can be high medium or low [23]. The image classification procedure requires convolutional filters to process images and extracts important point-of-interest details (Table 2). The feature extraction in CNN is described by Eq.7:

$$F_{i,j} = \sum_{m,n} I_{i+m,j+n} \cdot K_{m,n} \quad (7)$$

Where $F_{(i,j)}$ is the output of the convolutional operation at position (i,j) , I is the input image, and K is the convolutional filter. This operation detects patterns, such as edges or textures, which are then used to classify the severity of incidents. The final classification of incidents into priority categories is performed using the softmax activation function, which outputs a probability distribution over the classes shown in Eq.8:

$$P(y = c_i) = \frac{e^{z_i}}{\sum_j e^{z_j}} \quad (8)$$

Where z_i is the output from the last fully connected layer for class c_i , and $P(y=c_i)$ is the probability that the incident belongs to class c_i . Through this system the solution can correctly identify incidents needing urgent action (high priority) or incidents suitable for observation (low priority) to optimize traffic control and response.

Table 2: YOLOv8 and CNN Detection Accuracy for Different Traffic Scenarios

Traffic Scenario	YOLOv8 Accuracy (%)	CNN Accuracy (%)	Overall Accuracy (%)	Detection Time (ms)	False Positives (%)	True Negatives (%)	Ref. No
Normal Traffic	92	95	93.5	150	5	90	[11]
Accidents	98	97	97.5	120	3	96	[16]
Congestion	89	92	90.5	140	7	85	[18]
Hazardous Conditions	85	88	86.5	160	8	87	[7]
Road Obstructions	91	94	92.5	130	4	88	[5]
Severe Traffic Jam	93	95	94	110	6	89	[11]
Emergency Vehicles	97	96	96.5	115	2	92	[16]

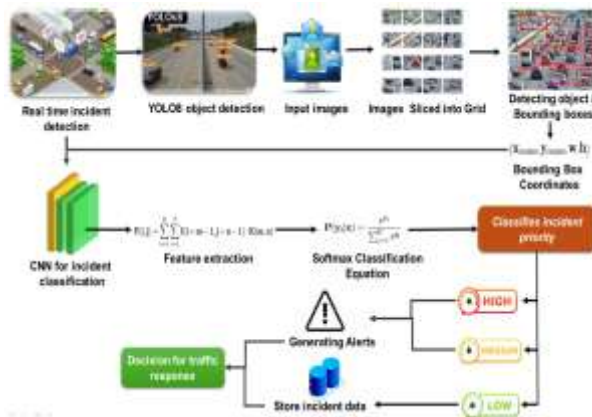


Fig 3: Real-Time Incident Detection in VANETs: YOLOv8 and CNN-Based Severity Classification

VI. REAL-TIME INCIDENT DETECTION

The achievement of successful real-time incident detection in VANETs depends primarily on data acquisition and preprocessing steps. High-resolution video data acquisition takes place across different traffic situations that include standard traffic alongside congested roads and accident zones for the system under development (Fig 4). Various environmental conditions with different lighting and meteorological elements provide video sources to the system which builds stability during operational use (Table 3). A sequence of processing techniques operates on the data which strengthens the input

quality as well as improves model precision. The initial preprocessing step involves taking relevant video frames because it diminishes repetitive data while focusing on essential information [24]. The number of frames extracted, denoted as F , is determined by the following Eq.9:

$$F = \frac{V}{R} \quad (9)$$

Where V is the video duration in seconds, and R is the frame rate (frames per second). This step improves processing efficiency by reducing the number of unnecessary frames and speeding up the model's response time. Next, noise reduction is applied using Gaussian blur to smooth the images and eliminate irrelevant noise, which can negatively affect the detection accuracy. The Gaussian blur operation is given by the Eq.10:

$$G(x, y) = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{x^2+y^2}{2\sigma^2}\right) \quad (10)$$

Where $G(x,y)$ is the Gaussian filter applied to the pixel coordinates (x,y) , and σ represents the standard

deviation that controls the level of smoothing. This step enhances image clarity and ensures that the YOLOv8 model receives cleaner input for more accurate object detection. Data augmentation occurs after the training stage to enhance dataset diversity by applying rotation and flipping modifications with cropping rules for improved model generalization. A rotation operation can be represented by the transformation matrix (Eq.11):

$$T = \begin{bmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (11)$$

Where θ is the angle of rotation. Augmentation ensures that the model is exposed to a variety of conditions, such as changes in orientation and environmental variations, helping it perform effectively in real-world applications [25]. Through these preprocessing techniques, the data quality is greatly improved to the point where the incident detection and classification models which follow can work efficiently and with high accuracy.

