Blockchain-Enabled Intelligent Vehicular Edge Computing

Shafkat Islam, Shahriar Badsha, Shamik Sengupta, Hung La, Ibrahim Khalil, and Mohammed Atiquzzaman

Abstract

Smart vehicles are expected to be equipped with high-dimensional, resource-intensive applications, including platoon control, augmented reality supported gaming, AI-based pedestrian detection, fuel scheduling, and so on, catering to diverse user preferences and enhancing safety and efficiency. These applications pose unique challenges for resource-constrained vehicles due to their intense computation requirements, whereas vehicular edge computing (VEC) networks, consisting of roadside units (RSUs) and MEC servers, contain the capability of providing cloud-like computing experience at vehicular edges while meeting performance requirements in terms of latency and throughput. Moreover, the development of intelligent VEC (IVEC) infrastructure is accelerated due to rapid advancement of AI algorithms in recent years. However, IVEC is prone to attacks, including fake computation feedback, unfair or biased resource allocation in a VEC server, and so on, due to its centralized governance and black box computation (edge computation works like a black box for end users). To combat such security vulnerabilities, we propose a blockchain-based decentralized architecture to enhance transparency in IVEC resource management and leverage edge consumers (e.g., vehicles) with a computation verification option. Additionally, we address the unbalanced load distribution issue and propose a secure IVEC federation model for balancing loads. We also outline the main challenges and provide a brief description of promising research directions to draw the attention of concerned stakeholders and parties in both the blockchain and edge computing domains.

Introduction

The concept of the Internet of Vehicles (IoV) [1] possesses potential for revolutionizing the automotive industry through its diverse offerings such as stable Internet connectivity, and compatibility with smart devices, edge, and cloud competency, among others. IoV, being an integral part of smart cities, enables smart vehicles to interact with almost everything, referred to as vehicle-to-everything (V2X), through heterogeneous networks in order to enhance on-road safety and cater for myriad infotainment preferences of vehicle users. Additionally, IoV leverages distinct business opportunities to vendor organizations in terms of connectivity and data analytics.

Next-generation smart vehicles are embedded with a multitude of resource-intensive artificial intelligence (AI) [2] applications, ranging from pedestrian detection to fuel scheduling. In contrast, each vehicle utilizes various onboard sensors (e.g., lidar, dashcam, ultrasound, and radar) to operate different autonomous tasks effectively. It is expected that every smart vehicle will generate approximately 100 TB of data in every eight-hour ride (https://www.dxc.technology/auto/insights); on the other hand, each vendor is projected to be operating in the Zetta scale by 2028 (https://datacenterfrontier.com/rolling-zettabytes-quantifying-the-data-impact-of-connected-cars/) due to such a gigantic generation rate. Uploading this enormous volume of data to the cloud is not efficient in terms of bandwidth and latency. Nevertheless, every piece of data is not essential enough for incurring storage burden. Also, the computation demanding implanted AI applications of smart vehicles serve as the primary consumer of such sensor data. In this regard, the IoV edge infrastructure, consisting of roadside units (RSUs), access points (APs), along with a mobile edge computing (MEC) [3] server, can facilitate smart vehicles with cloud-like computation capability through performing resource-intensive computations and analytics at edges while conforming with application-specific latency and quality of service (QoS) requirements.

With the rapid development of machine learning algorithms together with hardware advancement, accelerating the deployment of AI in MEC will enable edge servers to make autonomous decisions in dynamic environments, thus creating the notion of intelligent edge. In recent years, AI has been used in MEC for resource management [4], energy management [5], traffic offloading [6], and edge caching [7], to name a few; however, the existing literature lacks in analyzing the security issues related to intelligent edge infrastructure in terms of transparency and fairness. The situation is exacerbated in the IoV ecosystem as most stakeholders (e.g., a vehicle, RSU, and AP) are relative strangers to each other. Moreover, the edge computing service works like a black box for service consumers (e.g., vehicles). Additionally, RSUs and APs, despite being semi-trusted entities in the intelligent vehicular edge computing (IVEC) infrastructure, serve as a communication gateway between vehicles and MEC. Furthermore, the MEC orchestration is usually central, which poses the threat of a single point of failure and

Shafkat Islam, Shahriar Badsha, Shamik Sengupta, and Hung La are with the University of Nevada Reno; Ibrahim Khalil is with RMIT; Mohammed Atiquzzaman is with the University of Oklahoma

