A Framework for Decentralised, Real-time Reputation Aggregation in IoV

Haitham Mahmoud, Muhammad Ajmal Azad, Junaid Arshad and Adel Aneiba

***Abstract*—With the rapid increase in the number of connected and autonomous vehicles, there is a growing concern about the potential road accidents and collisions caused by malicious vehicles. A reputation system can help to mitigate these concerns and allow users to have safe journeys by providing a way to identify and estimate the behaviour of individual vehicles and to take appropriate actions in case of any malicious behaviour. Centralised reputation systems are widely used for reputation aggregation, but this setup requires Peer trust and could be a single point of attack. The alternative to a centralised system is the decentralised reputation system for IoV, in which the reputation information is collected and maintained by the vehicles rather than a central authority. There are several key considerations when designing a secure reputation aggregation system for the IoV. These include: i) It should ensure that vehicle feedback about other vehicles is kept private; ii) vehicles' interaction networks and positions should be protected; and iii) computations should be decentralised and not resource-intensive. Adopting a decentralised reputation system within IoV using blockchain can enhance security and privacy and mitigate many security concerns. In this paper, we proposed a blockchain-based reputation system which ensures the privacy of participants and provides secure and resilient reputation computation. The reputation value reflects the aggregate trustworthiness of vehicles and this is computed via feedback provided by the vehicles in a decentralized way. We analysed the security and privacy of the proposed system and provided the computation and communication performance.**

***Index Terms*—IoV, ITS, Blockchain, Preserving-Privacy, reputation.**

I. Introduction

Integrating smart roads into the Internet of Vehicles (IoV) can revolutionize the transportation industry by increasing traffic flow efficiency, enhancing safety, creating new economic opportunities, reducing ecological impact, and ensuring secure data transmission and preservation of vehicle identity. Tesla's Autopilot system is an example of smart roads' ability to detect obstacles, navigate roads automatically, and avoid pedestrians while keeping up with traffic [1].

However, with the increasing interconnections of vehicles and smart roads, the security and privacy of sensitive data transmitted between these entities have become a concern. The threat of malicious actors gaining unauthorised access to sensitive information or manipulating the system for their own gain raises concerns about its security. Therefore, the IoV ecosystem must have robust security measures to prevent such threats and maintain the privacy and security of sensitive information.

The authors work in the Birmingham City University, UK.
Manuscript received January 31, 2023; revised Month day, 2023.

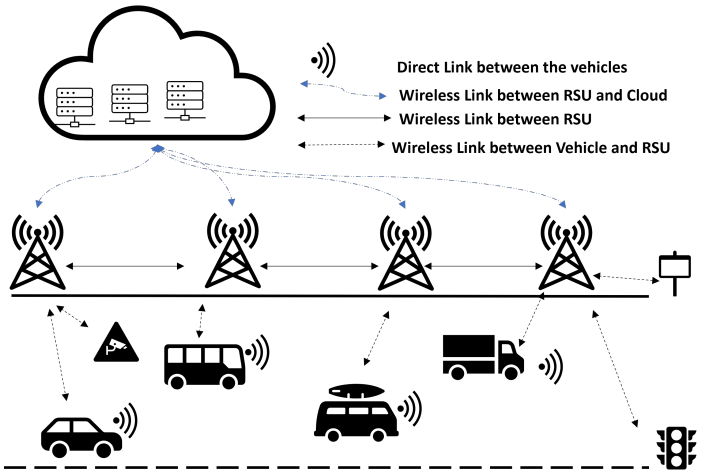

Fig. 1. Generic IoV architecture.

Fig. 1 shows a typical system model of a connected vehicular network which consists of two key components: 1) the vehicles which are equipped with a wireless connection and OBU (onboard Unit) which enable vehicles to communicate with other OBUs, vehicles and infrastructure devices, and 2) roadside units (RSUs) which are infrastructure nodes that are placed alongside the road to provide connectivity to the vehicles. The vehicles can either communicate directly with each other (vehicle-to-vehicle (V2V)) or can communicate via RSU i.e vehicle-to-infrastructure (V2I). V2V and V2I can be conducted using communication technologies such as including short-range communication protocols (dedicated short-range communication protocols) and cellular communication [2]. This infrastructure creates a collaborative environment where vehicles can exchange information with each other such as traffic updates, road status, and traffic jam information to enhance safety and navigation. Implementing V2I is technically similar, but it involves communication with infrastructure elements, such as signs that show reduced speed zones, that can transmit essential data to approaching vehicles and other sensing devices [3].

