

DistB-VNET: Distributed Cluster-based Blockchain Vehicular Ad-Hoc Networks through SDN-NFV for Smart City

Anichur Rahman*, MD. Zunead Abedin Eidmum†, Dipanjali Kundu‡, Mahir Hossain§,
MD Tanjum An Tashrif§, Md Ahsan Karim¶, and Md. Jahidul Islam||

*Dept. of Computer Science and Engineering, National Institute of Textile Engineering and Research (NITER),
Constituent Institute of Dhaka University, Savar, Dhaka-1350*

*Dept. of Internet of Things and Robotics Engineering, Bangabandhu Sheikh Mujibur Rahman Digital University,
Dept. of Computer Science and Engineering, Green University of Bangladesh*

*anis.mbstu.cse@gmail.com**, *1801031@iot.bdu.ac.bd†*, *dkundu@niter.edu.bd‡*, *mahihossain114@gmail.com§*,
mtashrif20@niter.edu.bd¶, *makarim11@niter.edu.bd||*, *jahid@cse.green.edu.bd***

Abstract—In the developing topic of smart cities, Vehicular Ad-Hoc Networks (VANETs) are crucial for providing successful interaction between vehicles and infrastructure. This research proposes a distributed Blockchain-based Vehicular Ad-hoc Network (“DistB-VNET”) architecture that includes binary malicious traffic classification, Software Defined Networking (SDN), and Network Function Virtualization (NFV) to ensure safe, scalable, and reliable vehicular networks in smart cities. The suggested framework is the decentralized blockchain for safe data management and SDN-NFV for dynamic network management and resource efficiency and a noble isolation forest algorithm works as an IDS (Intrusion Detection System). Further, “DistB-VNET” offers a dual-layer blockchain system, where a distributed blockchain provides safe communication between vehicles, while a centralized blockchain in the cloud is in charge of data verification and storage. This improves security, scalability, and adaptability, ensuring better traffic management, data security, and privacy in VANETs. Furthermore, the unsupervised isolation forest model achieves a high accuracy of 99.23% for detecting malicious traffic. Additionally, reveals that our method greatly improves network performance, offering decreased latency, increased security, and reduced congestion, an effective alternative for existing smart city infrastructures.

Keywords—Internet of Things, Blockchain, SDN, NFV, Ad-Hoc Network, VANET, Smart City.

I. INTRODUCTION

In recent years, the field of SDN and NFV has made significant advancements in the context of smart city systems. Previous studies [1]–[3] have explored this field of technology. With the increasing population, wireless connectivity has advanced, and research in VANETs has expanded, a critical component of smart city wireless systems. VANETs are designed to enable communication between vehicles and their operators to improve traffic safety and efficiency. VANET, a sub-category of the mobile ad hoc network, serves the function of the transmission of data between the vehicle and the vehicle operator.

In contrast to traditional VANET technology, there is an excellent opportunity for Blockchain that provides better security for the vehicle to the vehicle transmission system. As in the conventional system, the data from the devices are stored in a centralized server, and from this server, all other nodes collect and use the information required [4]. This centralized server may be the main attraction for hackers. Because the information stored here is very critical for efficient communication between the nodes of the transport system, this

information requires a secure platform where the data collected is stored securely and the data preserved effectively. Again, there is another emerging technology, Blockchain, which is a distributed decentralized technology, and the information is passed as a block. Here, only authorized block can take their place in the chain, thus maintaining the privacy of the blocks of information. The idea of a decentralized blockchain may, therefore, be a potential solution for VANET technology [5]. To effectively transfer information from one vehicle to another by storing it in a trusted location, leveraging the design of the Blockchain distributed process [6].

There are many critical issues that are still unsolved in VANETs, mainly in security, privacy, and time management. Communication delays between vehicles could cause accidents and hinder traffic management. Additionally, challenges like the high power demands for node creation and block authorization affect vehicular management systems [7]. Since cities are evolving in a smart way, efficient traffic management has become necessary, so improved accuracy, trust, transparency, and security are required. Technologies like SDN, NFV, AI, and Big Data can enhance performance, due to SDN offering a layered platform to manage increasing data from vehicle-to-vehicle communication [8]. However, centralized VANET architectures remain vulnerable due to centralized data storage, making them vulnerable to hacking. Delays or system failures could seriously impact traffic control. Despite efforts to improve them, a fully secure and reliable solution is still needed.

