Smart and Secure CAV Networks Empowered by AI-Enabled Blockchain: Next Frontier for Intelligent Safe-Driving Assessment

Le Xia, Yao Sun, Rafiq Swash, Lina Mohjazi, Lei Zhang, and Muhammad Ali Imran

***Abstract*—Securing safe-driving for connected and autonomous vehicles (CAVs) continues to be a widespread concern despite various sophisticated functions delivered by artificial intelligence for in-vehicle devices. Besides, diverse malicious network attacks become ubiquitous along with the worldwide implementation of the Internet of Vehicles, which exposes a range of reliability and privacy threats for managing data in CAV networks. Combined with the fact that the capability of existing CAVs in handling intensive computation tasks is limited, this implies a need for designing an efficient assessment system to guarantee autonomous driving safety without compromising data security. Motivated by this, in this article, we propose a novel framework, namely Blockchain-enabled intElligent Safe-driving assessmenT (BEST), that offers a smart and reliable approach for conducting safe driving supervision while protecting vehicular information. Specifically, a promising solution that exploits a long short-term memory model is introduced to assess the safety level of the moving CAVs. Then, we investigate how a distributed blockchain obtains adequate trustworthiness and robustness for CAV data by adopting a byzantine fault tolerance-based delegated proof-of-stake consensus mechanism. Simulation results demonstrate that our presented BEST gains better data credibility with a higher prediction accuracy for vehicular safety assessment when compared with existing schemes. Finally, we discuss several open challenges that need to be addressed in future CAV networks.**

I. Introduction

With the proliferation of information demands among connected vehicles, maintaining wireless connectivity between vehicular networks and roadside infrastructures is becoming increasingly indispensable. In this setup, the connection is primarily carried out through specialized communication technologies, e.g., road site units (RSUs)-based dedicated short-range communications (DSRC) or base stations-enabled cellular networks [1]. Both safe road-surveillance and reliable vehicle-control can be further ensured by allowing smart vehicle-to-everything communications. Additionally, the advancement of artificial intelligence (AI) has garnered a great deal of significance in vehicular networks, i.e., connected and autonomous vehicles (CAVs), to liberate humans physically and mentally from daily driving tasks. Thanks to intelligent navigation, automated scheduling, and orderly driving, the promotion of CAV applications not only mitigates traffic congestion and resource consumption, but also enforces travel effectiveness and even reduces the casualty rates of traffic accidents [2], [3]. Nevertheless, the current CAV network still faces several challenges, which can be briefly attributed to the following two aspects:

- *Driving safety*: Since the ultimate goal of autonomous driving is to reach the fifth level, i.e., full automation as defined by the Society of Automotive Engineers [4], the autonomy of the vehicle itself should be the most critical factor for safety. However, a malfunction resulting from unexpected erroneous bugs or security breaches may cause catastrophic consequences, like severe safety incidents or even casualties, such as the Uber accident occurred in 2018 [5].
- *Data security*: The security and authenticity of vehicular data are also crucial for driving safety. Unfortunately, current identification, authentication and management for vehicular information are all handled by third parties. As a result of this centralized management architecture, the fears of data tampering and privacy leakage is growing notably and leading to a core problem in trust. Furthermore, diverse malicious attacks on CAV networks also become pervasive nowadays (e.g., camera blinding and GPS jamming [6]) with its unceasing application scale.

In response to the aforementioned issues, the fusion of deep learning (DL) and blockchain techniques seems to be a promising solution here. First, DL should be a necessity to solve complicated prediction problems with its powerful neural networks [7]. This can be applied as an attractive method to accurately supervise the driving status of CAVs and then exploit the obtained feedback to implement proper countermeasures to the misbehaving vehicles, thereby, efficiently preventing accidents. Meanwhile, blockchain, as an authority-decentralized technique, leverages a distributed digital ledger that records authorized transactions in blocks without the need for a central trusted medium, which guarantees ample trustworthiness and credibility for vehicular data management [8].

Nevertheless, a perfect rationale of how to integrate DL with blockchain is very critical for the CAV network design. Considering the complex vehicular environments, the intrinsic feature that combines the two is the status information of mobile CAVs. Therefore, we specially consider to take the status data as the core hub between DL and blockchain models. On the one hand, these data are obviously indispensable for DL to accurately assess the vehicular safety level. On the other hand, blockchain can authenticate these data to prevent fake or dishonest content from mixing into the network to cause chaos, as well as to provide stable data source for DL prediction with sufficient reliability. To the best of our

Le Xia, Yao Sun (corresponding author), Lina Mohjazi, Lei Zhang, and Muhammad Ali Imran are with University of Glasgow;
Rafiq Swash is with AIDrivers Ltd. and Brunel University London.