Within this collaborative connected environment, the reputation of vehicles becomes more pivotal because it can affect the reliability and trustworthiness of the information exchanged between the vehicles within the network. For example, malicious vehicles may be less reliable in providing accurate and trustworthy information to the network. This could have an adverse impact on the overall behaviour of vehicles within the IoV network and could bring the life of passengers and other

users to danger. The trustworthiness of the message sender or vehicle must therefore be evaluated prior to making any decision.

Determining the reliability of a vehicular network, which is ad hoc and decentralised, is challenging. There are two ways to evaluate the trustworthiness of vehicles: 1) through a trusted third party that manages the data reported by vehicles and 2) through a decentralised system where vehicles can directly exchange information. A centralised system can become a single point of failure, be more susceptible to attacks, and threaten vehicle privacy as it stores sensitive information. Participants must also trust the third-party system for their information. Furthermore, centralized systems are not feasible for the physically dispersed and decentralized IoV due to the communication overheads. In a distributed system, there is no central authority to determine the trustworthiness of nodes, but it presents challenges concerning privacy protection and scalability. The trustworthiness of vehicles can be evaluated based on their history of sending accurate or trustworthy information. A weighted reputation system should be adopted, where the trustworthiness of vehicles is computed by considering the feedback submitted by vehicles for others and their trusted behaviour. However, this approach has three challenges: maintaining the privacy of vehicle feedback, protecting vehicles' interaction networks and positions, and ensuring that the computation is decentralised and not too resource-intensive.

Vehicle trustworthiness can be assessed using two methods: 1) a centralised approach relying on a trusted third party, and 2) a decentralised approach relying on direct data exchange between vehicles. The decentralised approach is more privacy-protective but faces scalability and privacy protection challenges. The trustworthiness of vehicles can be determined by their history of sending accurate information, with higher trust given to vehicles known to send trustworthy information. The trust weights from trusted vehicles should be considered in computing the aggregated reputation. However, implementing a weighted reputation system has challenges, such as protecting vehicle feedback privacy, protecting vehicles' interaction networks and positions, and ensuring computations are decentralised and not resource-intensive. Therefore, a reputation system that maintains vehicle security and privacy is essential. Moreover, it should aggregate the trust score in real-time and within the limitations of the device's resources.

In this paper, we propose a weighted reputation computation model to aggregate the trustworthy ratings submitted by vehicles while ensuring the privacy of feedback values. In our approach, we also considered the trustworthiness of feedback providers while aggregating their individual ratings. The proposed system is based on homomorphic encryption and ensures the integrity and confidentiality of participants' data. The approach is different from the others in the way that it considers both honest but curious and malicious threat models. To achieve complete decentralization, we also used blockchain for recording individual feedback and managing the aggregated reputation score. This paper makes the following major contributions.

1) A blockchain-based decentralised reputation system has been proposed for the IoV network that utilises weighted reputation aggregation. To this extent, we utilise the feedback from the vehicle while ensuring the privacy of feedback providers. The proposed framework addresses several challenges, including ensuring feedback authenticity, providing a secure storage mechanism, maintaining transparent reputation scores, and enabling verifiability. Reputation aggregation is carried out at RSUs which employ the weighted aggregation method to evaluate the reputation of vehicles.
2) The proposed system is evaluated for the honest but curious and malicious threat models. We also identified the limitations of reputation systems. The system has been evaluated from several aspects, including security analysis, privacy and integrity analysis, and performance evaluation.

This article is organised as follows: Section II presents the key definition, threat model and the existing study. Section III proposes the architecture by discussing reputation modelling and the key components in the system. Section IV discusses the results and the future research directions. Section V concludes the work.

II. Background

This section provides clear and concise explanations of key terms and concepts relevant to designing a decentralized reputation system for IoV.

A. Definitions

Several important concepts are defined in this section.