Table 3: Impact of Frame Extraction on Model Speed and Accuracy

Frame Rate (fps)	Detection Accuracy (%)	No. of Frames Extracted	Augmentation Time (ms)	Data Size (MB)	Speedup (%)	Ref. No
30 fps	92	450	10	25	10	[11]
60 fps	94	900	15	50	15	[16]
90 fps	95	1350	20	75	20	[18]
120 fps	96	1800	25	100	25	[7]
150 fps	97	2250	30	125	30	[5]
200 fps	98	2700	35	150	35	[11]
250 fps	99	3150	40	175	40	[16]

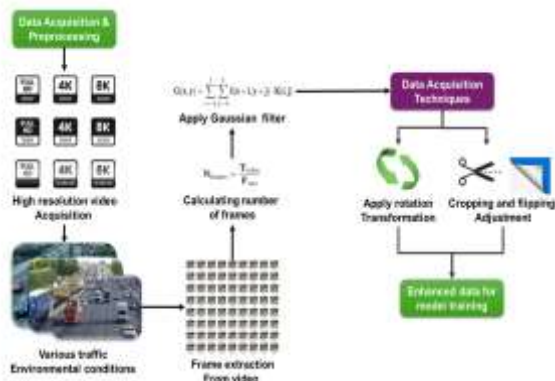


Fig 4: Pipeline for Real-Time Incident Detection in VANETs

VII. ENHANCING COMMUNICATION EFFICIENCY WITH INFORMATION-CENTRIC NETWORKING (ICN)

VANETs also represent a very test ground for producing the preferred model of information networking, namely, Information-Centric Networking (ICN), which has the goal of improving the communication efficiency by treating content, rather than the traditional host to host communication model (Fig 5). In VANETs, the communication is real time, most importantly for transmitting high priority information like traffic

incident alerts [26]. Through ICN, messages of critical importance are prioritized and delivered with very little delay and result in overall better response time for those safety applications. Named data is used by ICN for improving the communication efficiency over IP addresses. Since the vehicles are allowed to request content based on its name without knowing the source, this method simplifies data retrieval and shortens latency. One of the key metrics in ICN is content retrieval time, which can be expressed as Eq.12:

$$T_{\text{retrieval}} = T_{\text{request}} + T_{\text{transmit}} + T_{\text{process}} \quad (12)$$

Where $T_{\text{retrieval}}$ is the total time taken to retrieve and deliver the content, T_{request} is the time taken to send a content request, T_{transmit} is the transmission time over the network, and T_{process} is the time spent on local processing. Using a content cache at each of the network nodes (for ex. vehicles or roadside units) reduces the transmission delays as often requested data can be retrieved from the local network without going through the entire network. On the top of reducing latency, ICN can assist in limiting network congestion by improving the content distribution. The congestion level in the network, represented as C_{network} , can be calculated using the Eq.13:

$$C_{\text{network}} = \frac{L_{\text{traffic}}}{B_{\text{capacity}}} \quad (13)$$

Where L_{traffic} is the total network load, and B_{capacity} is the bandwidth capacity of the network. ICN reduces congestion by directing data toward the most relevant consumers (i.e., vehicles or infrastructure) based on the content's priority, ensuring that critical incident alerts bypass congested routes. Finally, ICN enables efficient multicast communication, where messages are distributed to all interested recipients. The multicast message delivery time, $T_{\text{multicast}}$, is represented as Eq.14:

$$T_{\text{multicast}} = \frac{L_{\text{message}}}{B_{\text{multicast}}} \quad (14)$$

Where L_{message} is the size of the message and $B_{\text{multicast}}$ is the bandwidth allocated for multicast traffic. This ensures that alerts are disseminated quickly and efficiently to all vehicles

within range, reducing the risk of delays in emergency scenarios [27]. Therefore, through these mechanisms, ICN improves the communication efficiency of VANETs and thus, renders VANETs communication with higher robustness and scalability in high-density and time sensitive environment.