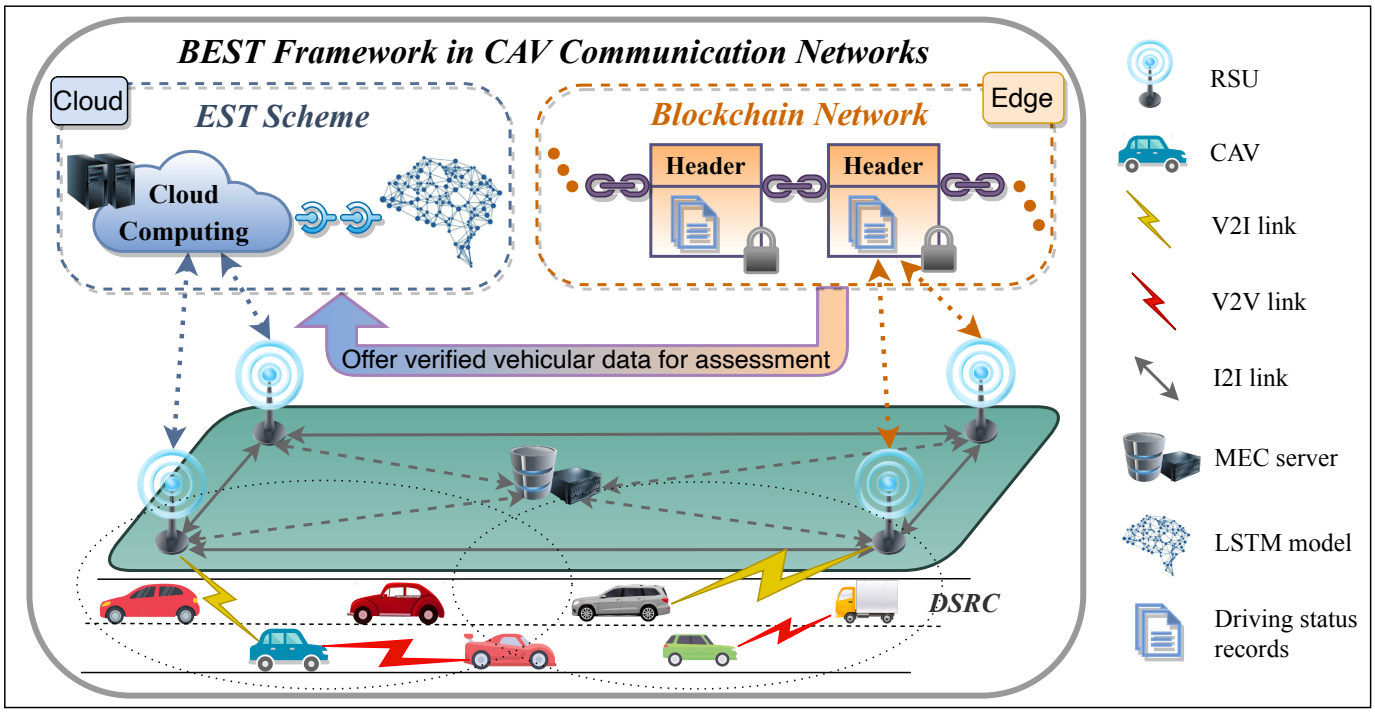

Fig. 1. An overview of the integrated BEST framework for CAV networks.

knowledge, no article has conducted the same research before. In this context, an efficient network architecture integrated with DL and blockchain becomes meaningful for provisioning driving safety and data security, simultaneously.

In this article, we propose a novel framework of Blockchain-enabled intElligent Safe-driving assessmenT (BEST) for CAV networks, as elucidated in Fig. 1. Specifically, BEST comprises two components, i.e., an intElligent Safe-driving assessmenT (EST) scheme and a blockchain network underpinning a data management platform. For the EST scheme, a long short-term memory (LSTM) model is first adopted to cope with time series-related prediction problems and align with high vehicular dynamics. By analyzing the driving status in different time-slots, each CAV can receive a current safety level from the LSTM, as well as potential countermeasures, which can be processed and executed in the cloud. In addition, we further introduce a consortium blockchain to guarantee information security and privacy, which is supported by a mobile edge computing (MEC) technique to alleviate the computational pressure. With the implementation of byzantine fault tolerance-based delegated proof-of-stake (BFT-DPoS) consensus mechanism, we store real-time driving status data in multiple blocks at a fast block generation speed, which not only makes vehicular information immutable and unforgeable, but also serves the EST scheme with data authentication and traceability. Moreover, simulations are conducted to compare the performance of BEST with existing schemes. The results show that our BEST can effectively avoid the false information sharing from malicious CAVs, and simultaneously assess the safety level for each CAV with a high accuracy. Finally, we outline several challenges and prospects of BEST from the perspectives of incentive, efficiency and resource utilization in CAV networks.

For the remainder of this article, we first give an overview of the conventional CAV network along with several current obstacles to emphasize the significance of our BEST framework. Then, we specifically demonstrate how the LSTM performs safety level assessment to cooperate with the blockchain system. Afterward, the BEST is verified and discussed by simulation results. Finally, we open the doors for future directions and close this article with conclusions.

II. Overview of CAV Networks and BEST Framework

A. Connected and Autonomous Vehicular Networks

First, we briefly introduce some core elements to provide a deeper insight of CAV networks, which are listed as follows:

- *CAVs:* The merits of AI are leveraged in numerous applications supported by CAVs. By analyzing information gathered from multiple in-vehicle devices, vehicles can map out the optimal driving trajectory followed by intelligent decision execution, including tire orientation control and the change of lane or velocity.
- *RSUs:* The RSU refers to a core roadside infrastructure that performs data access functions for CAVs within its signal coverage, and also offers bi-directional communication for vehicles and other associated servers.
- *Communication networks:* Sophisticated inter-vehicle communications provide multiple feasible options in automotive networking community. For instance, a CAV uses its on-board units to wirelessly connect with other CAVs via vehicle-to-vehicle links, or to access an adjacent RSU using DSRC characterized by short-distance and low-latency communications.

Despite its promising prospects, there still exists several critical challenges in the corner. Generally, autonomous driving mainly relies on sensors and networks control, making CAVs susceptible to unknown malfunctions at any time [9]. Besides, although RSUs build a feasible bridge between CAVs and the Internet, they expose the CAV network to possible malicious attacks. Here, we list some existing challenges in the CAV network below for summary.

Limitations in vehicular capability: Due to the increasing burden of data generation and limited processing capability, it becomes challenging for a single CAV to simultaneously perform tremendous computation and communication tasks. Additionally, the inaccuracy and inefficiency of in-vehicle devices detection may lead to erroneous decision-making, and thereby endanger the safety of passengers or passersby in close proximity [10].