Definition 1 - Trust: Trust is determined through direct experience or confidence in others. This enables us to evaluate the vehicle's behaviour. The t_{ij} represents the level of trust between two vehicles, v_i and v_j, in a vehicular network. The value t_{ij} is the binary value [0,1] indicating whether vehicle v_i trusts vehicle v_j or not.

Definition 2 - Reputation: Reputation is determined by aggregating the feedback or trust scores provided by the participants or vehicles. Suppose, for example, k vehicles reported their trust score on vehicle j, i.e., t_{ij} = t_{1j}, t_{2j}, t_{3j}, t_{Nj}, which can be used to calculate the vehicle's reputation j by averaging the direct scores given by the other peers: $R_j = (t_{ij}/k)$.

Definition 3 - Privacy in Vehicular Network: A vehicle network collaborates with fixed infrastructure and other vehicles to compute road conditions. Infrastructure units are also interested in knowing the number of vehicles within a specific geographic area without knowing their identities to improve services. V2V or V2I exchange of information can have some benefits for driver safety, but it can also provide access to private information about vehicles for anyone. It may be possible to uncover the location of the vehicles by comparing the trust scores of the connected vehicles with the trust scores of the other connected vehicles.

Definition 4 - Privacy-Preserving Reputation System:

A reputation system is intended to collect and analyse a vehicle's feedback or trust values. The privacy-preserving

reputation system preserves vehicles' privacy by aggregating their feedback without compromising their feedback values. Two key challenges are central to the design of Decentralized reputation systems: 1) Decentralised systems must protect participants' privacy (i.e., driver) while ensuring that reputation scores are accurate and reliable. Aggregate reputation scores should only be revealed to participants without disclosing the participants involved in aggregation scores and their trust values, and 2) The values cannot be used to determine vehicle relationship networks. While preserving feedback value, the system also ensures that the participant's provided feedback score is within a prescribed range without revealing the actual feedback score. This will limit misbehaving users to assign extremely high or low trust values to increase or decrease the reputation of specific vehicles maliciously. A vehicle that assigns feedback scores that are out of range is considered malicious in this study.

B. Threat Model

We aim to implement a privacy-preserving reputation system for IoV to achieve two objectives: 1) assess the trustworthiness of vehicles without revealing their feedback scores, and 2) calculate the aggregated reputation of the scores within a predefined range.

To meet these goals, we have devised a threat model that considers the possibility of honest feedback providers. Still, they are curious to learn private information related to other users and the malicious vehicles that might submit out-of-range values to manipulate the reputation of other vehicles. The proposed system encrypts scores and employs non-interactive zero-knowledge proofs to verify the validity of the encrypted scores. RSU are responsible for managing the data and preventing any vehicle collusion.

C. Related Works

Blockchain technology is introduced to IoV to utilise the decentralisation, verification and immutability characteristics. Blockchain incorporates with IoV to solve the problem of retrieving relevant information between network vehicles. Only a few considered calculating the trustworthiness of the vehicles based on the reputation reported by individual vehicles. Mollah et al., 2020) [4] focuses on an architecture for sharing data and resources based on the blockchain without considering the trustworthiness of the senders. Blockchain technology's economic, social, and environmental impacts on IoV are assessed [5]. This resulted in a system of rewards and punishments, reliability, and timeliness that can serve as a foundation for the entire blockchain Internet of Value. Moreover, Das et al.(2022) [6] develops a similar system to collect the toll tax from vehicles on national highways.

The few studies that focus on the reputation system within IoV are the following: Singh et al. (2020) [7] develops a smart contract for IoV that utilises blockchain to report any misbehaviour activity within the IoV based on the vehicles' trust. Hirtan et al. (2020) [8] proposes a network based on a reputation-based blockchain, but does not report any suspicious behaviour within the network. Moreover, Firdaus et al., (2021) [9] proposes a decentralised trust data sharing on IoV in which trustworthiness is calculated based on previous experiences using a game-theoretic model. This system is not focused on the authenticity of the feedback, storage security or reputation score transparency. Cocirlea et al., (2020) [10] relies on the reputation for validating data sharing using blockchain for IoV. A vehicle's reputation is determined by its past performance reporting events, and providing reliable data. However, all the data collected is processed by the master node.

