AI, Blockchain, and Vehicular Edge Computing for Smart and Secure IoV: Challenges and Directions

Ahmad Hammoud, Hani Sami, Azzam Mourad, Hadi Otrok, Rabeb Mizouni, and Jamal Bentahar

Abstract

Internet of Things (IoT) is turning into an undeniably developing point of discussion in both research and industrial fields. A key area that is witnessing a quick development in the utilization of IoT devices is the Internet of Vehicles (IoV), which allows information exchange among vehicles and infrastructures. Notably, Artificial Intelligence (AI) has been widely adopted for solving challenging vehicular problems and managing the IoV infrastructure. Despite the advantages AI carries for IoV, its deployment can be negatively affected by lacking computation resources and processing unreliable data. On the other hand, Blockchain is a decentralized and distributed peer-to-peer network architecture that can be employed to empower security and resist against undesirable data modification. However, integrating both technologies (i.e., AI and Blockchain) exhausts, even more, the IoV infrastructure. Therefore, we present in this paper an overview discussing the AI and Blockchain approaches and models for IoV and propose a new Vehicular Edge Computing based architecture embedding both technologies and overcoming the aforementioned limitations. We then discuss the main challenges and give notice to the concerned parties and stakeholders about promising directions that arise from enabling the three technologies for providing smart, secure, and efficient IoV.

Introduction

With the increasing need for generating data and computational tasks on vehicles and the rapid development of Internet and communication technologies, the Internet-of-Vehicles (IoV) concept arose to be one of the hottest topics nowadays. IoV is a distributed network that utilizes the data generated by vehicles to improve safety on the road for smart cities. It enables smart Vehicle-to-Everything (V2X) communication allowing the interaction of vehicles with other heterogeneous networks [1].

The new generation of vehicles embeds complex applications that require intelligent decision making. Hence, the advancement of Artificial Intelligence (AI) derived its path into IoV, yielding the innovation of smart vehicles. This emergence attracted many industries to invest in AI for IoV applications such as real-time navigation systems, autonomous driving, street surveillance, and other safety-related systems. For instance, Google has launched its project for self-driving vehicles using AI, where they used images, beams of radar, lidar, ultrasound, GPS navigation, and central computing to identify objects and predict behaviors accurately [2]. Consequently, the number of smart vehicles in IoV is going to increase in the upcoming years drastically. Therefore, careful consideration must be taken in order to manage the IoV infrastructure efficiently. In addition, after the emergence of modern applications in smart vehicles, Vehicular Edge Computing (VEC) came to meet the vehicles' demands for computation. VEC is composed of computation devices residing on roadsides or in proximity to the vehicles. Such architecture facilitates communication, computation, and data sharing among vehicles. This results in avoiding the delays in communicating with the cloud, which is more convenient for dynamic environments such as IoV. Hence, meeting the large computation demands can be done using AI to optimally decide and schedule tasks that need to be offloaded to the VEC infrastructure and properly manage the network usage. Here also comes the advantage of AI to solve such challenging problems considering the random or unexpected states that can be generated by vehicles.

Additionally, with the increasing number of automated vehicles, the burden of security, privacy, and trust fears has spread, affecting the industry finance and customer trust [3]. In parallel, Blockchain is a decentralized ledger that entails a high level of trustworthiness and availability. Correspondingly, the integration of Blockchain within the IoV has started to gain attention lately. It was essentially integrated by scholars to maintain high data credibility among vehicles, enabling traffic safety and efficiency. Many manufacturers are considering this framework to improve the driving experience [4].

Further, the expected large number of smart vehicles embedding several AI models obligates the need for a rich source of computation power. Simultaneously, employing Blockchain in such an environment raises many questions regarding its feasibility due to its high demand for resources. To the best of our knowledge, no research efforts have addressed the aforementioned limitations combined. Therefore, a need for integrating AI's learning process with a scalable Blockchain implementation within the same architecture arises for enabling smart, secure, and efficient IoV. In this regard, we propose a new VEC-based architecture embedding both AI and hybrid Blockchain models for:

1. Increasing the accuracy of IoV intelligent applications affected by lacking computation resources and processing unreliable falsified data.
2. Efficiently managing the IoV infrastructure resources to enable the successful deployment of both technologies.

Regardless, this synergy raises many limitations that need to be addressed for realizing the proposed architecture. Accordingly, we elaborate on a thorough list of challenges and research directions.

This article is organized as follows. We present the typical IoV architecture and emphasize the AI role within. We give an overview of Blockchain and its advantages in IoV, supported by some research work. We propose a VEC-based architecture integrating AI and Blockchain on different layers within IoV. Then, we open the doors for challenges caused by this combination and propose future research directions. Finally, we conclude the article.