Threats on data security and privacy: In addition to the loopholes of CAV itself, it is more likely to suffer attacks from external networks, compared with manually driven vehicles. Note that the malicious attacks here can be considered as harmful network viruses or massive fraudulent data spread by individuals or organizations, thus to interfere with the normal operation of the network and achieve their illegal purposes, such as stealing private information or even forcibly seizing control of targeted vehicles. Apart from this, attacks from malicious participants are ubiquitous as well, pretending to be normal vehicles or servers to sneak into the network and gaining benefits. These diverse attacks render conventional data protection methods (e.g., cryptography) to be inefficient and inappropriate when applied to CAV networks.

Centralization of network management: Generally, CAV networks are maintained via third entities with opening access, which may incur inevitable trust and security fears for clients as a result of centralization that makes networks more vulnerable to single point of attacks from outside. Hypothetically, once the central sever is centrally damaged through the external attacks (e.g., distributed denial of service attack [11]), it may result in severe consequences like transportation system paralysis or immense economic losses. Furthermore, as CAV networks continue to scale up, the centralized approach will become increasingly overwhelmed by handling and storing such massive data.

B. BEST Framework

In order to tackle the challenging issues above, here we propose a potential solution, namely the BEST framework for CAV networks. Notably, both components in BEST (EST scheme and blockchain network) are maintained and connected via RSUs. For the EST, a LSTM model is leveraged to assess the driving safety level of mobile CAVs, whereas each RSU is responsible for periodically collecting the driving status data of its covered vehicles. Meanwhile, RSUs can also promptly apply countermeasures to the vehicles with misbehaviors, by either warning or performing artificial suspension. Further, we integrate a scalable blockchain with the EST, in which transactions are securely encrypted, and the power that originally held in a third entity can be evenly decentralized to all RSUs. Here, "Transactions" can be interpreted as any information interaction in crypto between peers, mainly composed of the status records shared from mobile CAVs to RSUs in our roadmap, as depicted in Fig. 2. The Hash encryption algorithm can guarantee the blockchain to defend against most of malicious attacks, making the attackers almost impossible to forge or alter ledger without being detected. Note that each RSU participates in blockchain as a role of a blockchain node. Specially, all RSUs are functionally divided into two groups, i.e., consensus RSU nodes (CRNs) and ordinary RSU nodes (ORNs), which are to match the adopted BFT-DPoS consensus mechanism.

The main focus of this article is to integrate them into one network to effectively address driving safety and data security issues at the same time. Precisely, we believe that blockchain and AI can well complement each other in the BEST. First, since the recorded status data are well-reserved and easily-traceable in chained blocks, this makes the blockchain a primary and reliable dataset for the LSTM. Besides, the predicted results of LSTM on the vehicular safety level can also be stored in the blockchain, offering key information for the next round of prediction. It is this very compatible internal collaboration between blockchain and DL that makes the entire CAV network more reliable and resilient.

Herein, we take the workflow of a CAV registered in the BEST as an exemplification to facilitate understanding. The vehicle is first required to accurately capture various status information through its multiple sophisticated sensors while driving. Next, these data will be uploaded to the adjacent RSU, and the blockchain can thus verify them with the help of an effective consensus mechanism. Afterwards, not only the current authenticated data, but also the data stored in blocks at the past time, will be input together into a well-designed and mature-trained LSTM model for assessing the specific level of driving safety and making countermeasures. Furthermore, most computing tasks in blockchain process can be offloaded by deploying MEC on the clusters of RSUs for promoting system efficiency. Considering cost issues and relatively low-latency requirement of EST, the LSTM operation can be placed on remote cloud servers to firm ample computing resources while relieving the MEC servers and RSUs from extra computation load.

III. Operations of BEST in CAV Networks

In this section, we first illustrate the proposed EST scheme with an LSTM model to offer a smart and safe self-driving scenario. Then, the details of a blockchain system with its BFT-DPoS consensus mechanism applicable for CAV networks are presented, where its potential to assure data security and resilience for data management is highlighted.

A. LSTM-Enabled EST Scheme

As expounded before, due to the special operating mechanism and capacity constraints of CAVs, potential safety hazards cannot be completely eliminated. There is still a need to deploy effective and reliable supervision approaches to ensure safe self-driving. Meanwhile, as a result of the highly dynamic