A reputation value is generated based on network interactions in which the trustworthiness is determined based on the reputation [11]. This paper does not consider authenticity, secure storage, and individual vehicle feedback collection. Similarly, the system manages traffic-related cryptocurrencies to reward vehicles that assist it [12]. Vehicles are determined to be eligible for rewards based on their reputation. The paper does not provide details about the implementation of the reputation system; therefore, it is difficult to evaluate its reputation and trustworthiness.

According to the literature study, while some studies focuses on trust and reputation-based systems for the IoV, there is a significant gap in addressing feedback authenticity, safe storage, and transparency of reputation scores as shown in Table I. To ensure the security of data aggregation, a comprehensive approach that addresses the authenticity of feedback, secure storage, and transparency of reputation scores is required. Consequently, it is critical to design a secure and robust system capable of efficiently addressing these challenges and increasing the trustworthiness of the IoV network. This work intends to extend our work [13] by bringing the reputation system for IoV networks to the RSU level. The IoV system can be leveraged with security and privacy features.

TABLE I
COMPARISON OF PROPOSED REPUTATION SYSTEM WITH REPUTATION SYSTEMS.

	Storage Security	Scores Transparency	Privacy	Aggregation
[7]	×	×	×	Sum
[8]	×	√	×	Sum
[9]	×	×	×	Weighted Sum
[10]	×	×	√	Weighted Sum
[11]	×	×	√	Sum
This article	√	√	√	**Sum**

III. PROPOSED ARCHITECTURE

Using blockchain technology, we propose a decentralised reputation system for IoV, as shown in Figure 2. In our design choice, the vehicles provide their encrypted feedback score to the in-charged RSU, which is enabled with a blockchain system. Three fundamental challenges have been considered while proposing this architecture, which are the trustworthiness of the feedback score, the value of the feedback and the transparency of the reputation score. We use a token issued to vehicles for their interaction with other vehicles. The token is untraceable and unlinkable, ensuring that only honest vehicles (the ones who interacted) provide the feedback

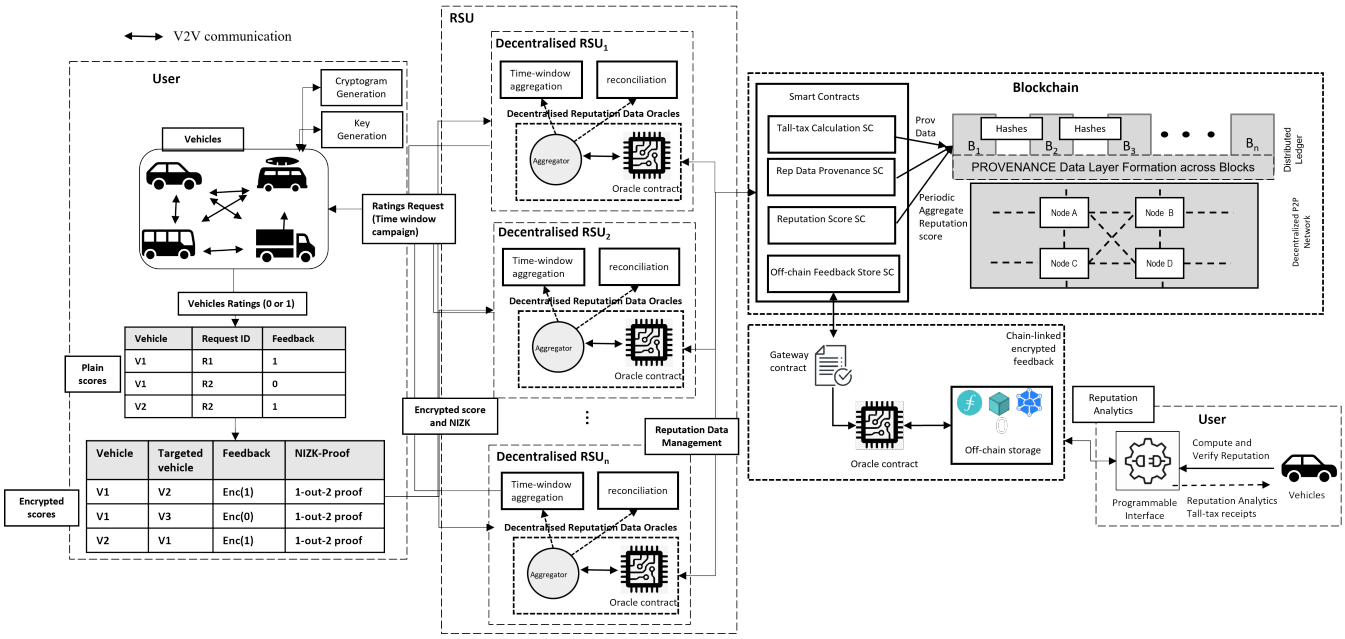

Fig. 2. Decentralised trustworthy Internet of Vehicles.