Digital Object Identifier: 10.1109/MNET.011.2000554

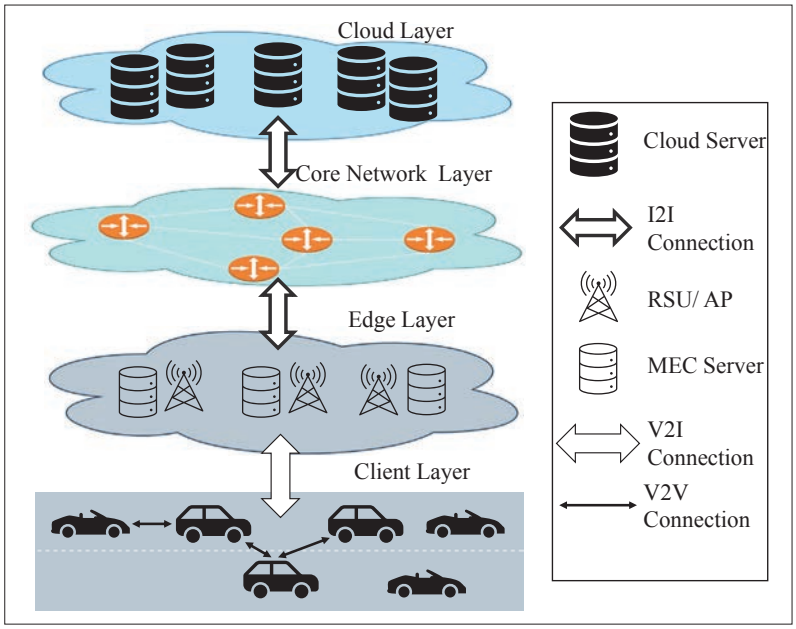

FIGURE 1. Illustration of a conventional IoV network.

unfair or biased resource allocation. Hence, IVEC is prone to attacks such as fake/forged feedback and unfair bias due to lack of transparency in the network.

Although the emergence of blockchain technology was initially dominated by cryptocurrency [8], over time, blockchain has manifested its diverse utility in cyber-physical systems [9], ride sharing [10], and the Internet of Things [11, 12], among others. Blockchain, a distributed ledger technology, privileges users with different features such as provenance, non-repudiation, decentralized governance, and tamper-proof ledger. Hence, any system built on blockchain technology exhibits a decentralized coordination and storage mechanism, without a central controller, through tamper-resistant distributed ledger update policies. Essentially, cryptocurrency and IVEC display some common kinds of problem scenarios. For instance, RSUs, APs, vehicles, and MEC servers in IVEC do not contain default trust during the peer-to-peer connection establishment process. However, deployment of blockchain technology in IVEC remains a challenging task due to scalability, encryption/decryption latency, communication overhead, storage burden, power consumption, and so on, as most vehicular edge infrastructure is resource-constrained. Hence, enormous research effort is required to develop lightweight IVEC blockchain architecture for enhancing trust within divergent entities of the IVEC ecosystem through incorporating verifiability and provenance.

The goal of this article is to investigate security vulnerabilities of IVEC infrastructure in terms of its centralized governance and black box computation property. Specifically, we propose a blockchain-based decentralized IVEC architecture and also present research challenges, scope, and exciting research directions in this domain. Additionally, we propose a secure VEC federation architecture for balancing computation loads on distributed VEC servers. Furthermore, decentralized service processing flow protocol is introduced for the elimination of centralized governance.

Overview of IVEC Architecture

This section outlines typical IVEC architecture along with its divergent applications and threat model.

IVEC Architecture

Figure 1 illustrates the traditional IoV architecture, which consists of multiple RSUs and APs, MEC and cloud servers, and vehicles. The MEC server contains the computation resources, whereas RSUs and APs serve as gateways between vehicles and MEC. Multiple RSUs/APs share the resources of a single MEC server to ensure cost effectiveness and efficient usage. Typically, vehicles and other roadside equipment (e.g., street cameras) are primary consumers of MEC resources. Vehicles communicate with the nearest RSU/AP and request hosting its computation at the MEC server. The corresponding AP/RSU forwards the request to the server for further processing. In a typical architecture, the MEC server is orchestrated by a controller that allocates computation resources (CPU time, CPU core, etc.) for each request. In IVEC, a trained machine learning policy is utilized for allocating resources in dynamic environments.

Threat Model

Understanding the probable threats in IVEC is mandatory to devise countermeasures and defend IVEC from cyber-attacks. The possible attack vectors are stated in the following sections.

Fake/Forged Feedback: In IVEC, RSUs/APs work as gateways, whereas in a vehicular ad hoc network (VANET) [13] RSUs/APs are considered as semi-trusted entities. The RSUs/APs usually relay service requests and computation results between vehicles and edge servers. Moreover, edge computing is considered as black box computing since the clients (e.g., vehicles) do not have access to the computation process. Hence, adversaries might target vulnerable RSUs/APs to manipulate computation results, which may have severe consequences in the operation of the service-requesting vehicle. This type of attack exploits the lack of verifiability and transparency in the system.

Free Riding: Free riding means providing fake computation results to clients without performing any computation due to a lack of available resources. This type of adversarial attack is conducted by the server controller to gain excessive incentives (e.g., monetary value). This can also lead to severe consequences for the client's vehicle. Such attacks are prevalent due to the centralized orchestration process and the absence of appropriate resource orchestration monitoring mechanisms.

