Integrated Blockchain Manufacturing Design for Distributed Authentication, Validation and Secure Sharing of Events in VANET

[1]Anand N Patil and [2]Sujata V. Mallapur
[1]Department of Computer Science & Engineering, Faculty of Engineering & Technology (Co-Ed),
Sharnbasva University Kalaburagi, Kalaburagi, Karnataka 585105, India.
[2]Department of Artificial Intelligence & Machine Learning, Faculty of Engineering and Technology
(Exclusive for Women), Sharnbasva University Kalaburagi, Kalaburagi, Karnataka 585105, India.
[1]patilanand1990@gmail.com, [2]sujatamallapur@gmail.com

Correspondence should be addressed to Anand N Patil: patilanand1990@gmail.com

Article Info
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi: https://doi.org/10.53759/7669/jmc202303003
Received 10 June 2022; Revised form 30 September 2022; Accepted 30 November 2022.
Available online 05 January 2023.

Abstract – Intelligent transportation system (ITS) is a technique to improve the driving conditions and safety through collaborative exchange of information between vehicles. Ensuring the authenticity and secure exchange of the events is an important functionality of ITS. Recently blockchain based decentralized solutions are proposed to address event's authenticity and secure exchange instead of traditional centralized trusted third-party solutions. Along these lines, this work proposes a block chain based decentralized architecture to realize additional functionalities of fine-grained access control to events, revocation of access to events and ensuring the trustworthiness of the events. Block chain along with IPFS is used to realize these functionalities in a fully distributed manner using smart contracts. Performance comparison of proposed solution with state of art demonstrates a better resilience to attacks and comparatively lower execution costs for smart contracts.

Keywords – VANET, ITS, IPFS, Blockchain, Machine Learning, Manufacturing Design.

I. INTRODUCTION

Intelligent transportation system is a promising technique to improve the driving conditions through exchange of information between vehicles. Vehicular Adhoc Network (VANET) facilities the exchange of information between vehicles through two techniques of vehicle to infrastructure (V2I) and vehicle to vehicle (V2I) communication with dedicated short-range communication (DSRC) radio [1]. Though exchange of events brings many advantages like reducing congestion, getting assistance etc it also exposes the network to various attacks and security vulnerabilities. False messages can be propagated by attackers. They can create social unrest by intercepting, modifying, replay or dropping messages. Ensuring authenticity, validity and integrity of event message is important to prevent from impersonation, malicious tampering and possible real-world fatalities. Many centralized solutions have been proposed for registration, authentication, and revocation of vehicles [2]. But these solutions are prone to various attacks like tampering, distribution for forged information, single point of failure, leakage of private information etc [3]. Various attempts have been made to solve the problems in centralized architecture by combining Blockchain with VANET. Blockchain is a distributed ledger technology [4] that provides tamper resistant storage for information. The parameter needed for authentication like certificates can be stored in blockchain and used for authentication [5-7].

Various blockchain based solutions for VANET have been proposed and discussed in detail in the Section II. Most of the solutions address vehicle authentication and secure event sharing. But these solutions have three important issues: revocation of access rights of misbehaving vehicles, does not check trustworthiness of event before storing to blockchain, there is no fine-grained access control on events depending on user's attributes. This work addresses these problems and proposes a Blockchain based distributed framework for VANET. As part of the work, a collaborative event confidence model is proposed to ensure the trustworthiness of the event before the event is uploaded to Inter planetary File system (IPFS). The information needed for authentication of vehicles are managed by both block chain and IPFS with support for revocation of misbehaving vehicles. In addition, the event message from vehicle is split to two categories of private and public. Private information is uploaded to IPFS with fine grained access control for the private information using a

modified cipher text policy attribute-based encryption (CP-ABE).
Following are the contributions of this work.

(i) Block chain with IPFS assisted authentication and revocation of vehicles.
(ii) A collaborative event confidence model to
ensure the trustworthiness of event before sharing it
(iii) CP-ABE based access control for private information sharing of events in a secure manner using IPFS.

The rest of the paper is organized as follows. Block chain based distributed authentication and event sharing solutions for VANET's are discussed in section II. Section III details the proposed solution for event authentication, validation, and secure sharing of events. Section IV details the results of the proposed solution and comparison with most recent solutions addressing the same problem. Section V presents the conclusion and scope for future research.