value. Individual vehicle feedback must be collected and stored is a second challenge while ensuring privacy and calculating aggregate scores. While all vehicle feedback can be stored on the chain as individual transactions, this has significant disadvantages, including privacy compromises, adverse scalability effects, and high storage costs. The third challenge is ensuring the reputation score's transparency and verifiability to ensure it is calculated accurately and all vehicle feedback is considered. A trustworthy reputation modelling system using homomorphic cryptography is being developed to address this issue. This will prevent malicious actors from discovering how a particular vehicle has rated others. Furthermore, we are currently working on ways to provide the public with access to the reputation scores calculated by the system. The following sections provide some information about our design choices and the components of the reputation system designed for this IoV.

A. Reputation Modelling

The Reputation Object in the system serves as a representation of a service's reputation. It contains attributes that make up the reputation score of a service, like the current value, historical value, and timestamp. These attributes provide structured information about a service, including its timeliness and a driver's driving style. The vehicle feedback system assigns a value to each attribute based on feedback from the vehicle. The feedback includes a value determined by the vehicle, a timestamp, and quality criteria related to the service, where each criterion can have a value of either 0 or 1.

A CrowdSensingFunction collects vehicle feedback which forwards vehicle feedback to ReputationCalculationFunction, which calculates the reputation score for a service based on the vehicle feedback at a given time instance by utilising appropriate functions.

B. Key Components

1) Vehicle Engagement: The proposed system does not require vehicles to anonymise their identities; instead, they conceal their ratings through cryptograms. Cryptograms are, in this case, encrypted feedback values, and the keys to the encryption have been generated by the vehicle itself to make it secure. Using this feature, the proposed system achieves end-to-end decentralisation while avoiding collusion between a central authority and a cryptogram generator. This rating score is encrypted using a cryptographic primitive (0 or 1, like or dislike, and a rating between 1 and 5 stars). Thus, an adversary on either side of this system, or the reputation system itself, cannot determine how a particular vehicle compares to another. The system could provide maximum privacy if it did not involve a maximum number of vehicles (n-1) colluding to determine the rating score of a target vehicle. In addition, the system is designed to ensure two other properties: 1) that vehicles are limited to providing ratings within a prescribed range and 2) that the reputation score provided by the system is publicly available.

2) Reputation Calculation: Once a vehicle has submitted its cryptogram and NIZK proof to the RSU, any entity (participant, system, or analyst) can calculate the aggregated reputation of that vehicle [14]. The RSU aggregator component performs this function by accessing the individual vehicle feedback provided by the RSU.

The reputation aggregation approach considers the objectives of implementing it over a decentralised blockchain. Public and private keys are generated by the vehicle and are published on its programmable APIs as part of the system. To contribute to the feedback score, the vehicle uses the public keys of all peers from the programmable API to compute the encryption keys and encrypts the score. A blockchain is used to aggregate the scores in a way that protects the privacy of

each individual.

The overall positive evaluation of a vehicle is determined by the sum of vehicles that have given it trust. The negative evaluations can be found by subtracting the positive evaluations from the total number of vehicles that have been evaluated. The final reputation of a vehicle is calculated using an aggregate beta reputation system as $REE = (PE-NE)/(n+2)$. n represents the number of vehicles that have submitted ratings. PE refers to the number of vehicles giving positive feedback about Entity E, and NE represents the number of vehicles that rated Entity E as untrustworthy.

Other reputation systems can also be easily adapted, e.g., averaging individual ratings over several vehicles can calculate an average rating. Despite valid transactions, new vehicles cannot gain a high reputation due to a small number of feedback scores. Our system addresses this problem by considering all vehicles with a reputation for a specified number of transactions. To prevent malicious activity, this method would secure the system from being taken advantage of by fraudsters. The reputation scores are calculated based on feedback values accessible in the centralised system, ensuring that the final reputation value will be accurate.