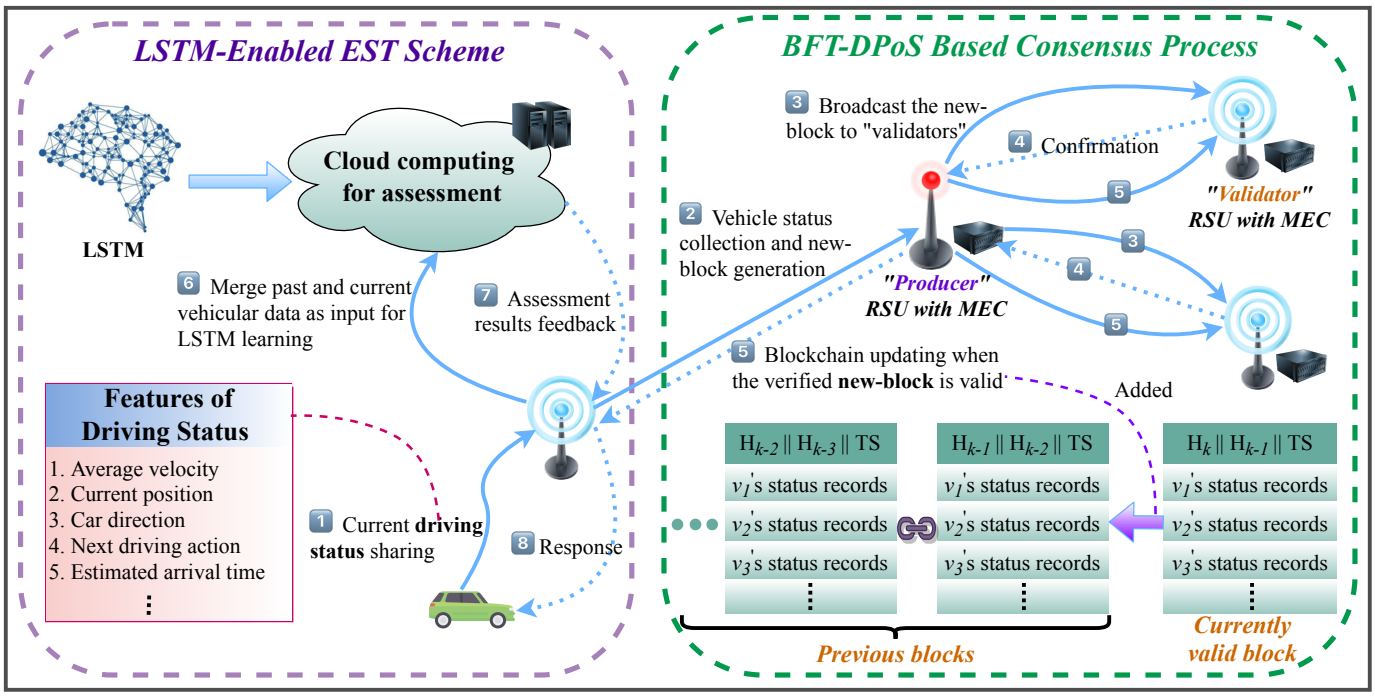

Fig. 2. Details of different phases of the proposed BEST framework in CAV networks.

nature of networks, CAVs' driving status in multiple time slots are necessary to be combined and taken into account. This yields time-related optimization and prediction problems. Accordingly, an incorporated assessment network with LSTM is proposed, as sketched in Fig. 3.

Generally, LSTM, as an evolved gated recurrent neural network, successfully overcomes the difficulties of long sequence time-series dependence and gradient disappearance, where the technical details can be found in [12]. Hence, we exploit the LSTM to process time-series vehicular data and extract useful information to complement our EST scheme. Meanwhile, multiple kinds of information exist in a moving CAV. Explicit features comprise but are not limited to its performed actions (e.g., velocity/accelerate/brake/turn), the safety level predicted at previous moment, and surrounding road conditions [13]. Among them, RSUs are to gather the information recorded at current and past moments, before commencing the assessment process. Specially, a performance metric, vehicle risk index (VRI), is defined to monitor different safety levels of CAV driving. It is worth mentioning that the definition of VRI is loose coupled with the design of BEST framework. In other words, the definition and the way of calculating can only affect the absolute value of VRI, but do not invalidate the relative performance enhancement of BEST framework. Hence, any other sophisticated and accurate VRI models can be embedded in BEST. In the following, we demonstrate each phase in detail for a better understanding of EST in Fig. 3.

- *(Phase 1) Information sharing and verification*: First, each RSU acts as an information collector within its communication range to receive encrypted driving information (within a given time interval T) of all registered CAVs with their digital signatures Sig_V and public keys K_V^u. Here, the Sig_V and K_V^u are used to verify the vehicle's identity. Then, currently received data will be certified via a consensus protocol of blockchain to get authorization. Elaborations on this will be provided later.
- *(Phase 2) Dataset preparation*: After authentications, RSUs will update their local database of blockchain and simultaneously read the past driving records of each vehicle to supplement datasets for LSTM. Then, RSUs upload prepared datasets to the cloud servers and wait for the assessment feedback.
- *(Phase 3) AI assessment process*: Exploiting cloud computing, time-series data-based regression problem can be rapidly solved by the mature-trained LSTM model. Owing to our settings, the outcome of LSTM is $(VRI \| K_V^u \| Sig_V)$, where the VRI ($VRI \in (0, 1]$) indicates the hazardous degree of current driving. Afterward, this result will be fed back to the corresponding RSU of each CAV.
- *(Phase 4) VRI analysis*: VRI represents the current safe driving circumstance of a moving CAV, where the lower the value, the safer the vehicle. Moreover, there should be different VRI thresholds considering the complex and dynamic road conditions in reality. Here, we take two standards as examples, i.e., a safe threshold of α and a dangerous threshold of β, respectively, where $0 < \alpha < \beta < 1$.
- *(Phase 5) Countermeasure response*: According to the feedback, appropriate countermeasures are taken in time for the misbehaving CAVs with higher VRI values. For instance, an urgent warning should be given when VRI is at a medium level, i.e., $VRI \in (\alpha, \beta]$. Similarly, when $VRI \in (\beta, 1]$, stricter measures (e.g., human intervention or forced suspension) should be executed immediately to prevent further serious consequences.