II. RELATED WORK

In [8] proposed a novel decentralized architecture using a combination of blockchain with IPFS. Authentic credentials are stored in blockchain, and vehicles are authenticated in decentralized manner. Events are shared among authenticated vehicles by storing in IPFS and sharing the location hash among vehicles. But the approach does not provide any access control for the events. The [9] proposed a secure blockchain based announcement message sharing framework for Internet of Vehicles. The messages are authenticated before storing on blockchain. When fake messages are found, the identity of sender is revealed and punished by imposing storage restrictions for further messages. The messages are stored on blockchain adding to load of blockchain and there is revocation of access rights on users. In [10] proposed a blockchain based message dissemination framework for VANET. Block chain is used to store both event messages and trust of the vehicles. Any vehicles which receive message notification, verifies the trustworthiness of the sender before getting the event from blockchain. The [11] proposed secure data storage and sharing framework using consortium blockchain. Digital signature technique using bi-linear pairing of elliptic curve is employed to ensure reliability and integrity when transmitting data. Fine grained access control on the shared data was not considered in this work. The [12] proposed a proof-of-concept event consensus mechanism for vehicular networks. The event consensus mechanism has two pass threshold-based event validation mechanism and two-phase consecutive transaction on block chain. The solution has higher overhead due to use of two block chains at local and global level. The [13] proposed a reputation-based data sharing scheme using consortium blockchain and smart contract technologies. Data sharing is restricted by authentication using blockchain. Reputation of vehicle is managed using a three-weight subjective logic model. Reputation scores are stored in block chain and vehicle receives events only from vehicles above a reputation score threshold.

In [14] proposed a privacy preserving announcement protocol for VANET called Credit Coin. Credit Coin is a block chain-based incentive scheme where users get credit for sharing traffic information. Users create anonymous signature with Credit coin and can disseminate the information using anonymous signature. Message exchanged in VANET network is prone to tampering and privacy attacks. At [15] proposed a data sharing architecture combining blockchain with federated learning. Hybrid block chain architecture is used in this work. Two-stage verification is done before data is shared through blockchain. The method brings higher overhead on blockchain due to storage of all events as separate blocks. In [16] proposed a block chain based reputation system for VANET. Distribution of forged messages is prevented based on historical interactions and indirect opinion of vehicles. The solution handled only trust of vehicles but security challenges in event sharing was not considered. In [17] improved block chain-based reputation system with certificate and revocation transparency using two separate blockchain. The trustworthiness of message is ensured using reputation of the sender. The [18] proposed a block chain based trusted data sharing scheme. Paillier crypto system is used to encrypt event data for data confidentiality. The integrity of the data is ensured by storing the hash in blockchain. Blockchain overhead is higher in this approach. In [19] proposed a secure data sharing scheme based on blockchain for vehicular networks [22]. Vehicle reputation values are calculated, and the reputation score is used for authenticating the messages. Data is stored in IPFS to reduce the overhead on blockchain. The solution could not provide fine grained access control over the events and does not support revocation of access.

III. BLOCKCHAIN IPFS FRAMEWORK FOR VANET

The proposed blockchain IPFS framework address three important gaps in existing distributed event authentication and sharing solutions for VANET: revocation, fine grained access control and continuous event trustworthiness model.

The architecture of the proposed solution is given in **Fig 1**. The architecture has following entities: trusted authority(TA), roadside unit (RSU), vehicle(VEH), blockchain network, IPFS storage and querying users.

The proposed solution has following stages: (i) Registration & Revocation, (ii) Event Processing, (iii) Access controlled event storage and sharing. Each of the processing stages is detailed in below subsections.

Registration & Revocation

RSU and vehicles must register to TA.

RSU selects his identifier RID_a , creates public key ($PURID_a$)and private key ($PRRID_a$). RSU sends ($RID_a, PURID_a$) to the TA. TA executes a smart contract updatePK to store the public key of RID_a into blockchain. The update PK function using the public key information table (PKIT) for updating in smart contract is given below.

Algorithm 1*: updatePK*

```
    Input: $PURID_a$,$RID_a$
    PKI[i]:PK ←$PURID_a$
    PKI[i].SID←$RID_a$
```

After storing the public key of RSU into public key information table, TA supplies a key K which is used for sharing any information among the RSU.