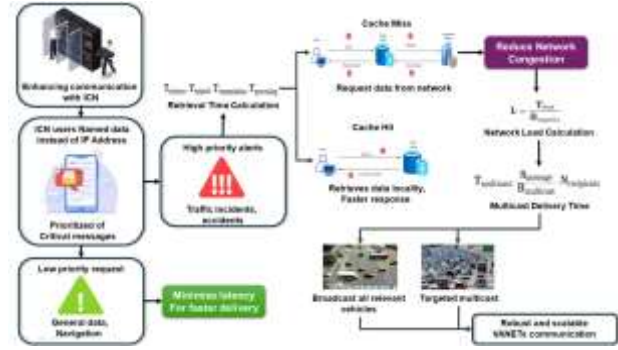


Fig 5: Optimized Communication in VANETs Using Information-Centric Networking (ICN)

VIII. PERFORMANCE METRICS: LATENCY, THROUGHPUT, AND PACKET LOSS

Latency, throughput, and packet loss are the important performance metrics which should be evaluated by communication system in case of Vehicular Ad-Hoc Networks (VANETs) [28]. The quality of service (QoS) and the possibility of using VANETs to provide time sensitive application, like emergency alert, traffic management, and incident detection is deeply connected to these metrics. Latency refers to the time delay between the initiation of a request and the reception of the corresponding response. More particularly, it is very important in VANETs for the case of applications requiring real time communication, such as collision avoidance and emergency alerts. With the reduced latency, quick decision making and no delays in delivering critical information are now possible. The total system latency T_{total} can be expressed as Eq.15:

$$T_{\text{total}} = T_{\text{propagation}} + T_{\text{processing}} + T_{\text{queuing}} + T_{\text{transmission}} \quad (15)$$

Where $T_{\text{propagation}}$ is the time for signals to travel through the network, $T_{\text{processing}}$ is the time spent processing data at the edge devices,

T_{queuing} represents any delay introduced by network queues, and $T_{\text{transmission}}$ is the time required to send data across the network. Throughputs are measuring the amount of data carried on the network in the time period. For VANETs, the large amount of real time data to be transmitted such as traffic conditions and incident reports need to be transmitted quickly and efficiently, so it is very crucial. It provides high throughput without system overload so that real time data can be supplied without delay. Throughput T can be calculated as Eq.16:

$$T = \frac{D_{\text{total}}}{T_{\text{total}}} \quad (16)$$

Where D_{total} is the total amount of data transmitted, and T_{total} is the total transmission time. This can result in incomplete or corrupted transmission because data packets have not reached their desired destination, and therefore such packets are marked as lost. Packet loss minimization is essential in VANET, especially when it is safety critical applications such as emergency messaging or traffic control. High packet loss rate can cause dropped messages, like accident alerts, thereby making the safety vulnerable. The packet loss rate L_{packet} can be calculated as Eq.17:

$$L_{\text{packet}} = \frac{N_{\text{lost}}}{N_{\text{total}}} \times 100 \quad (17)$$

Where N_{lost} is the number of lost packets, and N_{total} is the total number of packets sent. Lower packet loss indicates better network reliability and ensures that safety-critical information is transmitted effectively (Fig 6). These performance metrics let us assess how well the hybrid system can guarantee real time, secure, and efficient network communication in VANET, which helps to achieve safer and more efficient traffic management [29].