Unfair or Biased Resource Allocation: Unfair or biased resource allocation is defined as providing additional privilege (in terms of computation resources in the server) to specific clients while violating the regulations of resource allocation policy. This type of discrimination can occur by allocating additional resources for a specific service request or incrementing allocation frequency compared to similar requests/clients. This type of attack occurs if the server controller gets com-

promised. Such attacks persist due to the lack of transparency in the resource allocation process.

Applications of IVEC

Deployment of IVEC enhances the capabilities of smart vehicles in various aspects. Some key IVEC application scenarios are stated below.

Real-Time On-Road Safety Assurance: Safety-critical data, collected from on-road vehicles and roadside sensors, is required to be processed within the shortest possible time. In this respect, IVEC can provide a platform to process such data and disseminate the extracted knowledge (e.g., safety message) to respective vehicles. For instance, an on-road traffic camera can offload collision/accident images to the nearest IVEC infrastructure for processing, and the IVEC can process the images, detect collision/accident, and transmit the alert message to surrounding vehicles. Therefore, on-road vehicles can change lane or avoid that area in order to circumvent any unwanted situation.

Entertainment Services: Smart vehicles are equipped with diverse onboard entertainment services such as augmented reality, gaming, and video surfing. These services cause high computation and storage burden to the network. IVEC can serve as a caching platform to provide low-latency service to end users, thus enhancing user experience.

Traffic Flow Management: In large metro areas, such as New York and Los Angeles, traffic congestion is an unavoidable occurrence, which caused a loss of US$87 billion in 2018 in the United States alone (https://inrix.com/press-releases/scorecard-2018-us/). In this respect, IVEC can collect the status of vehicles in terms of speed, location, weather, and road condition, and provide flow management recommendations to RSUs by calculating the predicted flow rate through different regions. However, traffic flow management recommendation is a latency-tolerant application. Hence, IVEC is a suitable candidate to perform such tasks.

Real-Time Path Navigation: Optimal navigation path calculation is an exciting feature of modern autonomous vehicles. It reduces both fuel cost and navigation time. However, the calculation of an optimum navigation path requires the processing of a high amount of sensing data, which can cause an unwanted burden on host vehicles. Being at the edge of the network, IVEC can provide real-time navigation recommendation service to vehicles while eliminating storage and processing cost of resource-constrained vehicles.

Hosting Resource-Intensive Applications: Modern autonomous vehicles utilize AI-based resource-intensive applications for tasks such as fuel scheduling, object recognition, augmented reality, platoon head calculation, and convoy control. However, such applications are highly computation-intensive and cause a huge burden onboard vehicles, whereas IVEC can host such applications and provide real-time service to end users.

Overview of Blockchain

To understand the utility of a blockchain network in IVEC, we demonstrate the features and applications of a blockchain network in this section.

Blockchain Architecture

Blockchain, a subset of distributed ledger technology (DLT), is a chain of blocks in which security is ensured by connecting the hash values of two consecutive blocks. It is a distributed database system where multiple participating parties reach consensus regarding the ledger's state change, thus making the system decentralized. A consensus mechanism, including proof of work (PoW) [8], proof of stake (PoS) [14], practical Byzantine fault tolerance (PBFT) [15], and so on, are used to select the block proposing node (miner) during each update period. Each block contains a predefined set of transactions that is verified by the miner. However, the contents of each transaction vary according to the application and design requirements. Usually, transactions are stored in Markle tree leaves within each block.

Blockchain Features

Blockchain offers some exciting features for decentralized systems such as immutability, fault tolerance, transparency, and consistency. Blockchain possesses the potential of decentralizing businesses while eliminating the need for any central authority in transferring assets within business participants. This attribute has attracted stakeholders to deploy blockchain in diverse industries such as automotive, finance, and supply chain.

Immutability: The core feature of blockchain-based systems is tamper resistance. In blockchain, every transaction is validated with a consensus mechanism, making the distributed ledger tamper-proof given that any manipulation in transactions would be detected promptly by other participants. The immutability property is ensured by utilizing the property of hash functions.

Transparency/Auditability: As transactions are stored in a tamper-proof ledger, and each participant in the network contains a complete replica of the ledger, any participant can verify or audit any blockchain address/transaction. Hence, blockchain can bring transparency among network participants regarding the activity of each participant.

Fault Tolerance: Every blockchain-based system is tolerant of faults to a certain extent (e.g., majority). The double-spending problem in the monetary transaction system is eliminated in the blockchain network through the consensus process. As every node in the network holds an identical copy of the complete ledger, data manipulation can be detected promptly.

Consistency: Unanimity in the distributed ledger is confirmed through a unanimous consent process: consensus. Hence, the ledger status of peer nodes remains consistent throughout system lifetime.