Vehicle register to TA by sending its ID (VID_b) and a pseduonym (TID_b). TA calculates a secret credential (TA_b), it creates a block B_1 with information of ($VID_b, TID_b, TA_b,\ CSLocation$). $CSLocation$ is pointer in IPFS with information of where vehicle is valid or not, It has value as 0or 1. 1 mean vehicle is valid and 0 means vehicle is invalid.

The root Merkle hash of block $root_{mer}$ is computed as $root_{mer} = h(h(TID_b)||h(TA_b))$ (1)

This block B_1 is added into block list by a smart contract and the index of the block I_{B_1} is returned to the vehicle. By this way, this work adds a provision to revoke the vehicle. Vehicle renovation is done at TA. When a traffic administrator wants to penalize the vehicle, he contacts TA.

TA searches the matching block for a vehicle VID_b , it gets the $CSLocation$ from the block. At that location it sets value of 0, when it wants to revoke the vehicle.

Event processing

Vehicle detects an event E_m and send the event to RSU. At RSU, following are the stages in event processing.

- Authenticating the vehicle
- Check for integrity of event and
- Evaluating the trust of the event.

Vehicle sends the detected event with additional information by encrypting with public key of RSU (E_m, B, TID_b, TA_b, I_{B_1} , TS) B is calculated as

$$B = h2(E_m, TA_b) \tag{2}$$

Where TS is the time stamp.

When the encrypted (E_m, B, TID_b, TA_b, I_{B_1} , TS) is received, RSU decrypts using it private key.

It checks if the current timestamp – TS < threshold time. If it is less than threshold time, the event is processed, or it is treated as replay attack and dropped.