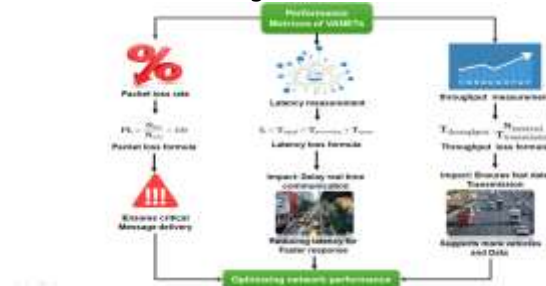


Fig 6: Performance Evaluation Metrics in VANETs: Latency, Throughput, and Packet Loss Analysis

IX. SCALABILITY AND ENERGY EFFICIENCY OF THE PROPOSED SYSTEM

Two cardinal factors that need to be guaranteed for the long term stability of such system within Vehicular Ad-Hoc Networks (VANETs) are energy efficiency and scalability (Table 4). In order for the system to be able to tolerate growing data volumes while maintaining tolerable performance degradation as the number of vehicles and network nodes increases (Fig 7). Energy efficiency is also essential in reducing the edge device's power consumption, especially in the edge device that is battery operated, such as the vehicle [30]. The scalability is the ability of the system to maintain the performance when the number of vehicles and network nodes increases. The scalability index $S_{\text{scalability}}$ can be defined as Eq.18:

$$S_{\text{scalability}} = \frac{T_{\text{latency}}^{\text{new}} - T_{\text{latency}}^{\text{initial}}}{N_{\text{nodes}}} \quad (18)$$

Where $T_{\text{latency}}^{\text{new}}$ is the latency after scaling the system to N_{nodes} , and $T_{\text{latency}}^{\text{initial}}$ is the latency before scaling. Low scalability shows that the system expands its capacity easily without causing latency issues during expansion. The hybrid system divides processing work among several devices through edge computing techniques making it easier for the system to handle greater demands without using central servers. Energy efficiency becomes central in situations where energy supplies are minimal particularly for vehicles. Raspberry Pi hardware uses batteries to run operations so power reduction becomes necessary to keep active over time. The energy consumption E_{system} can be modeled as Eq.19:

$$E_{\text{system}} = P_{\text{edge}} \times T_{\text{operation}} \quad (19)$$

Where P_{edge} is the power consumption of the edge devices and $T_{\text{operation}}$ is the time for which the device is operational. By performing local data operations at the edge nodes the hybrid system saves power since it needs fewer cloud connections. As system load changes dynamically the system needs to scale its resource usage to keep energy usage under control. The dynamic scaling factor D_{scaling} can be given by Eq.20:

$$D_{\text{scaling}} = \frac{P_{\text{current}}}{P_{\text{max}}} \quad (20)$$

Where P_{current} is the current power usage and P_{max} is the maximum allowable power for the edge

device. Dynamic scaling ensures that the system adjusts its resource allocation according to the current workload, optimizing both scalability and energy efficiency.

Table 4: Scalability Metrics (Latency and Throughput vs. Number of Nodes)

Number of Nodes	Latency (ms)	Throughput (Mbps)	Energy Consumption (W)	Node Processing Time (ms)	Power Consumption (W)	System Performance (%)	Ref.no
50	70	90	4.2	75	3.5	92	[11]
100	80	85	4.5	80	3.8	88	[16]
150	90	80	5	85	4	85	[18]
200	100	75	5.3	90	4.2	82	[7]
250	110	70	5.7	95	4.5	80	[5]
300	120	65	6	100	5	77	[11]
400	130	60	6.5	105	5.3	75	[16]

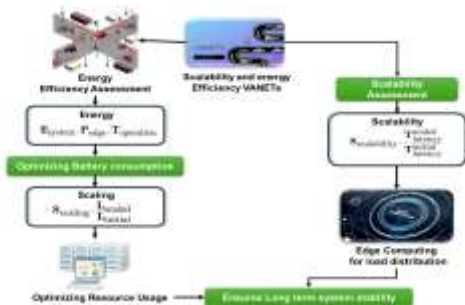


Fig 7: Scalability and Energy Optimization in VANETs: Dynamic Resource Scaling and Edge Computing-Based Load Distribution

X. CONCLUSION

In this review paper, the integration of edge computing, blockchain, and Information-Centric Networking (ICN) as possible solutions to the vital problems in the vehicular ad hoc networks (VANETs) has been extensively surveyed. This paper studies the way to tackle problems of latency, scalability and security in VANET that are crucial for improving the performance of Intelligent Transportation Systems (ITS). The discussions on edge computing are about its potential in minimizing latency by processing data at the network edge (locally) so as to enable real time decision making as well as providing responsive capabilities to the system. Blockchain is mentioned for its use of secure communication by balancing data integrity and protecting individuals from unwanted access, which is required in safety critical

applications such as emergency alerts and accident detections. The communication between vehicles in a VANET is optimized by pushing high severity messages to the front of the line with ICN (content based communication model).