As smart cities evolve, there is a growing need for advanced technologies that can handle complex urban systems more efficiently. In this context, efficient traffic management plays a pivotal role in ensuring safety and reducing congestion. Our proposed system combines SDN, NFV, and Blockchain to provide superior accuracy, trust, transparency, latency, and security. SDN, with its layered architecture, offers an effective platform to handle large volumes of data generated by vehicular networks. However, the reliance on centralized servers in SDN makes the system vulnerable to attacks. Integrating NFV helps mitigate these risks by decentralizing traffic management, reducing power consumption, and enhancing flexibility. In this system, NFV ensures that resources are allocated more efficiently, improving overall performance [9]. The combination of SDN, NFV, and Blockchain could solve the conventional problems in VANET. However, there are still

some research gaps about how to successfully integrate these technologies to find a better solution to the open challenges of the smart vehicle management system. Before incorporating SDN, the security challenges of SDN need to be mitigated. Some of the attacks of SDN, namely Denial of Service attacks, flooding attacks, and some others addressed by researchers [10], [11]. At the same time, NFV is rather not free from technical challenges [12]. Monitoring the flow of information, failure recovery, especially in the telecommunication system, and allocation of available resources are some of the significant issues in NFV-related technologies [13].

This research introduces a novel approach to enhance traditional VANET systems by integrating Blockchain with SDN and NFV in smart city environments. Blockchain's decentralized structure ensures secure vehicular data transmission while reducing the risk of central points of failure. In this system, clusters of vehicles are formed, with a cluster head communicating with distributed nodes linked to a central cloud. While Blockchain enhances security, challenges like high computational demands and delays need addressing. By combining SDN and NFV, this approach optimizes both security and performance in smart city VANETs. This work's contributions are as follows:

- The authors propose a distributed Blockchain-based Vehicular Ad-hoc Network "DistB-VNET" architecture that provides security, scalability, reliability and confidentiality as well as better traffic management in the VANET environment .
- An SDN technique has been integrated with multiple controllers from the data layer to the application layer to divide the load equally between the devices and controllers. Also, NFV is employed to ensure the automatic allocation of network resources efficiently.
- Additionally, an unsupervised model Isolation Forest is employed by the authors after the cluster head to detect and block malicious traffic in the edge level.

Organization: The rest of the paper has been formed as follows: We studied and discussed the related literature in section II. Then, section III performs the proposed model for smart cities. The result analysis and discussion are assessed in section IV. In addition, section V presents the conclusion with future directions.

II. RELATED WORKS

Recently, researchers have addressed enormous work based on emerging leading technologies such as SDN, distributed Blockchain, NFV, and VANET technologies. In this section, the authors present an overview of some recent works in literature.

Hemani et al. [14] proposed a tamper-proof and transparent data sharing system between the nodes of autonomous vehicles. The privacy of the shared information was preserved using smart contracts with solidity. Zalte et al. [15] suggested a integrating blockchain technology to solve problems with data dispersion in VANETs. In addition, this research covered a blockchain that uses AI and data analytics. Diallo et al. [16] proposed a new system for managing traffic-related data in VANETs (Vehicular Ad hoc NETworks) using blockchain technology in their work. In their study, Abdullah et al. [17] proposed a framework called Biometrics Blockchain (BBC) to secure data sharing between vehicles in Vehicular Ad-hoc

Networks (VANETs). The BBC framework used biometric information to verify the identity of vehicles without revealing their actual identity. Hailin et al. [18] explored the integration of blockchain technology with Digital Twins (DTs) to map real-world traffic scenarios into a virtual space in VANETs to enhance intelligent transportation and employ blockchain for secure data storage and transmission in smart cities. The proposed model demonstrated lower average delay times, stable data message delivery rates, and high network security.

Additionally, with this traditional VANET technology, other emerging technologies like SDN, Blockchain, NFV, Artificial Intelligence, Cloud computing, and so many other available technologies were incorporated together to solve and enhance the transportation management performance system. In their research, SULEYMAN et al. [19] investigated how Blockchain (BC) and SDN operate together in the context of the IoT [20]. The six main implementation objectives of security, computing paradigms (fog and edge), trust management, access control & authentication, privacy, and networking were used to categorize pertinent studies. Tahani et al. [21] in their article proposed a decentralized Blockchain-based trust management framework (BC-TMF) to compute trust metrics for vehicles and achieved better accuracy for malicious vehicles. In their study, Balaji et al. [22] discussed the difficulties with traffic management and energy efficiency in VANETs. In addition, the authors presented the SDNTFP-C method, which combined Deep Learning (DL) models with the scalability, flexibility, and adaptability of SDN controllers.