Types and Applications of Blockchain

Blockchain can be divided into three main types: public, private, and consortium. In a public blockchain, every node is equally privileged, and anyone can possess the complete ledger copy. Private blockchain consists of authorized participants, and each participant contains predefined access privileges. The access permission is configured based on three different matrices: read (access to the ledger), write (generate transaction), and commit (disseminate blocks). On the other hand, consortium blockchain is built on a permissioned network where a certified participant dominates the chain.

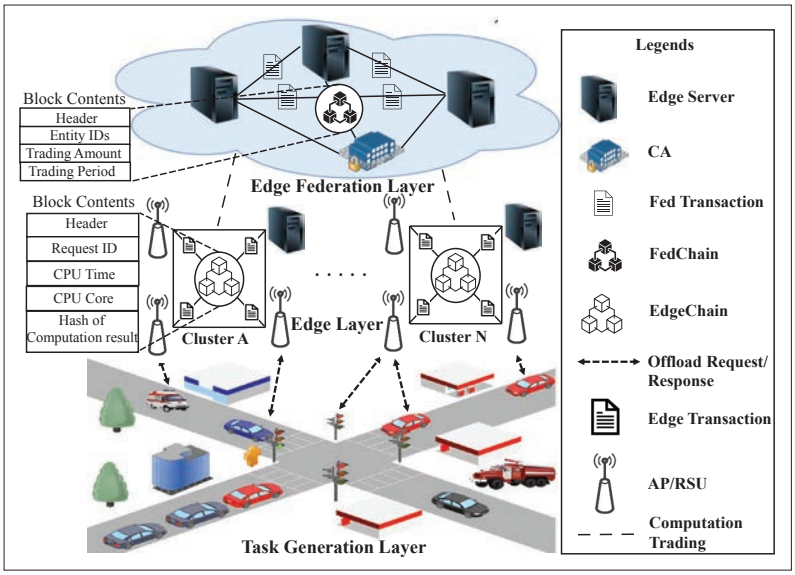

FIGURE 2. High-level architecture of the proposed IVEC system.

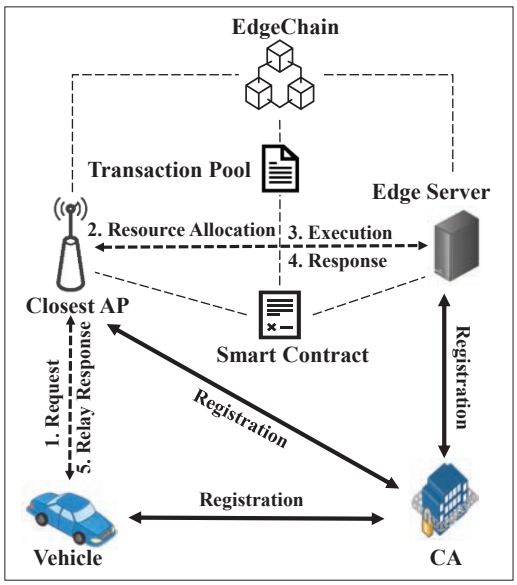

FIGURE 3. Service processing flow.

The recent advances in blockchain technology have attracted multiple industry stakeholders in deploying decentralized systems. Some of the use cases include but are not limited to trustless digital currency, smart-contract-based industry automation, trustless voting application, and decentralized digital marketing.

Proposed Architecture

In this section, we describe a high-level view of the proposed architecture that embeds blockchain network with IVEC infrastructure. We present the architecture in a bottom-up manner, starting from task offloading request to computation trading and the detailed procedure of block creation and addition to blockchain.

Hierarchical Model

In the proposed decentralized system, we adopt a hierarchical architecture, as illustrated in Fig. 2. The bottom layer, referred to as the task generation layer, consists of smart vehicles and roadside equipment (RSE, e.g., a street camera), which generates resource-intensive computing tasks for edge infrastructure in a continual manner. This layer initiates the transaction process through service offload request. We consider each offload task as a service for edge infrastructure. In the mid-layer/edge layer, a permissioned chain (EdgeChain) is formed by multiple RSUs/APs and corresponding edge servers within a predefined region. EdgeChain stores data related to each service request, such as server resource allocation amount (e.g., CPU time/core), hash of computation results, and identities of related entities and timestamps. This chain ensures transparency in resource orchestration and automates each process through smart-contract-based mechanisms to reduce human intervention. To balance loads within edge servers, an edge federation layer is formed on top of the edge layer. This federation layer consists of multiple edge servers together with a certificate authority (CA), while the entities form a permissioned network to store trading information into FedChain (a consortium blockchain formed by entities of the federation layer). A description of each layer is described in the following sections.