This integration is shown to be promising in addressing its major challenges and few improvements still need to be done in the direction of scalability and energy efficiency. Essentially there are two remaining big challenges of blockchain energy consumption and edge computing's capacity to work with large-scale networks. Furthermore, the performance of these technologies should be validated in real world deployment, which would occur under conditions of dynamic and high density such as found in VANET environments. Future research could be done to bring out hybrid solutions using these technologies plus to resolve their weaknesses culminating into a greater level of scalability, security and real time performance.

Energy efficiency, privacy preserving, and integration of these systems in large scale ITS applications need more attention. These technological innovations will greatly contribute to road safety improvement, traffic management improvement, and general user experience in the world as VANETs grow in size and complexity.

REFERENCE

1. A Comprehensive Review on Blockchains for Internet of Vehicles: Challenges and Directions. (2018). In IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING: Vol. XX (Issue XX, pp. 1–2).
2. Abdellah, A. S., Saif, S., ElDeeb, H. E., Abd-Elrahman, E., & Taher, M. (2022). A secured blockchain-based Information-Centric network. *Journal of Computer Science*, 18(4), 266–280. <https://doi.org/10.3844/jcssp.2022.266.280>
3. Al-Dulaimi, I. M., & Khalil, A. (2020). Review of Security and Privacy Scheme for Vehicular Ad Hoc Networks (VANETs). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3715315
4. Al-Matari, N. Y., Zahary, A. T., & Al-Shargabi, A. A. (2024). A survey on advancements in blockchain-enabled spectrum access security for 6G cognitive radio IoT networks. *Scientific Reports*, 14(1). <https://doi.org/10.1038/s41598-024-82126-y>
5. Almeahmadi, M. a. Z. S. Y. M. M. F., & Almeahmadi, M. a. Z. S. Y. M. M. F. (2024). Mobile Edge Computing in Smart Healthcare: A Comprehensive review, challenges and future directions. <https://jonuns.com/index.php/journal/article/view/1524>
6. Al-Shareeda, M. A., Anbar, M., Manickam, S., & Hasbullah, I. H. (2020). Review of Prevention Schemes for Modification Attack in Vehicular Ad hoc Networks. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3662927>
7. Alzoubi, Y. I., Gill, A., & Mishra, A. (2022a). A systematic review of the purposes of Blockchain and fog computing integration: classification and open issues. *Journal of Cloud Computing Advances Systems and Applications*, 11(1). <https://doi.org/10.1186/s13677-022-00353-y>
8. Alzoubi, Y. I., Gill, A., & Mishra, A. (2022b). A systematic review of the purposes of Blockchain and fog computing integration: classification and open issues. *Journal of Cloud Computing Advances Systems and Applications*, 11(1). <https://doi.org/10.1186/s13677-022-00353-y>
9. Askar, S. (2021a, August 19). Blockchain for Securing IoT Devices: A review. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3962701
10. Askar, S. (2021b, August 19). SDN based Fog Computing: a review. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3963001
11. Attkan, A., & Ranga, V. (2022). Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. *Complex & Intelligent Systems*, 8(4), 3559–3591. <https://doi.org/10.1007/s40747-022-00667-z>
12. Badidi, E. (2022). Edge AI and blockchain for smart sustainable cities: promise and potential. *Sustainability*, 14–14, 7609–7609. <https://doi.org/10.3390/su14137609>
13. Bekri, W., Jmal, R., & Fourati, L. C. (2020). Internet of Things Management Based on Software Defined Networking: A survey. *International Journal of Wireless Information Networks*, 27(3), 385–410. <https://doi.org/10.1007/s10776-020-00488-2>
14. Bekri, W., Jmal, R., & Fourati, L. C. (2024). Secure and trustworthiness IoT systems: investigations and literature review. *Telecommunication Systems*, 85(3), 503–538. <https://doi.org/10.1007/s11235-023-01089-z>
15. Bhat, S. A., Sofi, I. B., & Chi, C. (2020). Edge computing and its convergence with blockchain in 5G and beyond: security, challenges, and opportunities. *IEEE Access*, 8, 205340–205373. <https://doi.org/10.1109/access.2020.3037108>
16. Differential Privacy for Industrial Internet of Things: Opportunities, applications and challenges. (2021). In *IEEE Internet of Things Journal*. <https://doi.org/10.1109/JIOT.2021.3057419>
17. DistB-VNET: Distributed Cluster-based Blockchain Vehicular Ad-Hoc Networks through SDN-NFV for Smart City. (n.d.). <https://arxiv.org/html/2412.04222v1>
18. Dwivedi, S. K., Amin, R., Das, A. K., Leung, M. T., Choo, K. R., & Vollala, S. (2022). Blockchain-based vehicular ad-hoc networks: A comprehensive survey. *Ad Hoc Networks*, 137,