Emergence of AI within IoV

In this section, we present the typical IoV architecture and its components, followed by an overview of the current industrial and research directions utilizing AI for achieving intelligence in IoV applications and efficiency in managing IoV resources.

Digital Object Identifier: 10.1109/IOTM.0001.1900109

2576-3180/20/$25.00 © 2020 IEEE

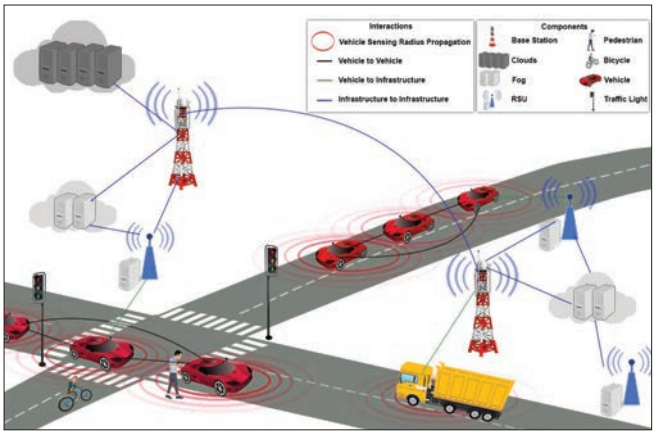

FIGURE 1. IoV architecture.

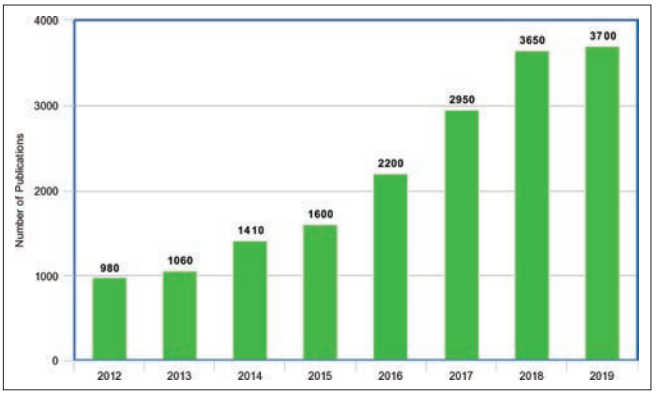

FIGURE 2. AI usage in IoV in terms of publications.

IoV Architecture

Ultimately, IoV is the consolidation of the Internet and IoT along with vehicles, enabling smart communication between vehicles and other heterogeneous networks to provide drivers and passengers with a variety of services [5]. Figure 1 summarizes the components and their interactions. Initially, vehicles offer computational capabilities within their On-Board Units (OBUs). In particular, the OBU can benefit from data generated by the integrated sensors (e.g. camera, GPS, radar) to assist the driver in making a certain decision. For instance, sensors can detect a possible collision with an object (e.g. pedestrian or bicycle). A warning can be sent to the driver accordingly to advocate on being cautious to unwanted interference.

As observed in Fig. 1, there exist several types of communication networks in this topology:

Vehicle-to-Vehicle (V2V): In V2V, vehicles are connected wirelessly to share information and create 360-degree awareness of other vehicles in proximity. With such connectivity and cooperation, the number of crashes will be reduced, as the self-driving vehicle (or the driver) will be alerted to take actions.

Vehicle-to-Infrastructure (V2I): V2I is considered to be a two-faced communication network. The infrastructure serves the car in bi-directional communication. In Intelligent Transportation System (ITS), travelers are linked to the available nearby VEC infrastructure, e.g. Road-Side Unit (RSU) and Base Station (BS), feeding it with road-data according to their destination to enhance their driving experience. From the other side, the VEC infrastructure plays a secondary role in assisting the OBUs in computational processing. The offloading technique is used to transfer tasks from vehicles to infrastructure due to resource-shortage a vehicle may suffer from. Once the task is processed, the infrastructure returns the execution result to the vehicle.

Infrastructure-to-Infrastructure (I2I): I2I is depicted by having infrastructures connected together in order to facilitate computation and network load-balancing and share information. Mainly, the components in such a communication network consist of a set of BSs, RSUs, Fog servers, and Cloud servers.

Intelligent IoV Applications

AI is being applied in a wide spectrum of areas and applications trying to solve complex and challenging tasks that usually require human intervention. Therefore, AI contributed in solving challenging vehicular tasks, which resulted in advancing the vehicular industry and its economy. Self-driving excels because of revolutionary advancements of AI in these IoV applications, including speed changing, objects detection, building trajectory, lane changing, real-time navigation, traffic light control, and video surveillance [6]. On the industrial level, Argo AI, Cruise, Waymo, and Aurora are examples of leading companies in developing autonomous-driving vehicular systems coping with the fast-growing self-driving research field. These companies were able to bring theory into reality by counting on sensed data and radars to identify objects, predict others actions, and build future trajectories up to three football fields distance. After the unprecedented success in self-driving technology, some influential players in the vehicular industry such as Hyundai, Audi, Mercedes, and BMW started integrating auto-piloting features into their new models at high prices after gaining customer's trust through several successful prototypes [7].