TABLE I
COMPARISON OF STATE-OF-ARTS

Works	Contributions	Research Gap
Hemani et al.(2024) [14]	Implemented a smart contract with solidity to reserve information privacy for AV	Excessive power consumption
Zalte et al. (2022) [15]	Solved data dispersion problems in VANETs	Computational power and Storage capacity Limitation
SULEYMAN et al. (2023) [19]	Combined Blockchain and SDN together in the Context of IoT	Lack of regulatory frameworks and greater complexity.
Tahani et al. (2022) [21]	Computed trust metrics for vehicles and achieved better accuracy	Privacy of vehicle owners is not protected
Balaji et al. (2023) [22]	Integrated deep learning (DL) models with the scalability, flexibility, and adaptability of SDN controllers	Lack of robustness

In summary, the current research is not sufficient, and there are still many challenges in this system. Table I shows the contribution and the limitations of the previous studies, which we are going to solve.

III. PROPOSED "DISTBLOCK-VNET" ARCHITECTURE FOR SMART CITIES

This section provides the architecture and operational framework of "DistB-VNET", a distributed blockchain-based VANET combined with SDN and NFV for smart cities. Fig. 1 shows the integration of vehicular cloud storage, blockchain, and SDN controllers. Vehicular cloud storage remains as a centralized repository for traffic data, vehicle IDs, and sensor information, enhancing data sharing among vehicles and city services. The blockchain network functions as a decentralized ledger, providing data integrity by storing transactions immutably. SDN offers a programmable network architecture, dividing control and data planes for centralized network management. SDN controllers regulate data flow, routing, and quality of service using northbound and southbound APIs. Vehicles collect data by the sensors, upload it to vehicular cloud storage for processing, and then send it to the blockchain for validation. Network services, managed by NFV, handle the validated data, while SDN controllers take real-time decisions

on routing, traffic management, and resource allocation. This integration provides a secure, scalable, and efficient vehicular communication network for smart cities context.

A. Detection and Block Malicious Traffic

In this architecture, IoT devices send traffic to the distributed nodes through the cluster heads. However, it may be vulnerable to cyber-attacks executed in the form of network traffic. Traditional intrusion detection systems or supervised models can only detect known types of cyber-attacks like DDoS, SQL injection, etc. Moreover, in real-world scenarios, the attacks may be new, as methods of cyber-attacks evolve daily. To address this issue, instead of training a supervised model, we train an unsupervised model. This unsupervised model, named Isolation Forest, is trained on the IDS 2018 Intrusion dataset [23]. The trained model functions as a primary verification system between IoT edge devices and distributed nodes. The Isolation Forest model checks all traffic, categorizing it as either benign or malicious. Malicious traffic is blocked by the verification process, and it is stored in temporary storage to prevent it from passing until it is cleared of malware [24].

B. Architectural Design for VANET with SDN-NFV Procedure

In the context of smart cities, SDN emerges as a critical technology by separating network control from data forwarding, thereby permitting dynamic traffic management. By using SDN's capabilities, traffic systems may adjust in real-time, enhancing efficiency and responsiveness. Integrating SDN with NFV further boosts system flexibility and scalability, enabling optimal resource allocation and minimizing operational expenses. The proposed architecture shown in Fig. 1 corresponds with SDN and NFV standards, supporting dynamic network management through components such as the SDN Network Slice Manager (NSM), Network Slice Orchestrator (NSO), and Vehicular Application Manager (VAM). In vehicle networking situations like VANET and the Internet of Vehicles (IoV), SDN, NFV, and Fog Computing play significant roles in facilitating connection and optimal resource usage. Network slicing provides for specialized networks with specified Quality of Service (QoS) needs, while protocol selection, such as AODV, DSDV, or OLSR, depends on network characteristics and mobility patterns. The integration of SDN and NFV offers benefits such as flexibility, scalability, and cost reduction, virtualizing network services to enable for effective resource usage and dynamic allocation based on traffic conditions. These components provide dynamic network management and orchestration, providing optimal network performance and dependable vehicular communication [25].

C. Proposed Algorithm for “DistB-VNET”

In this section, Alg. 1 is presented for our proposed Distributed Blockchain-based Vehicular Ad-hoc Network (DistB-VNET), integrated with SDN and NFV technologies for smart city environments. The algorithm is designed to handle secure communication, vehicle clustering, and efficient resource management in the network. The “DistB-VNET” system first measures signal strengths and processing power to make clusters via Roadside Units (RSUs) where cluster heads lead communications. Messages are encrypted using the public-private key pair and verified through blockchain to ensure integrity. They have finally been forwarded by the SDN controllers. Additionally, the controller manages traffic and allocates resources automatically using NFV to optimize performance and reduce latency.