102980.
<https://doi.org/10.1016/j.adhoc.2022.102980>
19. East Tennessee State University. (2023). Lightweight Blockchains and Their Network Impact on Vehicular Ad-hoc Network-based Blockchain Applications. In Electronic Theses and Dissertations. <https://dc.etsu.edu/etd/4242>
20. et.al. (2024). A Systematic review on blockchain-based access control systems in cloud environment. Journal of Cloud Computing. <https://ub-ir.bolton.ac.uk/esploro/outputs/journalArticle/A-Systematic-review-on-blockchain-based-access/9913710108841>
21. Faezi, S., & Shirmarz, A. (2023). A Comprehensive Survey on Machine Learning using in Software Defined Networks (SDN). Human-Centric Intelligent Systems, 3(3), 312–343. <https://doi.org/10.1007/s44230-023-00025-3>
22. Ghaffari, F. (2023). A novel blockchain-based architecture for mobile network operators: Beyond 5G [PhD dissertation, Institut Polytechnique de Paris]. In Artificial Intelligence. <https://theses.hal.science/tel-04328677v1>
23. Gill, S. S., Golec, M., Hu, J., Xu, M., Du, J., Wu, H., Walia, G. K., Murugesan, S. S., Ali, B., Kumar, M., Ye, K., Verma, P., Kumar, S., Cuadrado, F., & Uhlig, S. (2024). Edge AI: A Taxonomy, Systematic review and Future Directions. Cluster Computing, 28(1). <https://doi.org/10.1007/s10586-024-04686-y>
24. Grover, J. (2022a). Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review. Vehicular Communications, 34, 100458. <https://doi.org/10.1016/j.vehcom.2022.100458>
25. Grover, J. (2022b). Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review. Vehicular Communications, 34, 100458. <https://doi.org/10.1016/j.vehcom.2022.100458>
26. Hadian, M., Erfani, S. H., Deypir, M., & Mirabi, M. (2023). CD-TMS: a combinatorial design-based token management system to enhance security and performance in blockchain. Cluster Computing, 27(4), 4515–4536. <https://doi.org/10.1007/s10586-023-04184-7>
27. Hildebrand, B., Baza, M., Salman, T., Amsaad, F., Razaqu, A., & Alourani, A. (2022). A Comprehensive Review on Blockchains for Internet of Vehicles: Challenges and Directions. arXiv (Cornell University). <https://doi.org/10.48550/arxiv.2203.10708>
28. IEEE, Department of Electrical Engineering, Institute of Communications Engineering, National Tsing Hua University, Hsinchu 30013, Taiwan, & School of Electronics and Electrical Engineering, Lovely Professional University, Phagwara 144001, India. (2020). Edge Computing and Its Convergence With Blockchain in 5G and Beyond: Security, Challenges, and Opportunities. In SPECIAL SECTION ON BLOCKCHAIN TECHNOLOGY: PRINCIPLES AND APPLICATIONS (Vol. 8, p. 205340) [Journal-article]. <https://doi.org/10.1109/ACCESS.2020.3037108>
29. IEEE, King Saud University, & IEEE. (2024). A Systematic Review on Blockchain-Enabled Internet of Vehicles (BIOV): challenges, defenses, and future research directions. My Review.
30. Janbi, N., Katib, I., & Mehmood, R. (2023). Distributed Artificial intelligence: review, taxonomy, framework, and reference architecture. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.4347753>
31. Juárez, R., & Bordel, B. (2023). Augmenting Vehicular Ad Hoc Network Security and Efficiency with Blockchain: A Probabilistic Identification and Malicious Node Mitigation Strategy. Electronics, 12(23), 4794. <https://doi.org/10.3390/electronics12234794>
32. K, S., Goure, S., & Banu, S. (2023). A comprehensive review on edge computing. International Journal for Research in Applied Science and Engineering Technology, 11(1), 92–106. <https://doi.org/10.22214/ijraset.2023.48484>
33. Khalid, A., Rehman, R. A., & Kim, B. (2024). Caching strategies in NDN Based Wireless Ad Hoc Network: a survey. Computers, Materials & Continua/Computers, Materials & Continua (Print), 80(1), 61–103. <https://doi.org/10.32604/cmc.2024.049981>
34. Kufakunesu, R., Myburgh, H., & De Freitas, A. (2025). The internet of battle things: a survey on communication challenges and recent solutions. Discover Internet of Things, 5(1). <https://doi.org/10.1007/s43926-025-00093-w>