Service Processing Flow

Vehicles and RSEs generate edge tasks (service requests) depending on their operation. Each service request is forwarded to the nearest RSU/AP for further processing. We assume that each RSU/AP is equipped with a trained machine learning model and dynamic resource allocation policy to ensure fair resource allocation for each request, thus making the RSU/AP an intelligent entity. The task generation rate of each vehicle is independent of others. Therefore, the service request rate in different RSUs/APs is also independent of others. The server is located either at the mobile base station (MBS) or at the core network's edge. It is assumed that multiple APs/RSUs share common edge server resources. Vehicles/RSEs and APs/RSUs communicate through dedicated short-range communications (DSRC) protocol or other standard mobile networks.

Figure 3 illustrates a detailed service processing flow. In this architecture, vehicles/RSEs, servers, and RSUs/APs are registered to a certificate authority (CA), thus creating a permissioned network for service processing. A smart contract is deployed within the RSU/AP and server to automate the transaction update process. Transactions are stored in EdgeChain, and each participant node (e.g., RSU/AP and edge server) contains a complete copy of the ledger. Vehicles/RSEs are the clients of EdgeChain, and they hold the privilege of querying any transaction to participating nodes. In this architecture, servers execute services, and reply with computation results to corresponding RSUs/APs. At the same time, the RSU/AP determines resource amount (e.g., CPU time, CPU core) and relays the response to the requester (e.g., vehicle or RSE).

Figure 4 illustrates the transaction processing time of the EdgeChain network. In this EdgeChain network, we assume that the network contains four access points (or RSUs) along with a single edge server. We also assume that each vehicle in the network has an equal probability of sending

an offloading request to the edge server. From Fig. 4, we can observe that as we increase the transaction number in the network, the transaction latency is also increasing, which illustrates the bottleneck (in terms of scalability) of the EdgeChain network. To overcome this scalability issue, the EdgeChain network is expected to be adaptable with different transaction throughput optimization techniques (i.e., dynamic selection of block size and block generation frequency, off-chain solutions, etc.), which will make the network scalable to large numbers of transactions.

Computation Trading

The load pattern in different edge servers depends on the corresponding traffic flow in that region. However, traffic flow is an independent event. Hence, the load pattern for different servers is time-variant, which may lead to unbalanced load distribution throughout the IVEC infrastructure. To combat such circumstances and reduce service latency while serving excessive loads, it is necessary to expand the computation capability of edge servers in either the horizontal or vertical dimension. Moreover, vertical expansion causes communication latency; thus, increasing serving delay can become counter-productive. Therefore, horizontal maturation is imperative in IVEC in order to cope with growing service demand rates.

Figure 5 illustrates proposed computation trading process in IVEC infrastructure. In the architecture, the idle VEC server is defined as the server that possesses excessive computation capacity compared to its service request at a particular instance, whereas the scarce server is short of computation resources to serve its offload requests. We assume that an aggregator unit is established in the CA to determine appropriate matches for load balancing while considering other factors including distance between servers, available communication links, and so on. It is also assumed that the trading process is initiated periodically. As the federation layer's network is permissioned and the entities use pseudonym certificates issued by CA for authentication, it is obvious that CA is a completely trusted entity. In the architecture servers, both scarce and idle nodes and CA are full nodes of permissioned FedChain, and each of the participants contains a complete copy of the ledger. In FedChain, blocks store information related to each trading event such as ID of trading entities, trading duration, and trading amount (in terms of CPU time/core, request amount). The participants can utilize this ledger for verifying whether the appropriate match entities are engaged in trading or not, and if any entity is violating trading conditions. Moreover, FedChain can also be used for exchanging incentives within trading parties and verifying those exchanges in future terms.

Consensus Mechanism

Two fundamental performance matrices of any blockchain network is scalability and robustness, whereas these two matrices are highly dominated by consensus protocol. The proposed IVEC infrastructure deploys two different permissioned blockchain networks, EdgeChain and FedChain. The conventional PoW-based consensus protocol is not suitable in vehicular networks due to its resource-intensive hash calculation process. In a permissioned network, PBFT and PoS-based mechanisms are popular. However, PBFT creates a communication burden in the network at a polynomial scale with the increase in the size of the consensus committee.

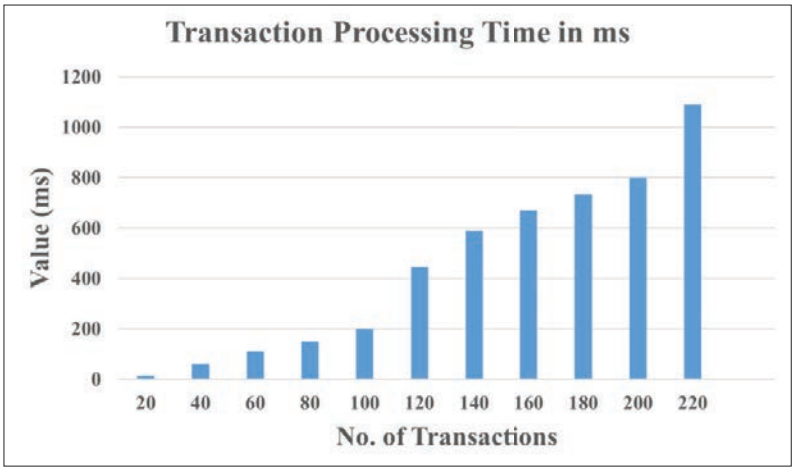

FIGURE 4. Transaction processing time in milliseconds.