Algorithm 1 DistB-VNET: Secure Communication and Clustering Algorithm

```

1: Initialization:
     $V$ : Set of vehicles
     $C$ : Set of clusters
     $R$ : Set of Roadside Units (RSUs)
     $S$ : SDN controller
     $K_{pub}(v)$ : Public Key of vehicle  $v$ 
     $K_{priv}(v)$ : Private Key of vehicle  $v$ 
     $B$ : Blockchain ledger
2: procedure CLUSTER FORMATION( $V, R$ )
3:   for each  $v \in V$  do
4:      $S(v), P(v)$                                  $\triangleright$  Measure signal strength and processing power
5:      $v \rightarrow r \in R$                           $\triangleright$  Broadcast to nearest RSU
6:      $CH \leftarrow \text{Elect}(R)$ 
7:      $C \leftarrow \text{Create Cluster}(CH)$ 
8:      $(K_C_{pub}, K_C_{priv}) \leftarrow \text{KeyPair}(C)$ 
9:   end for
10: end procedure
11: procedure SECURE COMMUNICATION( $CH, S, B$ )
12:   for each  $m$  from  $v$  to  $CH$  do
13:      $H(m) \leftarrow \text{Hash}(m)$ 
14:      $E(m, K_{priv}(v))$ 
15:      $m \leftarrow D(E(m), K_{pub}(v))$ 
16:      $H(m), K_C_{priv} \rightarrow S$                      $\triangleright$  Encrypt with  $K_{priv}$             $\triangleright$  Decrypt with  $K_{pub}$ 
17:     Validate( $S, B$ )
18:   end for
19:    $CH \rightarrow S$                                  $\triangleright$  Forward data
20: end procedure
21: procedure RESOURCE ALLOCATION( $S, NFV$ )
22:    $S \leftarrow \text{Collect State Info and Traffic Load}$ 
23:   Allocate( $NFV$ )                                 $\triangleright$  Optimize latency and performance
24:   Manage Traffic( $S$ )
25: end procedure

```

D. Vehicles Controlling via Distributed Blockchain and SDN

The combination of blockchain, SDN-VANET, IPFS and clustering provides a secure and scalable solution for smart city traffic management. Roadside Units (RSUs) transmit cluster data through a blockchain-based voting system. That safely selects the cluster head according to the vehicle type. As seen in Fig 2, the cluster head then secures the communication by creating cryptographic key pairs and signing messages, which are subsequently confirmed by the SDN controller via blockchain. By assembling vehicle requests through cluster heads, who then hash and forward messages to the SDN controller, clustering lowers networking load [26]. The controller ensures a two-step verification process and receives the original messages and contents from IPFS. Blockchain ensures communication integrity within clusters by using public key infrastructure for vehicle data verification. Blockchain guarantees tamper resistance and transparency by securing the storage of cluster keys, traffic data, and vehicle data. SDN provides efficient routing, resource management and centralized network control. IPFS facilitates distributed storage that guarantees scalability, While clustering improves communication by reducing latency and congestion. Interaction between RSU cluster members and SDN controllers is secured by cryptographic key management and secure message authentication. Guarantee the reliability and integrity of the system.

E. Real Life Application of “DistB-VNET” Framework in Smart Cities

Smart cities are regulated around huge volume of data generated by smart vehicles, IoT devices, sensors, actuators etc. As the concept of smart cities become popular, the issues of data safety, security becomes top priority. Distributed nature of blockchain ensures that all the data available is stored in multiple places so that they are less vulnerable to cyber attacks. For vehicular communication, it is important to preserve the privacy of the vehicle owner while sharing vehicle