35. Kumar, R., & Agrawal, N. (2023). Software defined networks (SDNs) for environmental surveillance: A Survey. *Multimedia Tools and Applications*, 83(4), 11323–11365. <https://doi.org/10.1007/s11042-023-15729-8>
36. Latif, N., Ma, W., & Ahmad, H. B. (2025). Advancements in securing federated learning with IDS: a comprehensive review of neural networks and feature engineering techniques for malicious client detection. *Artificial Intelligence Review*, 58(3). <https://doi.org/10.1007/s10462-024-11082-w>
37. Liu, L., Chen, C., Pei, Q., Maharjan, S., & Zhang, Y. (2020). Vehicular Edge Computing and Networking: a survey. *Mobile Networks and Applications*, 26(3), 1145–1168. <https://doi.org/10.1007/s11036-020-01624-1>
38. Mikavica, B., & Kostić-Ljubisavljević, A. (2021). Blockchain-based solutions for security, privacy, and trust management in vehicular networks: a survey. *The Journal of Supercomputing*, 77(9), 9520–9575. <https://doi.org/10.1007/s11227-021-03659-x>
39. Mlika, F., Karoui, W., & Romdhane, L. B. (2024). Trustworthy decentralization based on blockchain tools for social network architectures. *Social Network Analysis and Mining*, 14(1). <https://doi.org/10.1007/s13278-024-01252-7>
40. Moosavi, N., & Taherdoost, H. (2023a, October 29). Blockchain Technology Application in Security: A Systematic Review. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4626718
41. Moosavi, N., & Taherdoost, H. (2023b, November 8). Blockchain from the Security Perspective: A scoping review. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4626735
42. Moosavi, N., & Taherdoost, H. (2024, May 15). Blockchain from the Security Perspective: A Scoping Review. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4828470
43. Nagarajan, J., Mansourian, P., Shahid, M. A., Jaekel, A., Saini, I., Zhang, N., & Kneppers, M. (2023). Machine Learning based intrusion detection systems for connected autonomous vehicles: A survey. *Peer-to-Peer Networking and Applications*, 16(5), 2153–2185. <https://doi.org/10.1007/s12083-023-01508-7>
44. Premalatha, B., & Prakasam, P. (2024). A review on FOG Computing in 5G Wireless Technologies: Research challenges, issues and solutions. *Wireless Personal Communications*, 134(4), 2455–2484. <https://doi.org/10.1007/s11277-024-11061-y>
45. Punia, A., Gulia, P., Gill, N. S., Ibeke, E., Iwendi, C., & Shukla, P. K. (2024a). A systematic review on blockchain-based access control systems in cloud environment. *Journal of Cloud Computing Advances Systems and Applications*, 13(1). <https://doi.org/10.1186/s13677-024-00697-7>
46. Punia, A., Gulia, P., Gill, N. S., Ibeke, E., Iwendi, C., & Shukla, P. K. (2024b). A systematic review on blockchain-based access control systems in cloud environment. *Journal of Cloud Computing Advances Systems and Applications*, 13(1). <https://doi.org/10.1186/s13677-024-00697-7>
47. Rafique, W., Qi, L., Yaqoob, I., Imran, M., Rasool, R. U., & Dou, W. (2020). Complementing IoT services through software defined networking and edge Computing: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 22(3), 1761–1804. <https://doi.org/10.1109/comst.2020.2997475>
48. Rahman, A., Montieri, A., Kundu, D., Karim, M. R., Islam, M. J., Umme, S., Nascita, A., & Pescapé, A. (2022). On the Integration of Blockchain and SDN: Overview, Applications, and Future Perspectives. *Journal of Network and Systems Management*, 30(4). <https://doi.org/10.1007/s10922-022-09682-4>
49. Rejeb, A., Rejeb, K., Appolloni, A., Jagtap, S., Iranmanesh, M., & Edith Cowan University. (2024). Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions. In *Internet of Things and Cyber-Physical Systems (Vols. 4–4, pp. 1–18)* [Journal-article]. <https://doi.org/10.1016/j.iotcps.2023.06.003>
50. Saad, M., Khan, M. K., & Ahmad, M. B. (2022). Blockchain-Enabled Vehicular Ad Hoc Networks: A Systematic Literature Review. *Sustainability*, 14(7), 3919. <https://doi.org/10.3390/su14073919>