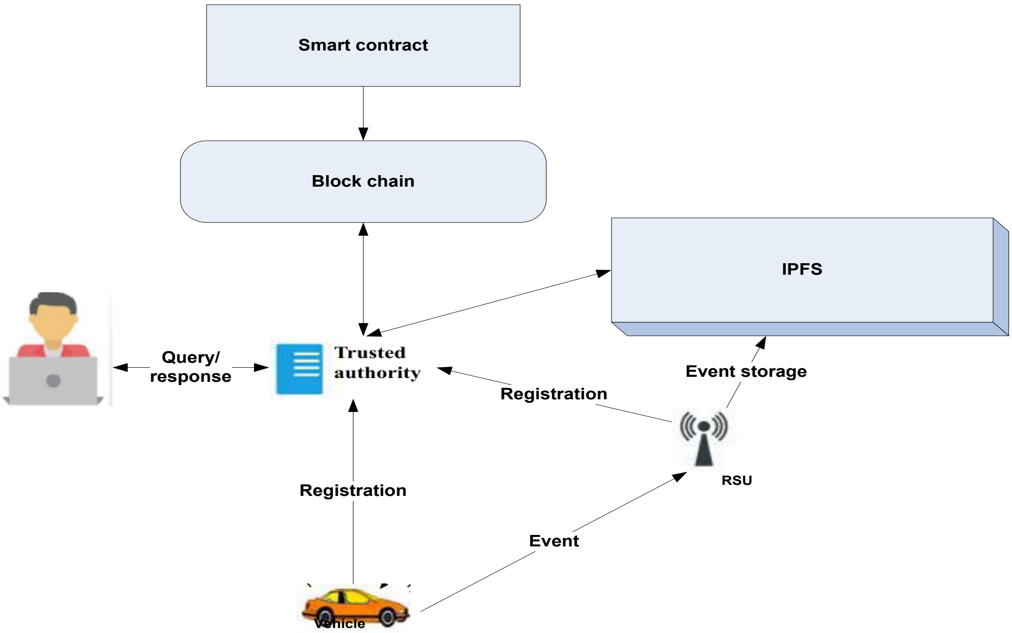

Fig 1. Architecture of Proposed Solution

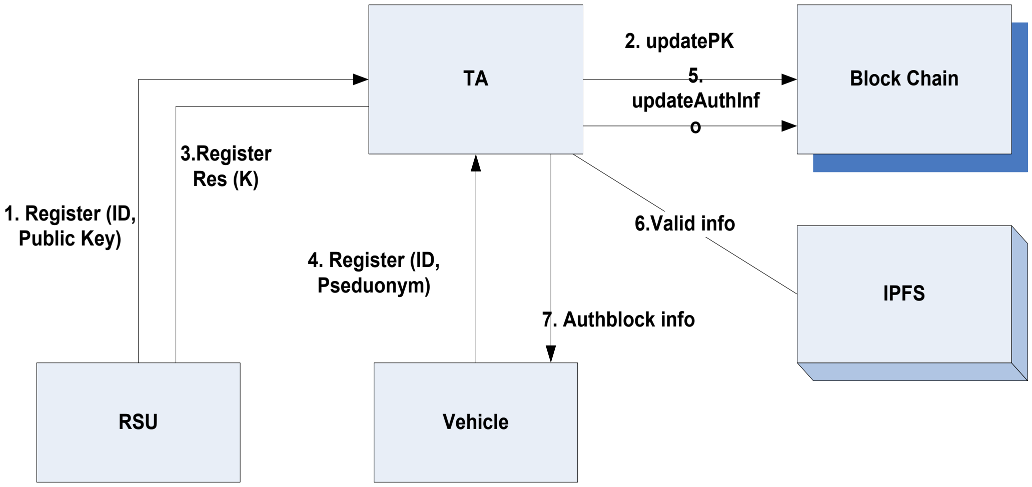

Fig 2. Processing Flow

RSU gets the $root_{mer}$ from the blockchain corresponding to I_{B_1}

$$\text{It calculates } root'_{mer} = h(h(TID_b)||h(TA_b)) \tag{3}$$

if $root_{mer} == root'_{mer}$, then vehicle is authentic. It then executes a smart contract to check if the vehicle is valid and not revoked.

Algorithm 2: CheckRevoke

```
Input: $TID_b$
CS← Block[$TID_b$]. $CSLocation$
If CS.Valid == 0
        Return true.
Else
        Return false
```

Once the vehicle is authentic and found not revoked, the next stage of checking the integrity of vehicle is launched.
RSU calculates $B' = h2(E_m, TA_b)$ and checks if $B' = B$, then E_m integrity is passed.
The next stage is checking the evaluating the trust of the event in **Fig 2**.
Event confidence model proposed in this work is an adaptation of model proposed in [18] except that instead of Bayesian confidence fusion followed, we have used trust scoring based confidence fusion in this work.

Access controlled event storage and sharing

The event from vehicle after it is confirmed by RSU, it must be stored in IPFS. Earlier solution did not supply any fine-grained access control on the event during access. The work views the event as E_m has multiple parts and the access control on these parts are different for different group of users.

There can be multiple users like Vehicles, Insurance company, Traffic enforcement etc. To supply differential access, this work uses a variant of Cipher text Attribute based encryption (CP-ABE).