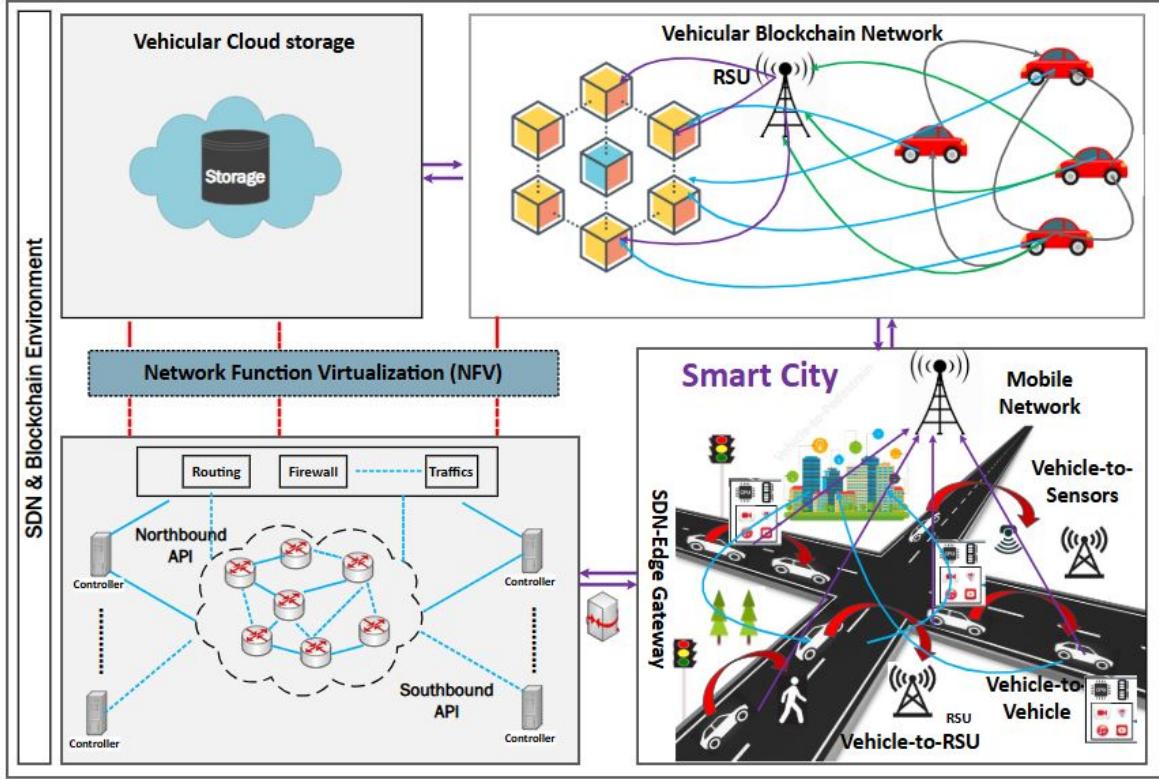


Fig. 1. Proposed “DistB-VNET” Architecture for Smart City

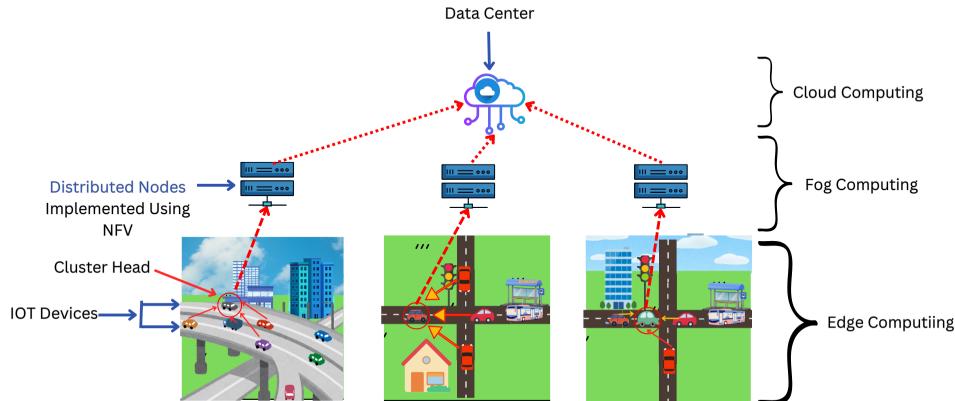


Fig. 2. Data Collection Scenario from the Edge Layers

information. This problem can be also solved by using the smart contracts. To avoid collision and fast and reliable data transfer, the latency should be minimal and throughput should be maximum. “DistB-VNET” framework ensures the minimal latency by using NFV automatic resource allocation process. Finally, this framework ensures data privacy, safety and secure communication of information for smart vehicles which make it very much suitable for real life application in the smart cities.

IV. RESULT ANALYSIS AND DESIGN

VANET is an important part of the smart city. Implementing blockchain to secure the network connection between smart vehicles in smart cities is a new addition, where the networking process can be taken to the next level using the combination of SDN-NFV with Edge and Fog computing. The persisting previous work of researchers in the field of Smart cities, Ad-Hoc networks, and blockchain inspired us to do this

work. We used two types of blockchain technology to secure our network, distributed and centralized. Our smart vehicle connects with the fog network which later connects with the cloud server. The SDN technology is used to control the network part and NFV is used to virtualize the process. The result of our model is promising and excellent. This result means that our proposed model can be used in modern smart cities.

A. Measurement Parameters

We have used various parameters such as gas consumption rate, throughput based on a number of vehicles, End-to-End Delay, Packet Delivery Ratio, Overhead, and throughput based on cluster size, to measure the performance of the proposed framework.