51. Scalable Approaches for Enhancing privacy in blockchain Networks: A Comprehensive review of differential privacy techniques. (2024). In Journal of Information Systems Engineering and Management (Vol. 8s) [Journal-article]. <https://www.jisem-journal.com/>
52. Sendros, A., Drosatos, G., Efraimidis, P. S., & Tsirliganis, N. C. (2021). Blockchain Applications in Agriculture: A scoping review. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.4055335>
53. Shafiq, S., Rahman, M. S., Shaon, S. A., Mahmud, I., & Hosen, A. S. M. S. (2024). A review on Software-Defined Networking for Internet of Things inclusive of distributed computing, blockchain, and Mobile Network Technology: Basics, trends, challenges, and future research potentials. International Journal of Distributed Sensor Networks, 2024(1). <https://doi.org/10.1155/2024/9006405>
54. Shakir, A. T., Islam, M. S., Mandeep, J. S., Islam, M. T., Abdullah, N. F., Taher, Y. H., Abdullahi, O. T., & Soliman, M. S. (2024). Systematic review of data exchange for road side unit in a vehicular ad hoc network: coherent taxonomy, prominent features, datasets, metrics, performance measures, motivation, opportunities, challenges and methodological aspects. Deleted Journal, 6(9). <https://doi.org/10.1007/s42452-024-06174-9>
55. Sheikh, A. M., Islam, Md. R., Habaeabi, M. H., Zabidi, S. A., Najeeb, A. R. B., & Adnan Kabani. (2025). A survey on Edge Computing (EC) Security Challenges: Classification, threats, and mitigation strategies. My Review. <https://doi.org/10.20944/preprints202502.1500.v1>
56. Sreekantha, D. K., Kulkarni, R. V., & Gao, X. (2021). Blockchain and 5G-Enabled Industrial Internet of Things: Application-Specific analysis. In Springer eBooks (pp. 531–569). https://doi.org/10.1007/978-3-030-67490-8_21
57. Sunkesula, M. a. K. A., & Siraparapu, S. R. (2024). Securing the IOT Landscape: A Comprehensive review of secure systems in the digital era. My Review. <https://doi.org/10.2139/ssrn.4883320>
58. Taherdoost, H. (2023, November 8). Blockchain and Machine Learning: A Critical Review on security. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4626844
59. Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions. (2024). Internet of Things and Cyber-Physical Systems, 4–4, 1–18. <https://doi.org/10.1016/j.iotcps.2023.06.003>
60. Wijesekara, P. a. D. S. N., & Gunawardena, S. (2023). A review of Blockchain Technology in Knowledge-Defined Networking, its application, benefits, and challenges. Network, 3(3), 343–421. <https://doi.org/10.3390/network3030017>