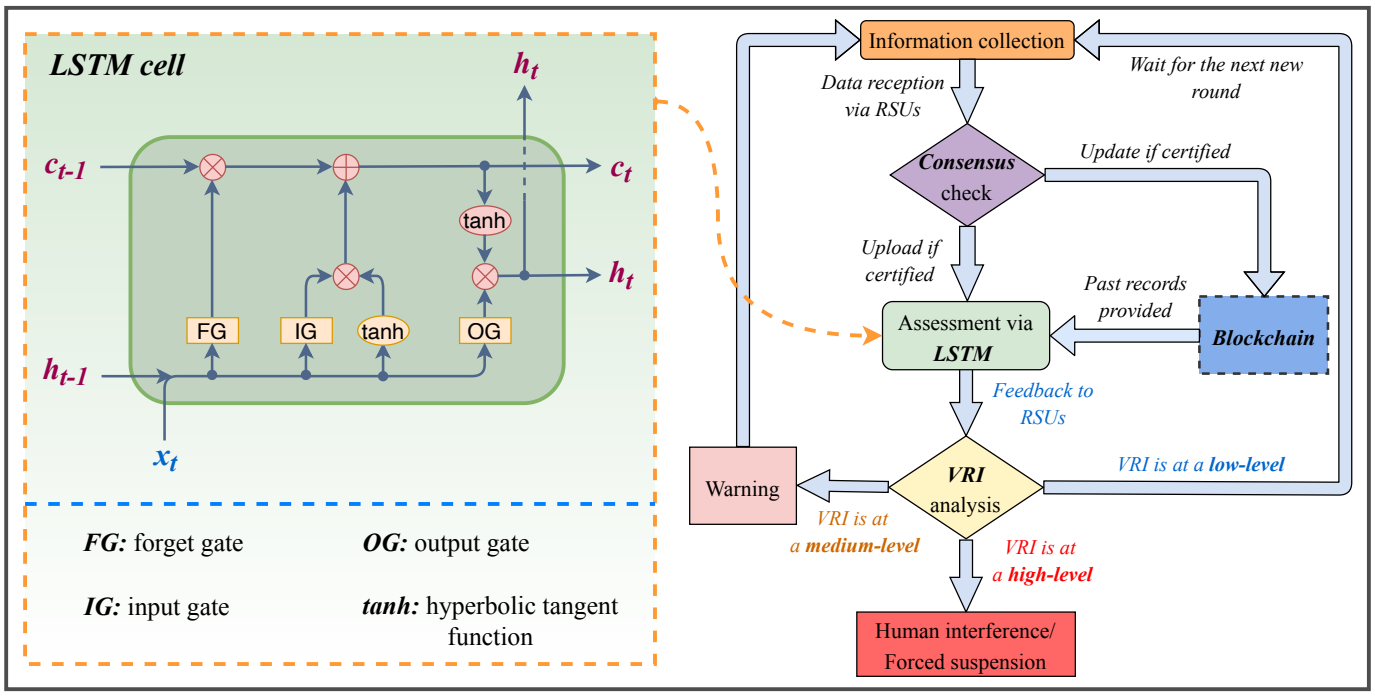

Fig. 3. The proposed EST scheme processing with LSTM network in the cloud.

B. BFT-DPoS Based Blockchain System

Since the vehicular communication mainly relies on the cluster of approved RSUs that allow external clients to conduct data interaction in an authorized manner, a consortium blockchain is really suitable in this framework. Generally, the most commonly used consensus mechanism in blockchain applications is Proof-of-Work (PoW) or Proof-of-Stake (PoS), however, neither of these two is the optimal alternative for autonomous driving. PoW demands countless computation resources with considerable power consumption to complete mining tasks, which would create a burden on RSUs even with the help of MEC. Besides, PoS requires Hash calculation-based mining operation with global validation, resulting in weak supervision and low efficiency.

For a better collaboration with EST, a BFT-DPoS consensus protocol is applied in our blockchain, as elucidated in Fig. 4, which ensures excellent transaction throughput necessary to support real-time operations in the CAV network. As an exemplification, cryptocurrency EOS leverages BFT-DPoS to reach an irreversible consensus within only $1s$ [14]. Specifically, DPoS is a democratic form of PoS based on the consensus nodes (i.e., CRNs group) voted via public delegation (i.e., all RSUs). Once finalizing a round of delegation procedure, CRNs are able to exercise their authorities of ledger management. Moreover, by incorporating an extra layer of BFT, DPoS mechanism can further guarantee an ultra-robust and highly-valid blockchain with low consensus delay [15]. To elaborate further, we give the workflow of BFT-DPoS process as follows:

- *Preparations*: Initially, the network elects several most trusted RSUs as CRNs based on the token deposits proportion voted in a stake pool, where more details can be discovered in [15]. The rest ones become the ordinary nodes (i.e., ORNs) who are only responsible for data interaction and blockchain storage. Next, a new round of consensus process is capable for commencement.
- *(Step 1) Block producer election*: According to the stake information fetched from all CRNs, a pseudo-random sequence of block generation opportunities is first generated. Correspondingly, each CRN is elected as a *producer* to propose new blocks in a round-robin fashion, while the others act as *validators* for auditing the new block at the same time.
- *(Step 2) New block generation*: The producer collects all records of vehicular driving status that occurred within T, then uses its private key to encrypt and pack them into a new block. Meanwhile, producer's signature Sig_{pro} with its public key is also attached to insure that validators can confirm the block source.
- *(Step 3) New block validation*: The BFT-DPoS enables the producer to broadcast new block to all validators at once, which replaces the traditional approach of sequential validation in DPoS and significantly promotes the validation efficiency. After that, each validator compares the received duplicated block with local replicas to verify the authenticity and feed the result with its signature Sig_{va} back to producer.
- *(Step 4) Result confirmation*: Based on the BFT rule, when exceeding $2/3$ different signed blocks are received by the producer [15], this new block is deemed valid and irreversible. Otherwise, the system will forcibly suspend the current procedure and return to the *Step* 1 to prepare for the next new round of consensus.
- *(Step 5) Blockchain extension*: After confirming that the new block is valid, the producer conducts the second broadcast to RSUs (both CRNs and ORNs) to complete the blockchain