Throughput in vehicular network, considering the cluster size, is given by following equation where $T(C)$ is the throughput (in Mbps) based on cluster size, C is the size of the cluster, $D(C)$ is the average data generated by each vehicle in the cluster, t_b represents the delay due to blockchain operations, t_s is the time delay from SDN operations, t_n accounts for NFV-related delays such as resource allocation, t_c refers to the intra-cluster communication delay.

$$T(C) = \frac{C \times D(C)}{t_b + t_s + t_n + t_c} \quad (1)$$

Moreover, throughput in a blockchain considering the number of vehicles, is given below where $T(V)$ is the throughput (in Mbps) based on the number of vehicles where V represents the total number of vehicles in the network, $D(V)$ is the average data generated per vehicle, t_b refers to the delay due to blockchain operations, such as transaction validation and block propagation, t_s is the time delay from SDN operations, including routing and traffic management, t_n accounts for the time delay due to NFV operations, t_v is the communication delay between vehicles and infrastructure..

$$T(V) = \frac{V \times D(V)}{t_b + t_s + t_n + t_v} \quad (2)$$

The gas consumption rate $G(T_x)$ depends on the number of transactions T_x and can be expressed as:

$$G(T_x) = G_0 \times T_x + C_b \times T_x \quad (3)$$

Where T_x denotes the total number of transactions processed in the blockchain, G_0 is the base gas cost required for validating a single transaction and C_b represents the additional gas consumption due to the complexity of blockchain operations.

B. Environment Setup

We have used a network emulator named Mininet and Ethereum for simulating our proposed methodology [28]. The parameters used for this simulation are shown in Table III.

C. Performance Evaluation

Table IV indicates the performance scores for our isolation forest algorithm. It achieves high accuracy of 99.23% following by high precision of 99.14%, recall of 99.15% and f-score of 99.07%.

Fig. 3 illustrates the change in throughput due to the size of the cluster size. Here, we consider two cluster sizes: size of 5 and size of 10. The throughput increases as we increase the cluster size of the proposed system. The gap between the throughput of clusters 5 and 10 is quite big. On the other

hand for each cluster size, the throughput decreases for the increase in the number of vehicle nodes. For cluster size 5 the highest throughput was for 15 number of vehicles and it decreases with the increase number of vehicle and reach the lowest point for 50 number of vehicles. On the other hand, the throughput decreases for the limit of 25 vehicles for cluster size 10 and after that it becomes saturated.

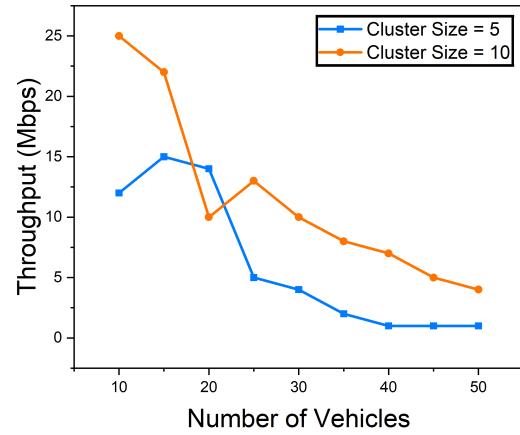


Fig. 3. Throughput of the proposed system in terms of different cluster size

Fig. 4 depicts the communication cost or the total number of exchanged messages for the proposed system against the total number of vehicles. Communication costs have always increased due to the rise in the number of vehicles.

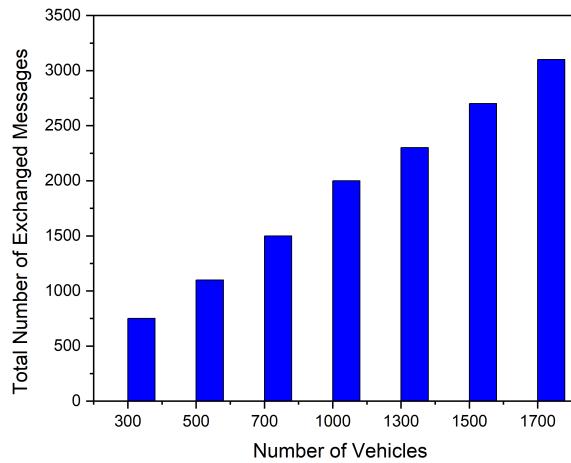


Fig. 4. Comparison of communication overhead

Table V exhibits the gas consumption with respect of the number of transactions. Gas limit represents the maximum possible required energy for a single transaction. For a small amount of transactions, the gas limit is very low, but it increases linearly for the increasing amount of transactions.

Table II shows the comparison of Throughput (THRPT), Packet Delivery Ratio (PDR), Network Lifetime (NLT), End-to-End Delay (ETED), and Energy Consumption (ECM) be-

TABLE II
COMPARISON OF PROPOSED AND IEAOCGO-C [27] METHODS ACROSS VARIOUS METRICS

Vehicles	NLT (rounds)		PDR (%)		THRPT (kbps)		ETED (m.J)		ECM (ms)	
	Proposed	IEAOCGO-C	Proposed	IEAOCGO-C	Proposed	IEAOCGO-C	Proposed	IEAOCGO-C	Proposed	IEAOCGO-C
20	5200	4500	99.37	94.14	71.23	63.25	6.04	8.14	30.96	34.22
30	4900	4400	89.25	86.34	78.68	69.43	6.06	9.04	51.68	62.32
40	4700	3900	86.45	85.13	83.14	74.45	6.09	9.45	70.19	82.33
50	4200	3600	84.32	83.42	89.23	79.66	7.45	10.32	85.41	105.46