Another important feature our reputation system considered is real-time reputation aggregation which refers to the process of collecting and aggregating the trust scores from the vehicles in real-time to provide a comprehensive view of the behaviour of the vehicles in the system. Within this context, reputation data is stored across multiple off-chains and represent the vehicle feedback scores for the specific time window. The data from the off-chain is then aggregated together to generate the real-time reputation score that reflects a participant's overall trustworthiness within the system for that particular time window. The reputation score is then aggregated for all time windows using the method mentioned above.

3) Programmable API: The API allows vehicles to access their reputation scores and tax-tall records. The API service will be implemented to provide a programmable interface that can interact with other components and external services for added benefits. This is conducted through cloud-based infrastructure.

4) Blockchain and On-chain Storage: With Blockchain, end-to-end decentralisation can be achieved, and reputation data can be stored in an unchangeable tamper-proof manner. This facilitates trustworthiness and verification. Various types of reputation data are available within this system. Firstly, the feedback the vehicles provide, i.e., when they are contacted to share their feedback within the vehicular system. Secondly, the aggregate reputation score is derived from individual vehicle feedback. The link between these two data types is preserved and used to obtain verifiable reputation scores.

Moreover, the system aims to gather critical provenance information such as the participant count, response count, and time stamp. These verifiable reputation scores rely on this information to gain credibility. By incorporating smart contracts into the blockchain consensus, reputation data (aggregate reputation score) and provenance are recorded as transactions.

5) Off-chain and Connectivity with Blockchain: This proposal suggests that vehicle feedback will be stored off the blockchain to improve verification, querying, and compatibility. Keeping the data off-chain will also enhance scalability and can have a customized security layer to prevent unauthorized access. The solution is designed to use an Oracle to connect the on-chain and off-chain components, making them interoperable. The Reputation Data Oracle Service (RDOS) is responsible for connecting with vehicles to collect feedback, and it will create encrypted feedback data based on the reputation model (0-5, 0,1, . . .).

6) Smart Contract Deployment: Our proposed blockchain system has been installed locally using Ganache and Web3, with smart contracts written in Solidity. Its implementation assures the system's dependability and security, allowing for the quick processing of transactions and data. Furthermore, the smart contracts were thoroughly tested with Truffle.

IV. Discussion and Future Research Directions

A. Security Analysis

1) Verifiability of Aggregated Scores and Provided Feedback: A database on-chain and off-chain is used to maintain the aggregated scores within this proposed system. Vehicles may access these data to verify computation scores, aggregated feedback values, and individual feedback scores provided by other vehicles. It provides a platform designed to handle large amounts of data efficiently. It allows for efficient processing and storing of reputation scores for many vehicles to build trust and confidence in the network.

2) Privacy and Integrity Analysis: To protect privacy and maintain data integrity, the system employs homomorphic encryption to encrypt individual feedback scores before storing them in the databases. Feedback scores are only revealed in aggregate form, meaning the individual feedback providers' preferences (like or dislike) cannot be revealed. However, the system is designed to be secure against potential threats such as collusions by multiple feedback providers. In the event that a group of n-1 vehicles (the number of vehicles that are participating in the feedback process) collude, the remaining vehicles will not be able to learn feedback from them. A centralised trusted system generates keys, secures key exchange, and does not collude with any third party. To attract new vehicles to participate in the system, vehicles must display their aggregate feedback scores on their programmable API to demonstrate their trustworthiness. However, these aggregate scores cannot be compared with other vehicles.

3) Performance Evaluation: This experiment is conducted with a web application, smart contracts, blockchain infrastructure, and off-chain storage (cloud). The web application provides the feedback function, installed on a personal server running Windows XP with a 2.4GHz processor and 16GB of memory. Personal servers also host proprietary oracles with reputation aggregation functions. On the Ethereum Ropsten testnet, smart contracts are deployed to enable on-chain storage on the Ethereum blockchain network. The proof of work consensus algorithm within the Ethereum Rospten testnet is used in our study. To achieve querying and verifying individual user feedback, Firebase is used as off-chain cloud storage.