In order to contextualize the importance AI is bringing to the field, we consider some scenarios elucidating on its main strength in solving IoV challenges. Considering a car in auto-piloting mode, the car collects the needed data before it starts moving on the road. In the simplest way, this can be done by continuously sending 360 beams of radar to predict, identify, and make decisions. Feeding these data to an AI model, which can be a combination of multi-agent Reinforcement Learning (RL), game-theoretical decisions, or logical reasoning, the vehicle can identify its current position on the road and is capable of understanding its surroundings. This is made through AI by identifying different types of objects, such as the traffic light color, moving pedestrians, objects crossing the road, and static objects. Furthermore, AI is used to plan or take instant actions. Examples of decisions can be turning left or right, speeding up or down, changing lanes, deciding on a break level when needed, or an immediate stop to avoid accidents. Additionally, predicting the behavior of neighboring drivers and objects is a crucial model supporting self-driving. In summary, AI is serving the IoV by deciding on a trajectory to follow through object detection, decision making, and behavior analysis. To academically study how AI is attractive within IoV, we show the number of publications by exploring the search results of Google Scholar[1] for the keywords "Internet-of-vehicles" or "self-driving" with the term "AI." As noticed in Fig. 2, the number of publications is huge and increasing every year.

IoV Infrastructure Management

Vehicles are becoming smarter; however, such intelligence comes at the cost of requiring complex computation that significantly utilizes IoV resources. Even though smart vehicles nowadays are embedded with computation resources or OBUs, these resources might not be enough to meet all the complex applications that are becoming more demanding. To overcome such limitations, recent works are proposing to offload vehicular tasks to VEC, which is a challenging decision to make under different constraints and mobility conditions [8]. A computation offloading problem on the Edge consists of a set of tasks, each having services and inputs that are sent to available connecting Edge. A basic Edge serving the IoV is formed of BSs, RSUs, and computing servers, while some other works use vehicles as part of it [9]. At one point, the Edge infrastructure might receive multiple offloading tasks at the same time. Having limited avail-

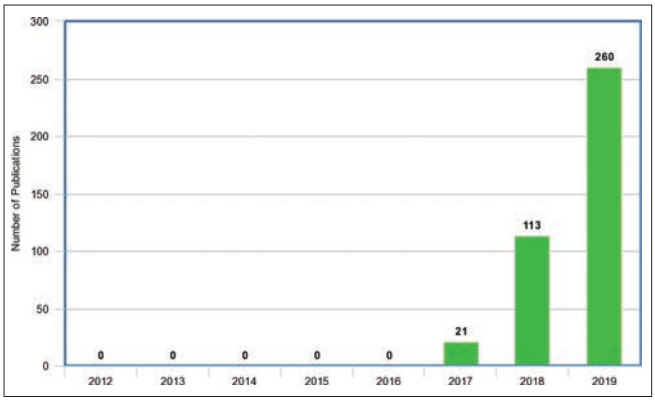

FIGURE 3. Blockchain usage in IoV in terms of publications.

able resources, the authors used AI, i.e., a RL model named Deep Q-Learning, to distribute the tasks among edge resources in the order of importance [8]. The importance of tasks distribution is defined by a cost factor which changes depending on the perspective of the AI offloading solution.

Consequently, the number of tasks to be offloaded from the same location and time can be large. Thus, managing network resources and scheduling its traffic is another challenge to be dealt with. To complicate things, the dynamics of vehicular networks, heterogeneous network available resources, and different Quality-of-Service (QoS) requirements for every vehicle make the vehicular network management problem non-trivial to solve. Learning vehicular mobility, such as traffic flows, trajectory prediction, and wireless channel estimation, leads to refine efficient network resource management models that meet the different vehicular links requirements. The authors in [10] present an overview of the literature that uses machine learning to solve difficult vehicular network problems, where learned dynamics help in building an efficient scheduling and routing network protocol for better management of V2X connections. Network congestion control is another challenging task in dense intersections or in a traffic jam. With the increasing number of vehicular nodes connected to the VEC, congestion parameters change depending on vehicle demands to avoid data collisions. The dynamics learned also help in managing the network resources or traffic transmission scheduling in vehicular networks. For instance, the problems can be formulated as Markov Decision Processes (MDP) and solved using RL to maximize reward values and meet the requirements of the dynamic links of the global network [10].