TABLE III
SIMULATION ENVIRONMENT

Parameter	Values
Blockchain Platform	Ethereum
Emulator	Mininet(version : 2.2.1)
Platform Type	Decentralized
Environment	Truffle, Ganache
Language	Solidity
Number of Nodes	80
Max. of deceleration	5m/s ²
Max. Acceleration	3.6 m/s ²
Max. vehicle speed	50m/s ²
Number of RSU Unit	10
Packet Size	100-512 bytes
Number of transactions	Variable
Block size	Variable
Transaction per Block	Variable

TABLE IV
PERFORMANCE METRICS OF ISOLATION FOREST

Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
99.23	99.14	99.15	99.07

TABLE V
GAS CONSUMPTION AGAINST NO. OF TRANSACTIONS

No. of transactions	Gas Consumption (ETH)
5	27000
8	36000
10	41000
14	55000
17	66000
22	78000
26	89000
30	100000

tween our proposed model and IEAOCGO-C algorithm on different vehicle numbers. Our proposed model outperform the IEAOCGO-C [27] algorithm on every factor for different vehicle numbers.

V. CONCLUSION

In this research, we have proposed “DistB-VNET”, a novel framework integrating ml based attack detection, Blockchain, SDN, and NFV to ensure the scalability, security, and efficiency of vehicular communication in smart cities. First, our model filters traffic and blocks malicious ones. Further, our framework utilizes SDN to separate control and data planes while ensuring dynamic resource allocation by NFV and data integrity through an immutable ledger by Blockchain. The results show improved throughput and communication efficiency across different vehicle volumes and cluster sizes. However, the system has not yet been tested in terms of increased transmission costs and gas fees as vehicle numbers and transactions grow. In future, we will focus on optimizing resource management and reducing blockchain transaction costs to improve system scalability.

REFERENCES

- [1] Z. H. Ali, N. A. Sakr, N. El-Rashidy, and H. A. Ali, “A reliable position-based routing scheme for controlling excessive data dissemination in vehicular ad-hoc networks,” *Computer Networks*, vol. 229, p. 109785, 2023.
- [2] A. Rahman, M. S. I. Khan, A. Montieri, M. J. Islam, M. R. Karim, M. Hasan, D. Kundu, M. K. Nasir, and A. Pescapè, “Blocksd-5net: Enhancing security of 5g network through blockchain-sdn with ml-based bandwidth prediction,” *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 4, p. e4965, 2024.
- [3] A. Rahman, M. A. H. Wadud, M. J. Islam, D. Kundu, T. A.-U.-H. Bhuiyan, G. Muhammad, and Z. Ali, “Internet of medical things and blockchain-enabled patient-centric agent through sdn for remote patient monitoring in 5g network,” *Scientific Reports*, vol. 14, no. 1, p. 5297, 2024.
- [4] A. Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan, and P. Tiwari, “Towards a blockchain-sdn-based secure architecture for cloud computing in smart industrial iot,” *Digital Communications and Networks*, vol. 9, no. 2, pp. 411–421, 2023.
- [5] L. Mendiboure, M. A. Chalouf, and F. Krief, “Survey on blockchain-based applications in internet of vehicles,” *Computers & Electrical Engineering*, vol. 84, p. 106646, 2020.
- [6] H. Fang, Y. Zhu, Y. Zhang, and X. Wang, “Decentralized edge collaboration for seamless handover authentication in zero-trust iov,” *IEEE Transactions on Wireless Communications*, 2024.
- [7] A. Hakiri, B. Sellami, and S. B. Yahia, “Joint energy efficiency and network optimization for integrated blockchain-sdn-based internet of things networks,” *Future Generation Computer Systems*, p. 107519, 2024.
- [8] A. Rahman, M. J. Islam, A. Montieri, M. K. Nasir, M. M. Reza, S. S. Band, A. Pescapè, M. Hasan, M. Sookhak, and A. Mosavi, “Smartblock-sdn: An optimized blockchain-sdn framework for resource management in iot,” *IEEE Access*, vol. 9, pp. 28 361–28 376, 2021.
- [9] A. Rahman, C. Chakraborty, A. Anwar, M. R. Karim, M. J. Islam, D. Kundu, Z. Rahman, and S. S. Band, “Sdn–iot empowered intelligent framework for industry 4.0 applications during covid-19 pandemic,” *Cluster Computing*, pp. 1–18, 2022.
- [10] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, “A survey on security attacks in vanets: Communication, applications and challenges,” *Vehicular Communications*, vol. 19, p. 100179, 2019.
- [11] J. Bhatia, Y. Modi, S. Tanwar, and M. Bhavsar, “Software defined vehicular networks: A comprehensive review,” *International Journal of Communication Systems*, vol. 32, no. 12, p. e4005, 2019.
- [12] A. Bradai, M. H. Rehmani, I. Haque, M. Nogueira, and S. H. R. Bukhari, “Software-defined networking (sdn) and network function virtualization (nfv) for a hyperconnected world: Challenges, applications, and major advancements.” *J. Network Syst. Manage.*, vol. 28, no. 3, pp. 433–435, 2020.
- [13] S. R. Chowdhury, M. A. Salahuddin, N. Limam, and R. Boutaba, “Re-architecting nfv ecosystem with microservices: State of the art and research challenges,” *IEEE Network*, vol. 33, no. 3, pp. 168–176, 2019.
- [14] Hemani, D. Singh, and R. K. Dwivedi, “Designing blockchain based secure autonomous vehicular internet of things (iot) architecture with efficient smart contracts,” *International Journal of Information Technology*, pp. 1–17, 2024.
- [15] S. Zalte, V. Ghorpade, and R. K. Kamat, “Synergizing blockchain, iot, and ai with vanet for intelligent transport solutions,” *Emerging Computing Paradigms: Principles, Advances and Applications*, pp. 193–210, 2022.
- [16] E.-h. Diallo, O. Dib, and K. Al Agha, “A scalable blockchain-based scheme for traffic-related data sharing in vanets,” *Blockchain: Research and Applications*, vol. 3, no. 3, p. 100087, 2022.
- [17] A. Alharthi, Q. Ni, and R. Jiang, “A privacy-preservation framework based on biometrics blockchain (bbc) to prevent attacks in vanet,” *Ieee Access*, vol. 9, pp. 87 299–87 309, 2021.
- [18] H. Feng, D. Chen, and Z. Lv, “Blockchain in digital twins-based vehicle management in vanets,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 19 613–19 623, 2022.
- [19] S. W. Turner, M. Karakus, E. Guler, and S. Uludag, “A promising integration of sdn and blockchain for iot networks: A survey,” *IEEE Access*, vol. 11, pp. 29 800–29 822, 2023.