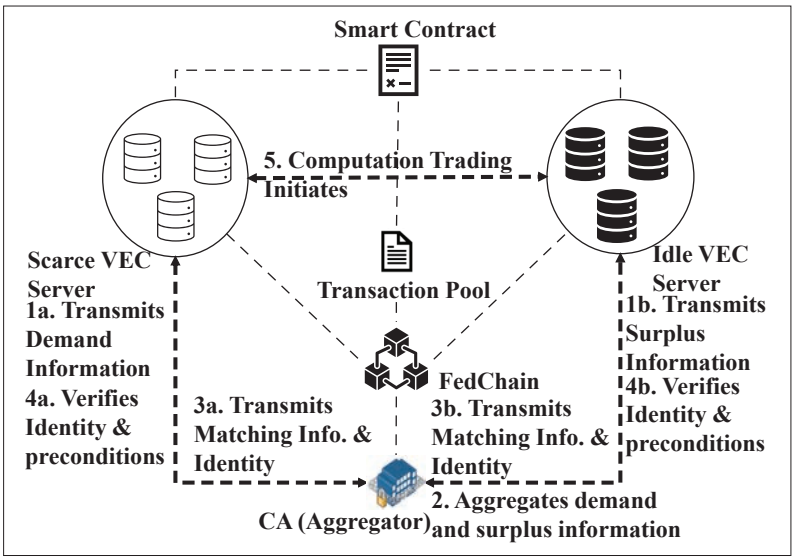

FIGURE 5. Computation trading procedure.

In FedChain, as the participants (e.g., server and CA) of this network are well resourced (compared to other entities in the vehicular network), PBFT consensus protocol can be deployed as the consensus protocol within this network. In this regard, we assume that FedChain entities are connected through a high throughput communication link. On the other hand, major participants of the EdgeChain network (e.g., RSUs/APs) are resource-constrained devices. Hence, deployment of PBFT without any modification would cause additional communication overhead in the network. Therefore, we develop a proof of vehicular services (PoVS)-based consensus committee formation protocol to minimize committee size at each tenure. In the following, we describe the characteristics of PoVS, which is illustrated in Fig. 6. In brief:

- In PoVS, the RSUs/APs that work with integrity should have a higher reputation value.

- Successful service providing rate is considered as a performance matrix for determining reputation value.
- Based on reputation values, a consensus committee is formed for specific tenures, and each entity needs to be re-evaluated for other tenures to make the selection process fair.
- The PoVS protocol assumes that CA contains an aggregation unit (AU) that aggregates, calculates, and broadcasts reputation values for committee formation.

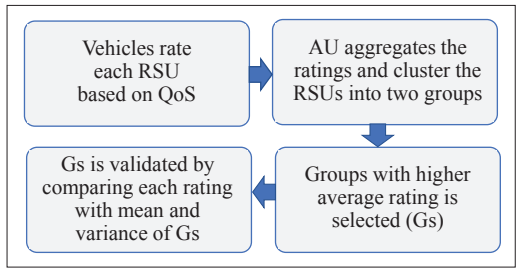

FIGURE 6. Illustration of PoVS protocol.

Technical Requirements

In order to deploy the proposed architecture, a vehicular network must be equipped with high-performing edge servers along with secure connectivity, which are expected within peer edge servers with high-throughput connections. Moreover, the vehicular network is required to be capable of handling high throughput traffic in dense areas where a large number of vehicles simultaneously offload tasks to edge servers.

Open Issues and Research Perspective

Integration of blockchain in IVEC possesses attractive benefits such as decentralization, transparency, and verifiability. However, it has drawbacks as well, which need to be resolved for efficient deployment. This section describes the integration along with related research challenges in the edge computing and blockchain domains.

Limitations of Permissioned Chain

Despite its divergent advantages, the consortium (permissioned) blockchain network entails drawbacks due to its semi-decentralized notion. Consortium blockchain exhibits properties of centralized architecture as a certified group of members dominates the network. Moreover, consortium chains use resource-saving lightweight consensus protocols suitable for resource-constrained devices; however, they pose the possibility of committing forged transactions if a good portion of certified individuals is compromised, thus subjecting the edge computation process to hijacking attacks. Therefore, there must be further investigation of the pros and cons of deploying different types of chains (permissioned, hashgraph, etc.) in the IVEC network and adopting a resilient but scalable consensus protocol. In this regard, developing a robust mining node selection protocol for a scalable consensus mechanism can be an exciting research direction.