Blockchain for Securing IoV

In parallel, Blockchain is a decentralized and distributed digital ledger that was developed as an underlying network structure for the well known secure crypto-currency system "Bitcoin" [11]. Recently, it has been adopted by a diverse set of applications, including financial services, IoT, voting systems, and healthcare [12]. Blockchain uses a fully distributed peer-to-peer architecture without relying on any centralized authority to operate. Consequently, applications and architectures that rely on Blockchain for managing their network infrastructure obtain a high level of data availability, security, privacy, and trust. For instance, Blockchain grants transparency by having all participating nodes owning a full copy of the database. Furthermore, the nodes must agree on the new transactions before updating their databases to reach consensus. Due to its massive success, Blockchain 2.0 was released, introducing many features, including the foundation of smart contracts. A smart contract is a self-executing piece of code that gets triggered once its predefined conditions are met, without relying on any trusted authority. There exist several types of derived Blockchain, each of which serves a different purpose as follows:

- Public Blockchain: A fully distributed ledger that relies on no central authority to manage. Anyone can become a member in this type of Blockchain. For instance, Bitcoin and Ethereum are public Blockchains for anonymous participation to empower their decentralization.
- Private Blockchain: A permission-based Blockchain that is mostly adopted by private organizations. It relies on a central authority to manage who can participate in this network, and restricts some participants from reading and writing inside of it.
- Consortium Blockchain: A hybrid type of Blockchain. It relies on a group of approved entities for its management. Such a type may adopt a hybrid access method, allowing the outside world to interact with it in an authorized manner. Corda and Quorum are examples of consortium Blockchain.

On the industry level, many leading automakers started considering Blockchain to ameliorate the driving experience by securely exchanging data in V2X [4]. For instance, GM and BMW[2] are considering deploying a Blockchain-based solution for sharing self-driving car data among themselves, which will fasten the existence of autonomous vehicles. Volkswagen,[3] on the other hand, is building a tracking system based on Blockchain to prevent the manipulation of the odometer done by sellers to raise the prices of their cars.

Lately, researchers have focused on integrating Blockchain within IoV for granting the latter the security and privacy it needs to function. We used Google Scholar[1] to observe the number of publications addressing the integration of Blockchain within IoV in the past few years, by exploring results containing the words "IoV" and "Blockchain" within the title or abstract. As observed in Fig. 3, the very first research efforts came to light in mid-2017. The number kept on increasing throughout the years as Blockchain proved its efficiency for supporting IoV. In particular, some works adopted Blockchain to provide data trustworthiness and credibility for enabling road-safety and efficiency. Others focused on preserving privacy for protecting drivers from any data leakage or Cyberbullying. In the following, we discuss some of these approaches:

- Empowering Security: The credibility of the broadcast messages among vehicles has attracted many research scholars lately. Some of these researchers employed the Blockchain technique to reinforce the security of the IoV paradigm by evaluating the credibility of the broadcast messages [12]. Others proposed authentication mechanisms to resist malicious attacks against IoV, enabling a safe and secure environment [5].
- Preserving Privacy: Most Blockchain implementations entail public-key encryption for privacy-preserving purposes. Consequently, Blockchain was also employed in IoV to reinforce the privacy of the drivers. Some scholars were interested in targeting how to protect the vehicles from any leakage of critically private information [13]. Certainly, by integrating the Blockchain, most communications will be encrypted, making it very hard for third parties to decrypt and extract critical information.

VEC-Based Architecture Enabling AI and Blockchain in IoV

Problem Statement

Initially, IoV applications are complex in a sense they require some advanced techniques to execute due to the unpredicted and random behavior of vehicles. Accordingly, scholars have been adopting AI to assist in the overwhelming decision-making process ever since (as discussed earlier). Despite these efforts and contributions, AI further increases the computation load on the IoV infrastructure and needs an incubating and malicious-free environment to perform as expected. Otherwise, AI can lose its reliability and threaten road-safety due to its vulnerability against cyber-attacks. Such attacks can manipulate these algorithms and disrupt their behaviors, with minimal changes, resulting in inaccurate decisions that may endanger people's lives. This is mainly due to the lack of explainability of the deci-