- [20] A. Rahman, K. Hasan, D. Kundu, M. J. Islam, T. Debnath, S. S. Band, and N. Kumar, "On the icn-iot with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives," *Future Generation Computer Systems*, vol. 138, pp. 61–88, 2023.
- [21] T. Gazdar, O. Alboqomi, and A. Munshi, "A decentralized blockchain-based trust management framework for vehicular ad hoc networks," *Smart Cities*, vol. 5, no. 1, pp. 348–363, 2022.
- [22] T. Balaji and S. Srinivasan, "Networking controller based real time traffic prediction in clustered vehicular adhoc networks," *Intelligent Automation & Soft Computing*, vol. 35, no. 2, pp. 2189–2203, 2023.
- [23] solarmainframe, "Ids intrusion csv dataset," 2018, accessed: 2024-09-28. [Online]. Available: <https://www.kaggle.com/datasets/solarmainframe/ids-intrusion-csv/data>
- [24] A. Rahman, J. Islam, D. Kundu, R. Karim, Z. Rahman, S. S. Band, M. Sookhak, P. Tiwari, and N. Kumar, "Impacts of blockchain in software-defined internet of things ecosystem with network function virtualization for smart applications: Present perspectives and future directions," *International Journal of Communication Systems*, p. e5429, 2023.
- [25] A. Rahman, M. J. Islam, Z. Rahman, M. M. Reza, A. Anwar, M. P. Mahmud, M. K. Nasir, and R. M. Noor, "Distb-condo: Distributed blockchain-based iot-sdn model for smart condominium," *IEEE Access*, vol. 8, pp. 209 594–209 609, 2020.
- [26] A. Rahman, M. J. Islam, M. S. I. Khan, S. Kabir, A. I. Pritom, and M. R. Karim, "Block-sdotcloud: Enhancing security of cloud storage through blockchain-based sdn in iot network," in *2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI)*. IEEE, 2020, pp. 1–6.
- [27] M. Elhoseny, I. M. El-Hasnony, and Z. Tarek, "Intelligent energy aware optimization protocol for vehicular adhoc networks," *Scientific Reports*, vol. 13, no. 1, p. 9019, 2023.
- [28] M. J. Islam, A. Rahman, S. Kabir, M. R. Karim, U. K. Acharjee, M. K. Nasir, S. S. Band, M. Sookhak, and S. Wu, "Blockchain-sdn-based energy-aware and distributed secure architecture for iot in smart cities," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3850–3864, 2021.