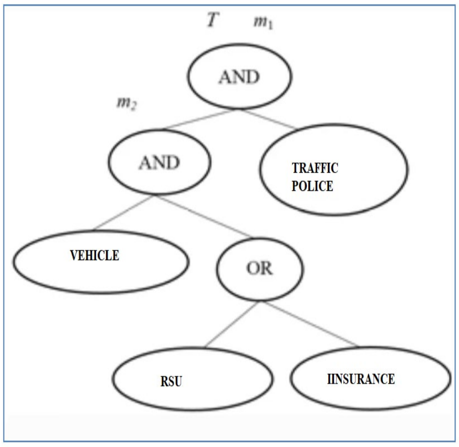

Fig 3. Access Control Rules

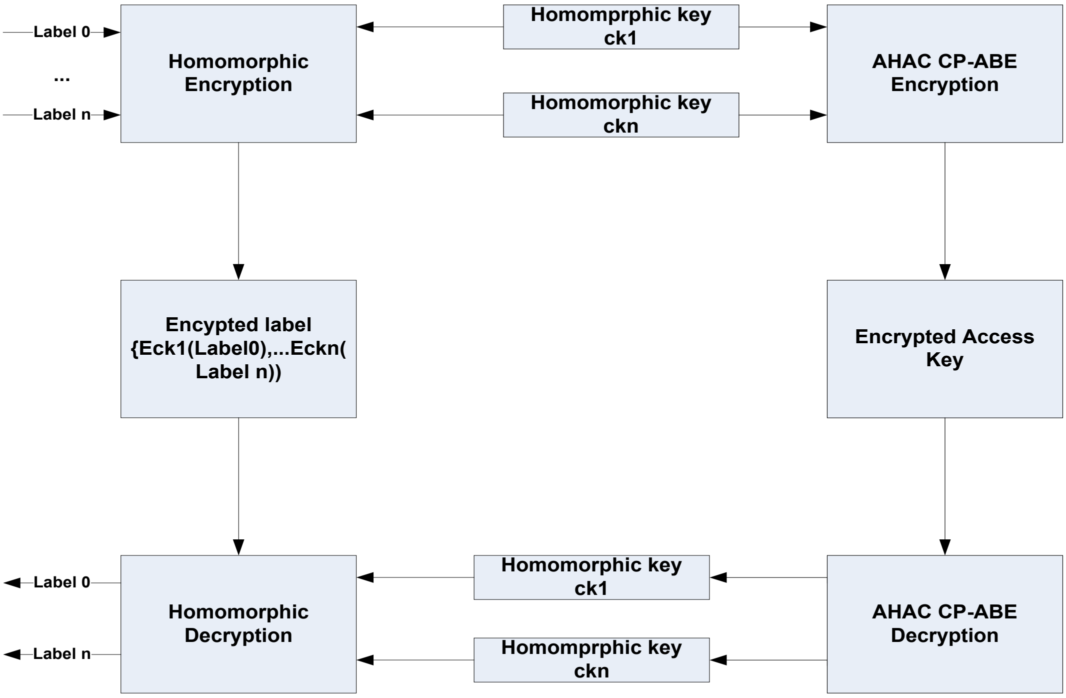

Fig 4. Fine Grained Access Control

The E_m data is arranged in multiple parts $label_o, label_1, label_{n.}$ etc, Each of the parts $label_x$ the data owner defines the access tree T. When a data user's attributes match the partial access structure (**Fig 3**), he can decrypt the data that associate with that level.

The access index of form $\{< T_1, Level\ x >, \ldots < T_n, Level\ x >\}$ where for each tree, the level of view for the user is defined. This access index is maintained in the cloud. Homomorphic encryption keys generated for each level $\{ck_{l0}, ck_{l1}, .. ck_{ln}\}$ is encrypted using AHAC CP-ABE algorithm.

AHAC CP-ABE encryption algorithm takes the access tree for each level and the homomorphic keys for each level as input and encrypts the homomorphic keys. AHAC CP-ABE decryption takes the level attributes and the encrypted homomorphic keys as input and provides the corresponding homomorphic key for the levels matching to level attributes and the level (lt). From the symmetric key, the encrypted token $eck_{l0}, eck_{l1}, .. eck_{ln}\}$ at level lt is decrypted using the corresponding key ck_{lt} with homomorphic decryption algorithm. The encryption and decryption flow using AHAC CP-ABE is given in **Fig 4.**

The trusted authority generates the homomorphic keys for each user and shares it all the RSU. It also maintains the Encrypted access key. Each of RSU, split the parts and encrypts the parts using homomorphic encryption. The encrypted label is then uploaded to IPFS, and the hash of the location returned by IPFS is stored in cloud. The map is kept at cloud with incident keyword vs the location hash of IPFS.

When users are requesting the information at TA, The encrypted access key and the access attributes of user are passed to AHAC CP-ABE decryption to get the decryption key for that particular user. Look up is done on cloud with the incident keywords as input, to get the location hash in IPFS. The data is retrieved from the location hash, decrypted with the decryption key found for the user and the decrypted information is given to the querying user.

IV. RESULTS

The performance of the proposed solution is simulated in Python and results are compared to state of art existing works. The VANET configuration used for simulation is given in **Table 1.**

Table 1. Simulation configuration

Parameter	**Values**
Number of vehicles	100-500
Mobility model	Krauss
Transmission range	300m
Simulation	4000m * 4000 m
Simulation time	30 minutes
Vehicle speed	20 to 100 Kmph

The simulation was conducted against following VANET topology **Fig 5** with RSU placed at all intersections (marked red).