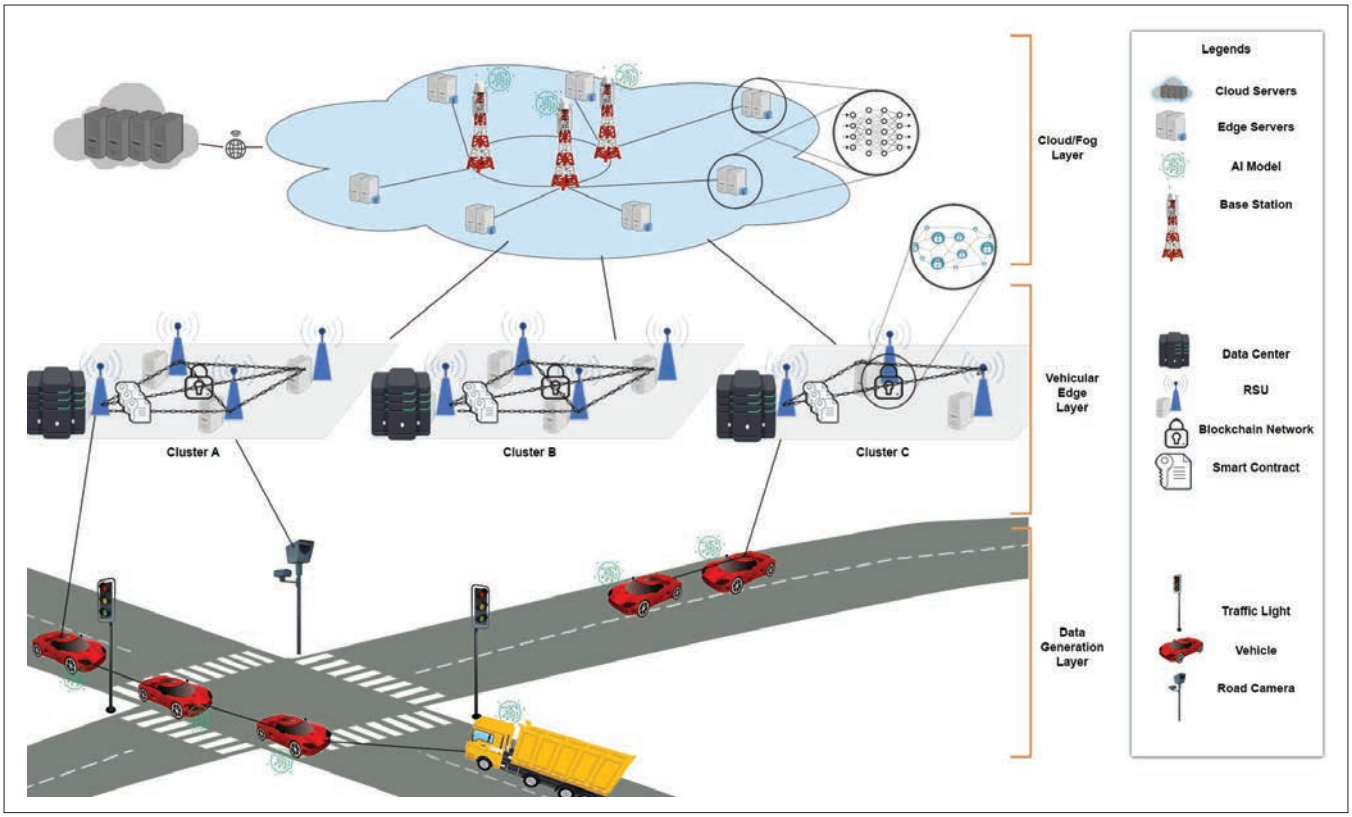

FIGURE 4. Blockchain-based VEC architecture supporting AI in IoV.

sions made by these algorithms. In this context, the integration of AI along with Blockchain entails advantages to the applications and infrastructure management, enabling decentralized, smart, and secure IoV. However, trying to overcome the above limitations by integrating Blockchain results in a higher computation load on the IoV infrastructure, which can harm its performance. Thus, there is a need for an architecture that combines both AI and Blockchain, and benefits from VEC to efficiently utilize and support the IoV infrastructure in order to meet the requirements of both technologies.

Proposed Architecture

In this section, we present a high-level view of our proposed architecture that embeds AI models with a scalable Blockchain network on a multi-layered VEC infrastructure. Figure 4 depicts how the three technologies can utilize the IoV components in three hierarchical layers: IoV Data Generation, Vehicular Edge, and Cloud/Fog. Presenting our architecture in a bottom-up fashion, we start by the different IoV components that generate vehicular data, run AI models, and execute a variety of tasks. At the Edge layer, data reliability is ensured through multiple hybrid Blockchains deployed on clusters of RSUs. After Blockchain approval, Vehicular data are managed and stored in data-centers. Moving forward, we utilize powerful fog servers connected to these Blockchains, assisted by cloud servers, to form a strong computation base to support IoV. Cloud/Fog servers execute computation tasks that are offloaded by vehicles. They are also responsible for updating vehicular AI models through learning from the new data stored in the data-centers. To elaborate further, we give below some details about the essential functionalities of each layer.

IoV Data Generation Layer: Initially, we suppose that vehicles are always connected to the Vehicular Edge, either directly or through a Master node. A vehicle (or any other IoV device, e.g., road camera) generates road data through the sensors it equips, and then sends them to the nearest RSU. In addition, this layer generates computation tasks to be offloaded to the VEC infrastructure.