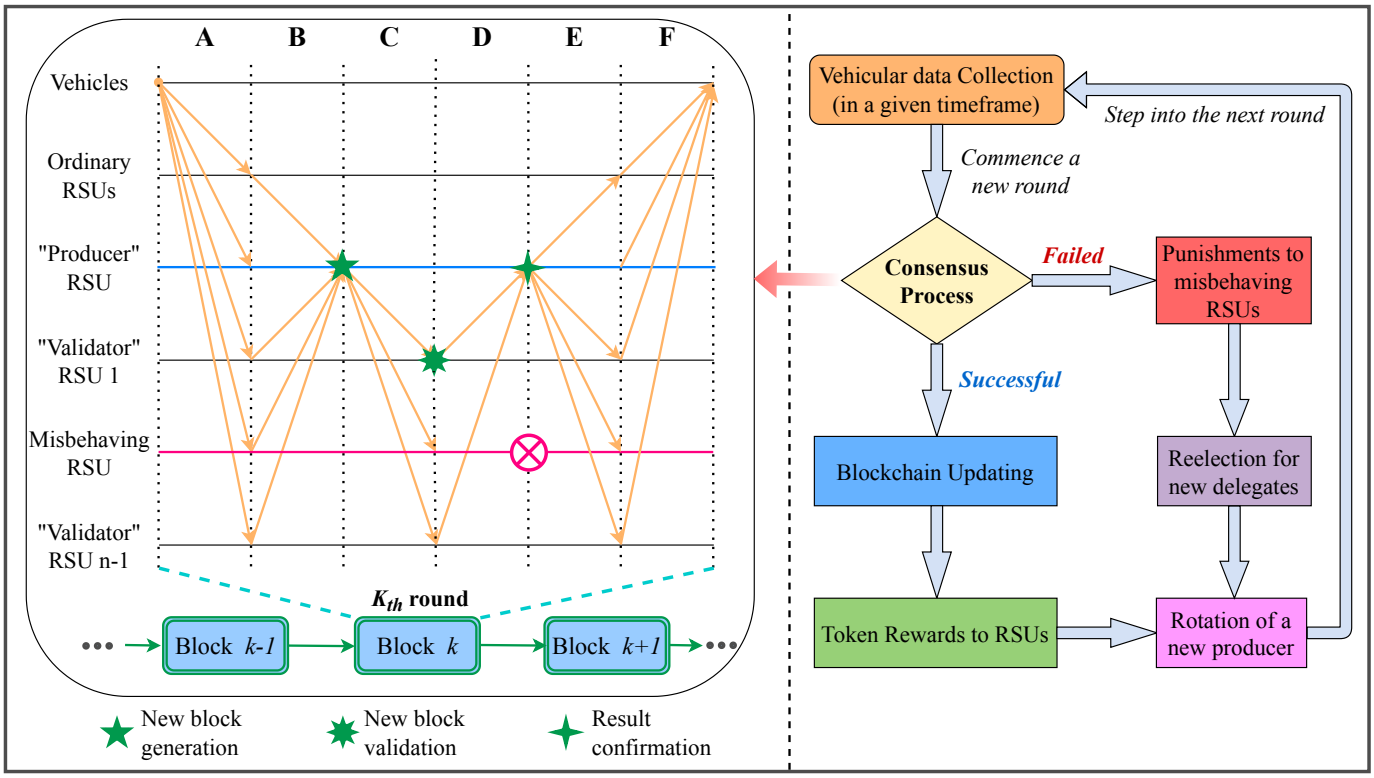

Fig. 4. The K_{th} round of BFT-DPoS based consensus process in a consortium blockchain. A: Information sharing; B: Records collection; C: New block broadcast; D: Authentication feedback; E: Blockchain update; F: Data response.

update. In the meantime, a new round of consensus process will commence from the next producer in the established sequence. Consequently, the driving records gathered by RSUs can be uploaded to the EST with authorization.

- *Rewards and punishments*: To enforce integrity and credibility in blockchain, a reward and punishment-based incentive mechanism is devised to encourage trustworthy delegation and consensus participation. After each round, CRNs receive a token-reward proportional to the deposits they voted. This rule is also applied to the ORNs to gain some dividends. However, the CRNs with misbehaviors will be confronted with the risks of voting out and token deduction. If one RSU is removed from the committee, a new replacement will be reelected from the ORNs to fill the vacancy.

In summary, the proposed BEST can offer sufficient security protection for vehicular data and driving. Nevertheless, since the delay and communication overhead cannot be neglected in such a time-critical driving scenario, we briefly analyze their impact in the BEST here for clearer understanding. First, the communication delay in BEST is the same when compared to conventional CAV networks, because no further burden here is imposed on the communication interplay phase. For the computing delay, note that no extra delay is caused by the EST scheme, thanks to the pre-training mechanism that can make a well-trained LSTM be directly used for prediction. Meanwhile, we also deploy powerful MEC serves, as aforementioned, to offload most blockchain tasks from the RSUs and greatly reduce the computing delay. Besides, the BFT-DPoS consensus we choose is a very efficient mechanism ($0.5s$ per block [14]), where the delay can be considered tolerable in the BEST scenario at such a fast block generation speed. As for the communication overhead, it can be observed in Fig. 4 that only a small amount of signaling interaction is demanded for blockchain to finalize a round of consensus confirmation, while only several bits are required for each signaling transmission. In this context, either the delay or the communication overhead issue can be well tackled in a BEST-enabled CAV network.

IV. Simulation Results and Analysis

In this section, simulations are presented to demonstrate the performance of the proposed BEST (i.e., blockchain with LSTM) when compared with three other combination schemes of *LSTM, deep neural network (DNN), blockchain, and centralization approaches*, in environments involving multiple malicious CAVs. Herein, the centralization approach indicates that all data from CAVs are managed solely by a central entity, which is only accountable for storing the uploaded information, and adopting the conventional data encryption method like cryptography but without any participation of blockchain. Besides, we choose the most commonly used DNN model as the benchmark of LSTM, where the aforementioned VRI metric is set as the target monitoring parameter.