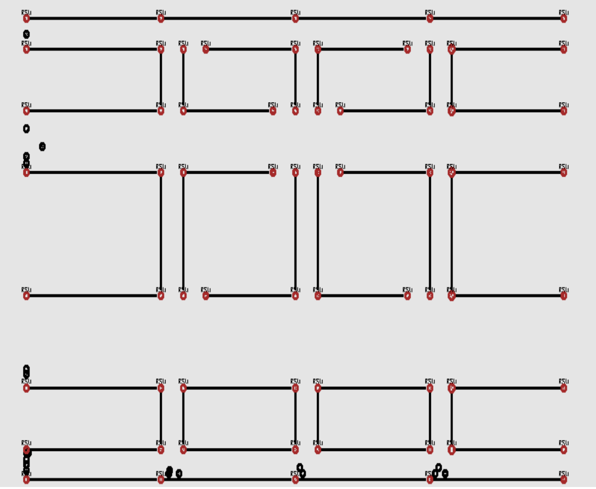

Fig 5. VANET Topology

Hyperledger fabric was used for Block chain with IPFS with architecture shown in **Fig 6**. Two smart contracts: updatePK, checkRevoke are written as chaincode in Python. Chain code runs in secured Docker container. It initializes and manages ledge state. Two chain codes updatePK, checkRevoke are managed as application chain code and realized as stateless UTXO (unspent transaction output) asset management. Each of the chain code is realized as standalone contracts.

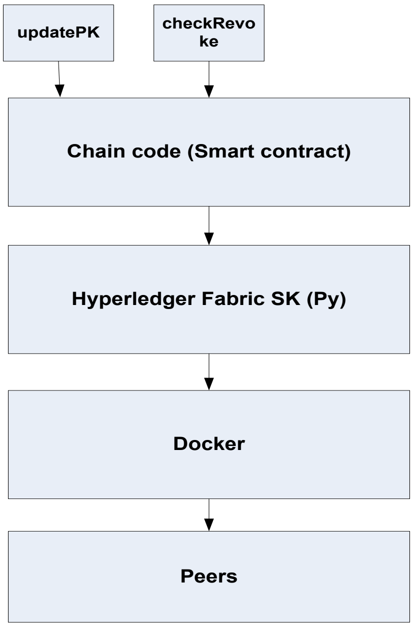

Fig 6. Block Chain Realization

Hyper ledger fabric setup configuration used for simulation is given in **Table 2.**

Table 2. Hyperledger Simulation Configuration

Parameter	Values
Fabric version	Fabric 1.4
No of peers	2
Block size	500
Database type	CouchDB
Tx arrival rate	50 to 200 tps
Work load	Uniform,
Zipfian skew	1

The performance of the proposed solution was measured in terms of: vehicle authentication time, event authentication time, communication cost, storage cost, throughput &latency on block chain and fake message detection effectiveness. The performance of the proposed solution is compared against Secure IPFS enabled event storage framework proposed by [8], block chain based secure data storage proposed by [19] and Block chain-based data storage with privacy protection scheme proposed by [20].

The average vehicle authentication **Fig 7** time [21] is measured by varying the number of vehicles and the result is given in **Table 3**.

Table 3. Vehicle Authentication Time

No of vehicles	Proposed	Dwivedi et al [8]	Javed et al [19]	Shi et al [20]
100	2.2	2.3	2.6	2.7
200	2.4	2.5	2.9	2.9
300	2.5	2.7	3.0	3.1
400	2.7	2.9	3.1	3.2
500	2.8	3.0	3.2	3.3
Average	**2.52**	**2.68**	**2.96**	**3.04**