Table II presents the performance data, including the amount of input supplied by individual vehicles and the time required

for aggregation. For instance, the feedback by an individual vehicle uses 128bytes. This can support the scalability of this framework and does not require a high data rate for transmission. Moreover, it can be demonstrated that the time required for end-to-end feedback is 78.32ms which is insignificant and can help in building system efficiency.

TABLE II
BENCHMARK PERFORMANCE EVALUATION

Benchmark	Value
Individual Vehicle feedback size	128bytes
Aggregation score size	128bytes
Time required for Public and Private Keys generation	62.5ms
Time required for Tokens generation	0.2ms
Time required for Storing individual feedback to blockchain	15.62ms
Time required for end-to-end feedback	78.32ms

In summary, the system aims to balance the need for verifiability and privacy by using homomorphic encryption in a decentralised system and securing the exchange of feedback scores between vehicles. This allows the system to provide valuable insights and benefits to various stakeholders, such as improving road safety, possibly reducing fuel consumption and enabling better decision-making for fleet management.

B. Future Research Directions

In addition to enhancing the limitations of the suggested system, there are several potential future research directions for IoV using blockchain, including:

- Consensus: The IoV environment requires efficient consensus mechanisms for transmitting high-frequency, high-velocity data and low communication time. An appropriate consensus mechanism is the foundation of any blockchain-based system and provides the basis for decentralised trustworthiness between the nodes and objects in the system. The most commonly used mechanisms are Proof-of-Work (PoW), Proof-of-Stake (PoS), and Delegated-Proof-of-Stake (DPoS), although many others have been explored, including Proof-of-Reputation (PoR). A system's complexity and security can also be affected due to this.
- Standards and Incentives: IEEE and 3GPP are actively working to implement data transmission on the IoV; more research will be necessary to ensure they effectively address the IoV environment's unique requirements. Moreover, investigating the best methods for motivating and discouraging good behaviour within the IoV network by rewarding vehicles and entities with a good reputation and penalizing those with a poor reputation.
- Secure reputation storage, sharing and access control: Implementing cryptography techniques such as homomorphic encryption and secure multiparty computation to enhance reputation data storage and sharing within decentralised storage. In addition, reputation-based access control mechanisms allow or deny access to specific IoV network resources, such as communication channels or sensor data, based on the reputation data.
- Fully decentralised, there is currently a centralised implementation of the proprietary Oracle database. It limits its implementation in a decentralised manner. Because Chainlink provides a decentralised approach to aggregation, a solution can be developed to leverage the system's security by decentralising the aggregator.

V. CONCLUSION

We developed a trustworthy decentralised, verifiable reputation system for IoV using blockchain. With external services (off-chain), the system aims to provide a trustworthy reputation while maintaining security, privacy, accountability, and unlinkability. We evaluated the system based on security requirements. As a result of the evaluation, the system is demonstrated to be performance efficient and effective. In conclusion, we have outlined future research directions to serve as a road map for other researchers.

REFERENCES

[1] Jiajia Liu and Jianhao Liu. Intelligent and connected vehicles: Current situation, future directions, and challenges. *IEEE Communications Standards Magazine*, 2(3):59–65, 2018.

[2] Muhammad Ajmal Azad, Samiran Bag, Simon Parkinson, and Feng Hao. Trustvote: Privacy-preserving node ranking in vehicular networks. *IEEE Internet of Things Journal*, 6(4):5878–5891, 2018.

[3] M Najmul Islam Farooqui, Muhammad Mubashir Khan, Junaid Arshad, and Omair Shafiq. An empirical investigation of performance challenges within context-aware content sharing for vehicular ad hoc networks. *Transactions on Emerging Telecommunications Technologies*, 33(10):e4157, 2022.

[4] Muhammad Baqer Mollah, Jun Zhao, Dusit Niyato, Yong Liang Guan, Chau Yuen, Sumei Sun, Kwok-Yan Lam, and Leong Hai Koh. Blockchain for the internet of vehicles towards intelligent transportation systems: A survey. *IEEE Internet of Things Journal*, 8(6):4157–4185, 2020.

[5] Xiaomin Du, Yang Gao, Chia-Huei Wu, Rong Wang, and Datian Bi. Blockchain-based intelligent transportation: A sustainable gcu application system. *Journal of Advanced Transportation*, 2020, 2020.