In our simulations, the BEST framework is implemented in a computer with six CPU cores and Inter Core i7 processor, while the main software environment is Tensorflow 2.1.0 and Python 3.7. We first simulate a general CAV network scenario, in which the numbers of RSUs and CAVs are set to 20 and 300, respectively. Specifically, RSUs are set in a given area

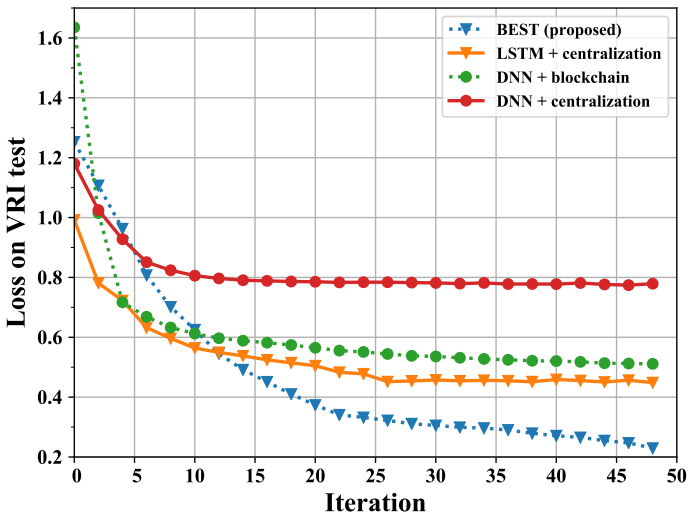

Fig. 5. VRI prediction loss *vs.* training iteration with different approaches.

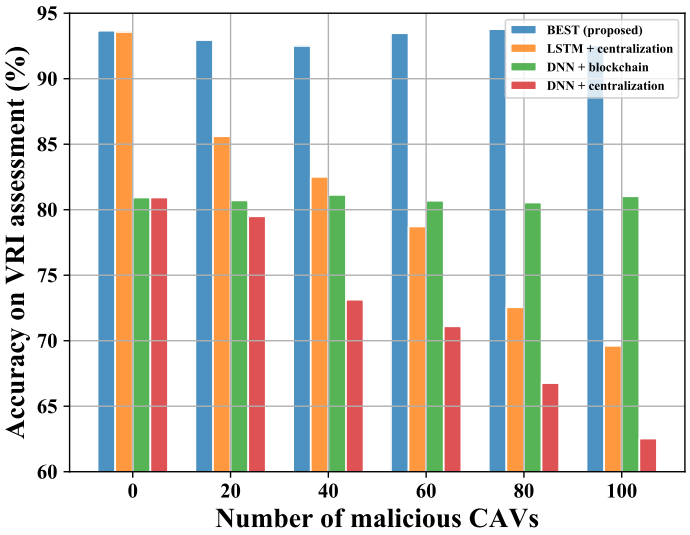

Fig. 6. Accuracy comparison of VRI assessment under different number of malicious CAVs.

and have fixed positions, while the CAVs randomly locate and each CAV is associated with their nearest RSU for simplicity. For each CAV, the initial velocity is randomly distributed between $0 \sim 50km/h$ with a steady acceleration between $-10 \sim 10m/s^2$. Note that these parameters are only as the input status data without affecting any performance of the BEST. Some other status information, including the amount of neighboring vehicles, minimum distance to other vehicles, and position, etc., is also shared with its adjacent RSU per second. Herein, we assume that all CAVs have fixed driving directions, and all driving status data within $10s$ of the CAVs are then collected for subsequent analysis. For VRI calculation, we initially set a total of four risk levels (low, medium, high, and accident level) for CAVs in the simulation, thereby becoming a classification optimization problem (i.e., cross-entropy is adopted as the loss function). For blockchain system, the RSU-enabled consensus rule is considered and deployed in this network, where the block size is 8 MB and the maximum block interval is set as $1s$. Meanwhile, a two-layer LSTM is constructed to predict VRI with a comparison object of a four-layer DNN. Dropout technique is also exploited to avoid the overfitting problem and an Adam optimizer is utilized for gradient updates.

As depicted in Fig. 5, we first show the loss convergence results for VRI predictions under the four different schemes. Obviously, the proposed integrated framework of LSTM with blockchain achieves the optimal VRI prediction loss of around 0.2 in 50 training iterations, which far outperforms the case using DNN instead. Notably, we add 50 malicious CAVs in this figure to continuously forge fake, meaningless, and dishonest content, and upload them to RSUs for causing chaos to the training dataset. This setting aims to better test and compare their respective tolerance to malicious content attacks. By observing the curve trends of centralized approaches, it seems that traditional cryptography cannot effectively preclude the negative impacts from fake content attacks, causing a high prediction loss. Nevertheless, the schemes using the blockchain technique can significantly identify and eliminate false content in the contaminated dataset and attain very low loss with fast convergence speed.

Next, we further compare the accuracy of VRI assessment with different numbers of malicious CAVs participating in the network as shown in Fig. 6, thus to investigate the robustness of the four schemes. It can be clearly seen that the proposed BEST always maintains high prediction accuracy of $92.5 \sim 93.8\%$, while the accuracies of other approaches are far below it (all lower than 85.6%). For instance, the VRI assessment performance of centralized approaches drops drastically as the number of malicious CAVs increases from 0 to 100. Due to its inability to authenticate fake data, the performance apparently becomes poor when many malicious CAVs exist. In contrast, the blockchain method can successfully detect and eliminate these fake data via its powerful consensus rule and unforgeable unified ledger, greatly improving the purity of dataset and ensuring a relatively stable precision level for AI prediction. This conclusion is also highly consistent with the results obtained in Fig. 5. In summary, instantiations that rely on our BEST framework can smoothly realize safe-driving assessment at a very high accuracy, while gaining adequate data credibility and security in autonomous driving networks.

V. Open Challenges and Discussions

In spite of many superiorities, the proposed BEST framework still imposes some associated and nontrivial challenges that should be discussed before unlocking its full potentials.

Inactive information sharing: Since the actual effect of the proposed framework primarily depends on the information shared by CAVs in the communication community, vehicles may lack the enthusiasm to upload their data to RSUs without ample compensation. Therefore, a rewards-based incentive mechanism for CAVs can be embedded into the BEST to encourage vehicles to spontaneously share information and attract more other vehicles to participate in this framework.