Vehicular Edge Layer: The generated data needs to be stored, filtered, and then transferred securely, without being tampered, to computationally-rich servers for processing. Edge nodes, in our case RSUs, are responsible for such tasks, in addition to avoiding network congestion on higher layers due to the massive amount of data. As shown in Fig. 4, neighboring RSUs form a cluster for serving vehicles efficiently. Due to the RSU's poor storage capabilities, we assist the cluster by deploying a data-center within its reach. New data received by the RSU is forwarded to the data-center. The receiving RSU only uses metadata that references the new data for processing. To securely store data and maintain the anonymity of vehicles generating them, we propose employing a consortium Blockchain 2.0 architecture as the underlying network for each cluster of RSUs. In such a Blockchain, the used consensus method differs from the typical Proof-of-Work (PoW) that drains a lot of energy and time. Typically, it uses an efficient consensus algorithm, such as Istanbul Byzantine Fault Tolerance, Selective Endorsement, and Raft-based Consensus mechanisms, which can process a great number of transactions at higher speed rates with less energy consumed. Moreover, it enables hybrid access so that both internal and external entities are granted full or limited access, depending on their role, to manage the Blockchain and make inquiries. In this context, the Edge is responsible for a certain set of actions embedded in three distinguished smart contracts as listed below.

- Participants Authentication: In order for a vehicle to interact with the infrastructure, first the authentication contract acknowledges the connection with this vehicle. After that, it creates a profile and stores basic information about it that shall remain active while staying under the same Edge cluster coverage.
- Data Storing: This contract can differentiate among several types of sensed data. It embeds a mechanism that categorizes and labels the data to be forwarded to the data-center. Such a phase eases the process of forwarding the data collected to the various types of applications requesting it.

- Vehicular AI Models Management: Supposedly, vehicles are in recurrent communication with the Edge. Once the vehicle is authenticated, this contract gets triggered frequently to handle updating the IoV application models (such as the self-driving AI model) embedded within the vehicles whenever a new version is received from the Cloud/Fog layer. The updated model gets transferred to vehicles running the related AI application.

It is important to mention that the Blockchain only stores metadata of the data received from the vehicles, which makes our proposal more scalable.

Cloud/Fog Layer: As the challenges imply, there is a need for a secure and computationally-rich environment to do heavy processing. Typically, refining an up-to-date AI model requires heavy processing, which can be offered by the Fog servers provided by trustworthy providers. The updated models rely on new road data retrieved from the Vehicular Edge layer for updating them and increasing their accuracy due to the dynamicity of IoV. In case the fog servers are overloaded, they rely on offloading some tasks to the Clouds. AI application models are forwarded to the vehicle itself through the Edge for granting the latter an ability for instant decision generation. The resource management model can be deployed on the BSs for optimally managing the Fog servers' resources for granting satisfying QoS.

Challenges and Research Directions

Despite its advantages, the proposed architecture imposes many challenges and opens several research directions related to the three paradigms (i.e., AI, Blockchain, and VEC).

Draining IoV Infrastructure: Having traffic congestion in some locations can lead to a high volume of data being sent to the Edge. Likewise, the computation tasks generated by vehicles for offloading will increase. This causes drainage in computation, network, and storage capacities of the infrastructure and affects its performance [14]. Therefore, efficiently managing the IoV infrastructure and exploring new sources of computation is vital. In the following, we list some promising research directions.

- Elaborating intelligent model, e.g., RL used in [8], for deciding where the computation should be offloaded and how the network can be managed to enhance the efficiency of utilizing the IoV infrastructure. For instance, the computation can be sent to the fog or cloud servers. Building such a model and deciding on a reward function that takes into consideration the current servers' loads and vehicles' geographic locations is encouraging.
- Proposing on-demand formation of vehicular clusters can be a solution for aiding the IoV infrastructure by providing more sources of computation power. Further, deciding on how to form these on-demand vehicular clusters, what type of tasks they can run, and how these tasks are distributed should be considered.
- Developing an intelligent network and storage resource management approach [10] for the Edge clusters is another promising research direction. This can be possible by studying the possibility of offloading the data and tasks to other neighboring clusters. This methodology ought to consider the location of the model, the effect of data transmission on the network, and the division of tasks among several clusters after studying their capacities. In this context, the use of containers instead of virtual machines can ease the process of migration, resource scaling, and maintenance of services.
- Collecting IoV data might still be costly due to adopting a Blockchain solution. Hence, there is a need for further optimizing the cost in terms of network, storage, and computation resources in order to attract stakeholders to invest in such technology.

Fog Federation for Load Balancing: Unbalanced traffic congestion raises an important question toward the vertical resource expansion in the computation layer. Such complication results in an uneven data load sent to different Fog servers. This opens the door for further exploring solutions through horizontal maturation. To elaborate more, we advocate studying the aforementioned problem by proposing the concept of Fog Federation as a solution to overcome the resource-shortage caused by offloading big data to specific Fog locations. Such types of federations can be achieved by reaching a service-level agreement among Fog Providers.