Untrustworthy Vehicular Nodes

Compromised vehicular nodes may offload fake tasks to edge servers that may consume significant edge servers' resources, impeding legitimate users from leveraging edge resources. However, this opens up multiple exciting research directions. One possible approach is to analyze the interaction of vehicles with edge infrastructure through game-theoretic models and utilization of multi-agent reinforcement learning (RL) for filtering out fake task requests. In this case, machine learning models can be applied to analyze network traffic, learn the pattern, and detect traffic requests from illegitimate users. Moreover, a reputation-based vehicle node classification method can be adopted to identify malicious vehicles from legitimate vehicles. In this regard, it is expected that vehicles which perform according to the edge computing protocol will have higher reputation value. Multiple different techniques can be utilized, including Bayesian-network-based reputation evaluation, neural-network-based calculation, and so on, to calculate the vehicles' reputation values.

Flexible Operation

Although blockchain is a decentralized system, it requires intervention at different stages of its operation. For instance, the block size and the difficulty level of the puzzle (in terms of PoW) in Bitcoin relies on human operators. Moreover, in the wireless blockchain network (e.g., vehicular blockchain), block size has a dynamic relationship with transaction throughput. Therefore, the static determination of such hyperparameters is not suitable. Hence, a dynamic operation mechanism must be devised to minimize human intervention and enhance network throughput. In this regard, interested researchers can investigate whether machine-learning-model-based dynamic network parameter selection in vehicular blockchain enhances utility (in terms of transaction throughput and latency) or not.

Double Spending Elimination

In the bitcoin network, double spending is checked by verifying the balance in the sender's wallet address. This type of verification is not straightforward for vehicular applications. Moreover, counterfeit transactions can consume significant edge resources, which can deteriorate the edge computing efficacy. Hence, devising a verification mechanism in IVEC in order to eliminate broadcasting fake transactions is a challenging task. In order to formulate an appropriate verification mechanism for vehicular applications, analyzing the interaction of different roles in the blockchain network is required. Therefore, game theoretic approaches can be applied to analyze the interactions by deploying multiple different attacker-defender scenarios. Thus, we need to formulate an effective and efficient transaction verification method for vehicular applications.

Load Balancing

Unbalanced load distribution in an edge server causes inefficient resource utilization, as the overloaded server cannot serve legitimate users, whereas underloaded servers remain idle. Edge computation power can be increased in two different ways: horizontal expansion (e.g., edge federation) and vertical expansion (e.g., increasing server size/number or federation with cloud) to provide services to excessive requests. However, vertical expansion causes either deployment cost

or service latency. On the contrary, horizontal expansion does not require deploying additional resources. Latency does not increase significantly as services are still executed in the edge network but on different servers. In the proposed architecture, we propose a computation trading model for creating edge federation at IVEC to minimize the effect of uneven load distribution and utilize most of the available edge resources efficiently. In this regard, the development of an appropriate incentive mechanism for horizontal expansion can be an exciting research direction where game-theoretic approaches can be applied to analyze inter-server interaction.

Privacy Preserving Analytics

In the proposed architecture, vehicles may offload different personally identifiable information (PII), including credit card information, trajectory map, destination, and so on, to edge servers for accomplishing different tasks. However, such information poses the threat of revealing daily habits of vehicle owners, which is undesirable. Therefore, instead of offloading/querying to the edge server in plain-text, vehicles can offload/query in ciphertext mode. However, conducting analytics on cipher-text is a time-consuming operation. In this respect, research can be conducted on quickening the homomorphic computation techniques to develop new privacy-preserving protocols for edge computation offload or querying. Moreover, the proposed EdgeChain and FedChain do not store any such PIIs of vehicle users, and thus preserve the privacy of vehicle owners.

Conclusion

The integration of AI and vehicular edge computing (VEC) creates an enormous opportunity for leveraging edge resources to process high-volume vehicular data. However, the existing works faial to investigate issues (e.g., bias/unfair resource allocation, free riding, forged output) related to lack of transparency in IVEC. In this regard, the integration of IVEC infrastructure and blockchain technology is persuasive due to its features such as immutability and auditable interaction. In this article, we present blockchain-based hierarchical IVEC architecture to enhance transparency in resource management and leverage edge clients (e.g., vehicles and RSEs) with computation verification options. Furthermore, we propose a secure computation trading model in IVEC for expanding edge computation power in the horizontal dimension in order to efficiently manage unbalanced load distribution. We also describe security vulnerabilities in IVEC infrastructure and conclude with some exciting and state-of-the-art research directions in the domain of edge computing and blockchain.