Highly dynamic road conditions: The road conditions of different RSUs vary according to their locations in the city,

and traffic congestion under the same RSU in different time periods is also distinct. This fact leads to an imbalance of task allocation in BEST, where an excessive volume of vehicular contents may be sent to a single RSU while some other RSUs only receive a few. To this end, proposing a real-time task scheduling scheme for RSUs can promote the effectiveness of information gathering for BEST under high road condition dynamics.

Resources allocation in CAVs: It is inevitable to consume a certain amount of wireless communication resources for data collection, signal transmission, and information sharing in BEST. However, due to the limited resources, CAV networks have to well allocate them across multiple devices with different communications tasks to reach an optimal resource utilization. In this case, reinforcement learning algorithm might be a promising solution to automatically and smartly achieves resource allocation for each operation in moving CAVs.

VI. Conclusion

In this article, we proposed a novel BEST framework that incorporates AI and consortium blockchain, offering driving safety and data security simultaneously in CAV networks. An LSTM model was applied in the EST scheme for evaluating the VRI, followed by a blockchain system for a supplement of data credibility through its powerful consensus mechanism. Simulation results further demonstrated that our BEST could maintain significantly high accuracy of driving risk assessment when compared to existing schemes, even if there is a high amount of false content interference from malicious CAVs. Finally, several open challenges and potential solutions were discussed. We hope that this work becomes a pioneer in building an efficient and reliable supervision system based on AI and blockchain to underpin future autonomous driving applications.

VII. Acknowledgement

This work was supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC under grant number EP/S035362/1. Besides, we would like to thank for support from AI Drivers for the studentship.

References

[1] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and cellular network technologies for V2X communications: A survey," *IEEE transactions on vehicular technology*, vol. 65, no. 12, pp. 9457–9470, 2016.

[2] G. De La Torre, P. Rad, and K.-K. R. Choo, "Driverless vehicle security: Challenges and future research opportunities," *Future Generation Computer Systems*, vol. 108, pp. 1092–1111, 2020.

[3] J. Wang, J. Liu, and N. Kato, "Networking and communications in autonomous driving: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1243–1274, 2018.

[4] SAE On-Road Automated Vehicle Standards Committee, "Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems," *SAE Standard J*, vol. 3016, pp. 1–16, 2014.

[5] A. Efrati, "Uber finds deadly accident likely caused by software set to ignore objects on road," *The information*, 2018.

[6] R. Xing, Z. Su, N. Zhang, Y. Peng, H. Pu, and J. Luo, "Trust-evaluation-based intrusion detection and reinforcement learning in autonomous driving," *IEEE Network*, vol. 33, no. 5, pp. 54–60, 2019.

[7] Q. Ye, W. Shi, K. Qu, H. He, W. Zhuang, and X. Shen, "Joint RAN slicing and computation offloading for autonomous vehicular networks: A learning-assisted hierarchical approach," *IEEE Open Journal of Vehicular Technology*, vol. 2, pp. 272–288, 2021.

[8] J. Posner, L. Tseng, M. Aloqaily, and Y. Jararweh, "Federated learning in vehicular networks: opportunities and solutions," *IEEE Network*, vol. 35, no. 2, pp. 152–159, 2021.

[9] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Networks*, vol. 90, p. 101823, 2019.

[10] Y. Jie, C. Z. Liu, M. Li, K.-K. R. Choo, L. Chen, and C. Guo, "Game theoretic resource allocation model for designing effective traffic safety solution against drunk driving," *Applied Mathematics and Computation*, vol. 376, p. 125142, 2020.

[11] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE communications surveys & tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[12] A. Sherstinsky, "Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network," *Physica D: Nonlinear Phenomena*, vol. 404, p. 132306, 2020.

[13] M. Singh and S. Kim, "Branch based blockchain technology in intelligent vehicle," *Computer Networks*, vol. 145, pp. 219–231, 2018.

[14] IO, EOS, "EOS. IO technical white paper v2," *EOS, Tech. Rep., March*, 2018.

[15] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020.

Le Xia (l.xia.2@research.gla.ac.uk) received his B.Eng. degree and M.Eng. degree in electronics and communication engineering from UESTC in 2017 and 2020, respectively. He is currently pursuing his Ph.D. degree with James Watt School of Engineering, University of Glasgow, UK. His research interests include driverless vehicular networks and intelligent wireless communications.

Yao Sun (Yao.Sun@glasgow.ac.uk) is currently a Lecturer with James Watt School of Engineering, the University of Glasgow, UK. He has won the IEEE Communication Society of TAOS Best Paper Award in 2019 ICC. His research interests include intelligent wireless networking, blockchain system, and resource management in mobile networks.

Rafiq Swash (Rafiq.Swash@brunel.ac.uk) is the founder of AIDrivers Ltd., a lecturer with Brunel University London, and also a visiting professor with Changchun Institute of Optics. He has given scientific talks in number of international scientific and innovation conferences as a keynote speaker in Europe, China, Qatar, India, and UAE.

Lina Mohjazi (Lina.Mohjazi@glasgow.ac.uk) is a Lecturer in the James Watt School of Engineering, University of Glasgow, UK. She received her Ph.D. degree from the University of Surrey, UK, in 2018. Her research interests include beyond 5G wireless technologies, wireless power transfer, machine learning, and reconfigurable intelligent surfaces.

Lei Zhang (Lei.Zhang@glasgow.ac.uk) is a Senior Lecturer at the University of Glasgow, U.K. His research interests include wireless communication systems and networks, blockchain technology, data privacy and security, etc. He is an associate editor of IEEE Internet of Things (IoT) Journal, IEEE Wireless Communications Letters, and Digital Communications and Networks.

Muhammad Ali Imran (Muhammad.Imran@glasgow.ac.uk) is a Professor of communication systems with the University of Glasgow, UK, and a Dean with Glasgow College UESTC. He is also an Affiliate Professor with the University of Oklahoma, USA, and a Visiting Professor at University of Surrey, UK. He has over 20 years of combined academic and industry experience with several leading roles in multi-million pounds funded projects.