Inconsistency and Inefficiency of AI Models' Updates: Following our architecture, an AI model is updated on fog servers, which receive data from the connected Blockchains. Running AI updates independently on separate fog clusters results in inconsistencies among AI models located in different locations and may affect the performance of the applications. Therefore, an aggregation mechanism to achieve model consistencies for the same IoV application is crucial. In order to overcome this issue, we suggest the development of a Distributed Machine Learning model that can benefit from the clustered and distributed nature of fog servers in our architecture and is capable of updating the AI models with large data received from different locations in parallel. However, careful consideration should be given to the design of the AI model used to qualify for distributed computing.

Consortium Limitations: Consortium Blockchain leverages significant advantages that may be enough to suit our VEC architecture well. Nevertheless, it entails some drawbacks due to its hybrid and semi-decentralized mechanism. On the one hand, only a certified group of members allows others to participate, leading to a state of monopolism in some cases. On the other hand, the resource-saving consensus algorithms applied for this Blockchain could lead to committing unwanted transactions to feed the AI learning process with bogus data since the consensus participants are pre-approved nodes on the network and can be subjected to hijacking attacks. This opens the door for further exploring the pros and cons of adopting a different type of Blockchain and consensus methods for IoV as an attempt to overcome these challenges.

Unreliable Vehicles: Vehicles may publicize fake data intentionally or due to a broken sensor, and feed them to the Edge [15]. The latter forwards them to the Cloud/Fog servers for model learning regardless of how trustworthy it is. In case of fake data, the model will be inaccurate and exposed to making wrong decisions. Such a challenge unravels many exciting research areas. In our proposal, the advantage of having a three-layered architecture allows us to vertically and/or horizontally refine an assessment model for the data to assist the evaluation of its trustworthiness further. An attractive direction may consist of combining a decentralized game-theoretical model, in particular security games, along with a multi-agent RL mechanism toward filtering falsified data from malicious partners. The model should also deal with conflicting data, for instance, data reporting conflicting or inconsistent traffic situations.

AI-Enabled Smart Contract: Data is generated on the user level, and gets forwarded to the Cloud/Fog for analysis. Edge resembles the man-in-the-middle for such a process to help the Cloud/Fog preprocessing the data according to the vehicle profile. However, a key challenge is to recognize unfamiliar data patterns and categorize them according to the various conditions. Possibly, an RL model might be a promising solution to overcome this problem. A feasibility study can be addressed in the future to embed an intelligent model within our Data Storing smart contract. The evolved contract will intelligently recognize and categorize new data patterns instead of having them statically defined.

Conclusion

The use of AI within IoV has gained great attention lately in the academic and industrial sectors. However, such integration requires efficient resource management mechanisms due to AI's exhaustive learning process and entails secure approaches

for generating trustworthy data. In this context, Blockchain's decentralized and security-enhancing architecture offers the aforementioned paradigm the trustworthiness it needs to function; nonetheless, it further exhausts the infrastructure. In this regard, we first elaborated on the use of AI for IoV applications and resource management, followed by Blockchain techniques addressing the security issues. We then proposed a new multi-layered hybrid Blockchain-based VEC architecture for supporting the AI integration within IoV to overcome the aforementioned challenges. Finally, we offered a thorough list of challenges and research directions that open the door for further investigation.

References

[1] O. Kaiwartya *et al.*, "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," *IEEE Access*, vol. 4, 2016, pp. 5356–73.

[2] J. Krafcik, "Say Hello to Waymo: What's Next for Google's Self-Driving Car Project," *Medium*, Dec. vol. 13, 2016.

[3] J. Cui *et al.*, "A Review on Safety Failures, Security Attacks, and Available Countermeasures for Autonomous Vehicles," *Ad Hoc Networks*, vol. 90, 2019, p. 101823.

[4] E. Uhlemann, "Time for Autonomous Vehicles to Connect [Connected Vehicles]," *IEEE Vehic. Tech. Mag.*, vol. 13, no. 3, 2018, pp. 10–13.

[5] A. Arora and S. K. Yadav, "Block Chain Based Security Mechanism for Internet of Vehicles (IoV)," *Proc. 3rd Int'l. Conf. Internet of Things and Connected Technologies (ICIoTCT)*, 2018, pp. 26–27.

[6] B. Schoettle and M. Sivak, "A Survey of Public Opinion about Autonomous and Self-Driving Vehicles in the US, the UK, and Australia," University of Michigan, Ann Arbor, Transportation Research Institute, Tech. Rep., 2014.

[7] X. Krasniqi and E. Hajrizi, "Use of IoT Technology to Drive the Automotive Industry from Connected to Full Autonomous Vehicles," IFACPapersOnLine, vol. 49, no. 29, 2016, pp. 269–74.