[6] Debashis Das, Sourav Banerjee, Puspita Chatterjee, Manju Biswas, Utpal Biswas, and Waleed Alnumay. Design and development of an intelligent transportation management system using blockchain and smart contracts. *Cluster Computing*, 25(3):1899–1913, 2022.

[7] Pranav Kumar Singh, Roshan Singh, Sunit Kumar Nandi, Kayhan Zrar Ghafoor, Danda B Rawat, and Sukumar Nandi. Blockchain-based adaptive trust management in the internet of vehicles using smart contract. *IEEE Transactions on Intelligent Transportation Systems*, 22(6):3616–3630, 2020.

[8] Liviu-Adrian Hîrţan, Ciprian Dobre, and Horacio González-Vélez. Blockchain-based reputation for intelligent transportation systems. *Sensors*, 20(3):791, 2020.

[9] Muhammad Firdaus, Sandi Rahmadika, and Kyung-Hyune Rhee. Decentralized trusted data sharing management on internet of vehicle edge computing (iovec) networks using consortium blockchain. *Sensors*, 21(7):2410, 2021.

[10] Dragoş Cocîrlea, Ciprian Dobre, Liviu-Adrian Hîrţan, and Raluca Purnichescu-Purtan. Blockchain in intelligent transportation systems. *Electronics*, 9(10):1682, 2020.

[11] Richard Dennis and Gareth Owen. Rep on the block: A next generation reputation system based on the blockchain. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 131–138. IEEE, 2015.

[12] Nyothiri Aung, Tahar Kechadi, Sahraoui Dhelim, Tao Zhu, Aymen Dia Eddine Berini, and Tahar Guerbouz. Blockchain application on the internet of vehicles (iov). *arXiv preprint arXiv:2205.03832*, 2022.

[13] Junaid Arshad, Muhammad Ajmal Azad, Alousseynou Prince, Jahid Ali, and Thanasis G Papaioannou. Reputable–a decentralized reputation system for blockchain-based ecosystems. *IEEE Access*, 10:79948–79961, 2022.

[14] Hoang Giang Do and Wee Keong Ng. Blockchain-based system for secure data storage with private keyword search. In *2017 IEEE World Congress on Services (SERVICES)*, pages 90–93. IEEE, 2017.

VI. Biography Section

Haitham Mahmoud is a research fellow in the field of Future Information Systems with a focus on 5G technologies. He received his PhD from Birmingham City University (BCU), UK in June 2022. Prior to this, he obtained M.Sc. and dual B.Sc. degrees in Electronics and Communication Engineering from the Arab Academy for Science and Technology (AAST), the British University in Egypt (BUE), and the Loughborough University (LU). Currently, he is a research fellow in the Future information networks research group at BCU, where he is involved in cutting-edge research projects.

Muhammad Ajmal is a Senior Lecturer in Cyber Security at Birmingham City University. Prior to this, they were a Senior Lecturer at the University of Derby and a Research Fellow at the University of Warwick, where they worked on privacy-preservation aggregation and analytics. They received their PhD in Electrical and Computer Engineering from the University of Porto and have worked in a leading VoIP telecommunication company in Pakistan. Their research interests include network security and privacy, specifically designing systems to secure telecommunications users from spam and exploring ways to protect the privacy of telephone users.

Junaid Arshad is an Associate Professor in cybersecurity at Birmingham City University, UK. Junaid achieved his PhD from the University of Leeds, UK where he investigated the challenge of effective intrusion severity analysis for clouds. His research is focused on challenges within cyber security emphasising the impact of novel and emerging technological paradigms, such as blockchain, distributed systems, cloud computing and big data. He has been actively involved in publishing high-quality research within this field and has served on the Program and Review Committee of a number of journals and conferences.

Adel Aneiba is a Professor at Birmingham City University with a PhD. in mobile computing and distributed systems. He has worked as a Senior ICT Consultant for over 10 years for international and governmental organizations, managing large ICT projects. Aneiba is the research lead for the Cyber-Physical Systems Research Group and supervises several PhD students working on various topics such as IoT, SDN, 5G, and blockchain applications in smart cities. His research interests include IoT, computer networks, evaluation and optimization, and blockchain. He is a member of ACM, IET and a Fellow of HEA.