References

[1] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of Vehicles: Architecture, Protocols, and Security," *IEEE Internet of Things J.*, vol. 5, no. 5, 2018, pp. 3701–09.

[2] N.J. Nilsson, *Principles of Artificial Intelligence*, Morgan Kaufmann, 2014.

[3] N. Abbas *et al.*, "Mobile Edge Computing: A Survey," *IEEE Internet of Things J.*, vol. 5, no. 1, 2017, pp. 450–65.

[4] H. Peng *et al.*, "Deep Reinforcement Learning Based Resource Management for Multi-Access Edge Computing in Vehicular Networks," *IEEE Trans. Network Science and Engineering*, 2020.

[5] Z. Ning *et al.*, "Mobile Edge Computing-Enabled Internet of Vehicles: Toward Energy-Efficient Scheduling," *IEEE Network*, vol. 33, no. 5, Sept./Oct. 2019, pp. 198–205.

[6] Y. Wang *et al.*, "Traffic and Computation Co-Offloading With Reinforcement Learning in Fog Computing for Industrial Applications," *IEEE Trans. Industrial Informatics*, vol. 15, no. 2, 2019, pp. 976–86.

[7] Z. Ning *et al.*, "Intelligent Edge Computing in Internet of Vehicles: A Joint Computation Offloading and Caching Solution," *IEEE Trans. Intelligent Transportation Systems*, 2020, pp. 1–14.

[8] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Manubot, Tech. Rep., 2019.

[9] O. Bouachir *et al.*, "Blockchain and Fog Computing for Cyberphysical Systems: The Case of Smart Industry," *Computer*, vol. 53, no. 9, 2020, pp. 36–45.

[10] M. Baza *et al.*, "BRide: Ride Sharing with Privacy-Preservation, Trust and Fair Payment atop Public Blockchain," *IEEE Trans. Network Science and Engineering*, 2019.

[11] L. Tseng *et al.*, "Blockchain for Managing Heterogeneous Internet of Things: A Perspective Architecture," *IEEE Network*, vol. 34, no. 1, Jan./Feb/ 2020, pp. 16–23.

[12] I. A. Ridhawi *et al.*, "A Blockchain-Based Decentralized Composition Solution for IoT Services," *Proc. IEEE ICC*, 2020, pp. 1–6.

[13] H. Hartenstein *et al.*, "A Tutorial Survey on Vehicular Ad Hoc Networks," *IEEE Commun. Mag.*, vol. 46, no. 6, June 2008, pp. 164–71.

[14] J. Kang *et al.*, "Incentivizing Consensus Propagation in Proof-of-Stake Based Consortium Blockchain Networks," *IEEE Wireless Commun. Letters*, vol. 8, no. 1, 2019, pp. 157–60.

[15] O. Onireti *et al.*, "On the Viable Area of Wireless Practical Byzantine Fault Tolerance (PBFT) Blockchain Networks," *Proc. 2019 IEEE GLOBECOM*, 2019, pp. 1–6.

Biographies

Shafkat Islam is currently pursuing a Ph.D. in computer science and engineering at the University of Nevada, Reno. He received his M.S. in informatics (with Distinction) from Northern Arizona University in 2019. His current research interests include cybersecurity, machine learning, and blockchain.

Shahriar Badsha is currently serving as an assistant professor in cybersecurity in the Department of Computer Science and Engineering at University of Nevada, Reno. He completed his Ph.D. in computer science and software engineering from RMIT University, Australia. He was also with data61, CSIRO, in Melbourne, Australia.

Shamik Sengupta is currently the executive director of the UNR Cybersecurity Center at the University of Nevada, Reno. He is also serving as an associate professor in the Department of CSE. He has authored over 150 research papers. He was awarded Ralph E. & Rose A. Hoeper Professorship Award in 2019.

Hung La is an associate professor of CSE at the University of Nevada, Reno. He is also the associate director of the INSPIRE Tier 1 University Transportation Center. He has authored over 116 research papers, and eight of his papers have won best conference paper awards and best paper finalists in the top ranked robotics conferences (IROS 2019, SSRR 2018, ICRA 2017, ISARC 2015, etc.).

Ibrahim Khalil is currently an associate professor in the Department of Computer Science and Software Engineering at RMIT, Australia. He obtained his Ph.D. from the University of Berne, Switzerland, in 2003. He has several years of experience with Silicon Valley companies. He also worked with EPFL and the University of Berne and Osaka University, Japan.

Mohammed Atiquzzaman is the Edith Kinney Gaylord Presidential Professor in the School of Computer Science at the University of Oklahoma, Norman. He is the Editor-in-Chief of the *Journal of Networks and Computer Applications*, the founding Editor-in-Chief of *Vehicular Communications*, and has served on the editorial boards of many journals, including *IEEE Communications Magazine*, the *IEEE Journal on Selected Areas in Communications*, and so on.