[8] Z. Ning *et al.*, "Deep Reinforcement Learning for Vehicular Edge Computing: An Intelligent Offloading System," *ACM Trans. Intelligent Systems and Technology (TIST)*, vol. 10, no. 6, 2019, p. 60.

[9] Q. Qi *et al.*, "Knowledge-Driven Service Offloading Decision for Vehicular Edge Computing: A Deep Reinforcement Learning Approach," *IEEE Trans. Vehic. Tech.*, vol. 68, no. 5, 2019, pp. 4192–203.

[10] L. Liang, H. Ye, and G. Y. Li, "Toward Intelligent Vehicular Networks: A Machine Learning Framework," *IEEE Internet of Things J.*, vol. 6, no. 1, pp. 124–135, 2018.

[11] S. Nakamoto *et al.*, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[12] Z. Yang *et al.*, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," *IEEE Internet of Things J.*, vol. 6, no. 2, 2018, pp. 1495–505.

[13] X. Wang *et al.*, "An improved Authentication Scheme for Internet of Vehicles Based on Blockchain Technology," *IEEE Access*, vol. 7, 2019, pp. 45,061–072.

[14] T. Dbouk *et al.*, "A Novel Adhoc Mobile Edge Cloud Offering Security Services Through Intelligent Resource-Aware Offloading," *IEEE Trans. Network and Service Management*, 2019.

[15] O. A. Wahab *et al.*, "CEAP: SVM-Based Intelligent Detection Model for Clustered Vehicular Ad Hoc Networks," *Expert Systems with Applications*, vol. 50, 2016, pp. 40–54.

Biographies

Ahmad Hammoud received his B.S. in business computing and M.S. in computer science from the Lebanese University in 2016 and the Lebanese American University in 2019, respectively. His current research interests include cloud federation, fog federation, game theory, Blockchain, Artificial Intelligence, and security.

Hani Sami received his M.Sc. degree in computer science from the American University of Beirut and completed his B.S. and worked as a research assistant at the Lebanese American University. The topics of his research are Fog Computing, Vehicular Fog Computing, and Reinforcement Learning. He is a reviewer for several prestigious conferences and journals.

Azzam Mourad is currently an associate professor of computer science with the Lebanese American University and also an affiliate associate professor with the Software Engineering and IT Department, Ecole de Technologie Superieure (ETS), Montreal. He has served/serves as an associate editor for *IEEE Transactions on Network and Service Management*, *IEEE Network*, *IEEE Open Journal of the Communications Society*, *IET Quantum Communication*, and *IEEE Communications Letters*, the General Chair of IWCMC2020, the General Co-Chair of WiMob2016, and the Track Chair, a TPC member, and a reviewer of several prestigious journals and conferences. He is an IEEE senior member.

Hadi Otrok holds an associate professor position in the department of ECE at Khalifa University of Science and Technology, an affiliate associate professor at Concordia Institute for Information Systems Engineering at Concordia University, Montreal, Canada, and an affiliate associate professor in the electrical engineering department at Ecole de Technologie Superieure (ETS), Montreal, Canada. He received his Ph.D. in ECE from Concordia University. He is a senior member of IEEE, and an associate editor for *Ad-Hoc Networks* (Elsevier) and *IEEE Network*. He served on the editorial board of *IEEE Communication Letters*. He co-chaired several committees at various IEEE conferences. His research interests include the domain of computer and network security, crowd sensing and sourcing, ad hoc networks, and Blockchain.

Rabeb Mizouni is an associate professor in electrical and computer engineering at Khalifa University. She received her Ph.D. and her M.Sc. in electrical and computer engineering from Concordia University, Montreal, Canada in 2007 and 2002, respectively. Currently, she is interested in edge computing, crowd sensing, blockchain and cloud computing.

Jamal Bentahar received the bachelor's degree in software engineering from the National Institute of Statistics and Applied Economics, Morocco, in 1998, the M.Sc. degree in the same discipline from Mohamed V University, Morocco, in 2001, and the Ph.D. degree in computer science and software engineering from Laval University, Canada, in 2005. He is a professor with Concordia Institute for Information Systems Engineering, Faculty of Engineering and Computer Science, Concordia University, Canada. From 2005 to 2006, he was a postdoctoral fellow with Laval University, and then an NSERC postdoctoral fellow at Simon Fraser University, Canada. He was an NSERC Co-Chair for Discovery Grant for Computer Science (2016-2018). His research interests include cloud and services computing, trust and reputation, game theory, computational logics, model checking, multi-agent systems, and AI.

Footnotes

[1] https://scholar.google.com/

[2] https://www.coindesk.com/gm-bmw-back-blockchain-data-sharing-for-self-driving-cars

[3] https://businessblockchainhq.com/business-blockchain-news/volkswagen-blockchain-efforts-to-prevent-odometer-fraud/