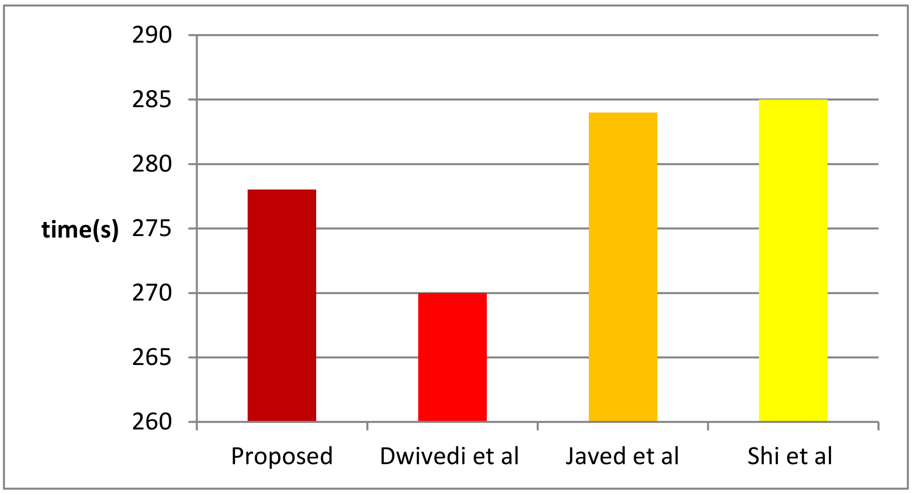

Fig 7. Comparison of Vehicle Authentication Time

The average vehicle authentication time in proposed solution is 6% lower compared to Dwivedi et al, 17% lower compared to Javed et al and 20% lower compared to Shi et al. The authentication time has reduced slightly lower in proposed solution due to use of only three interactions and only two fields required for authentication compared to more number of interactions in Javed et al and Shi et al.

The average event authentication time **Fig 8** is measured varying the number of vehicles and the result is given in **Table 4**.

Table 4. Event Authentication Time

No of vehicles	Proposed	Dwivedi et al [8]	Javed et al [19]	Shi et al [20]
100	110	121	140	144
200	115	124	142	146
300	120	128	145	150
400	125	132	147	151
500	131	135	149	153
Average	**120.2**	**128**	**144.6**	**148.8**

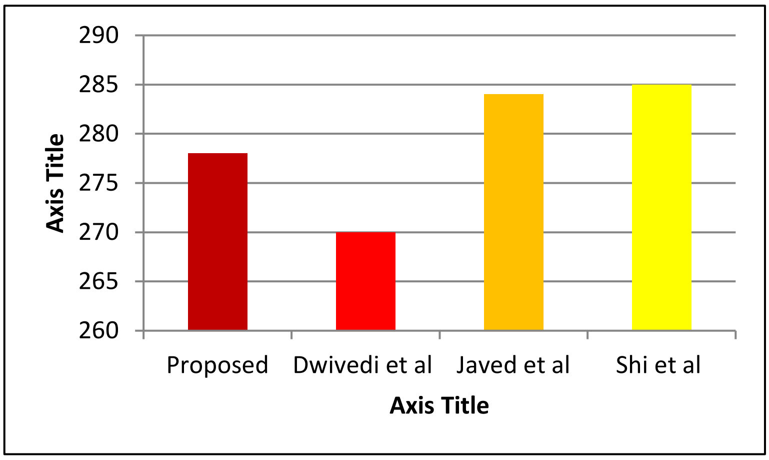

Fig 8. Comparison of Event Authentication Time

The average event authentication time in proposed solution is 6% lower compared to Dwivedi et al, 20% lower compared to Javed et al and 23% lower compared to Shi et al. The event authentication is lower in proposed solution as the information needed for authentication are computed offline and readily available in Blockchain.

The communication cost **Fig 9** is measured varying the number of vehicles and the result is given in **Table 5**.

Table 5. Communication Cost

No of vehicles	Proposed	Dwivedi et al [8]	Javed et al [19]	Shi et al [20]
100	17017	26016	27416	28123
200	31133	38919	39713	39912
300	42314	46214	47842	48101
400	47423	50542	51121	52321
500	51543	54672	55212	56101
Average	37886	43272	44260	44911

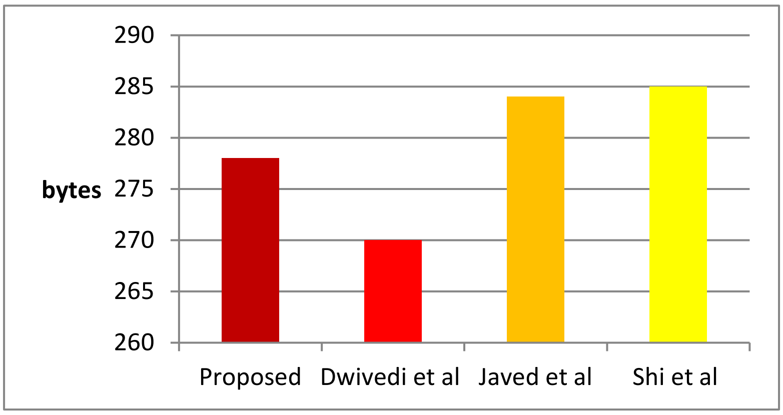

Fig 9. Comparison of Communication Cost

The average communication cost in proposed solution is 14% lower compared to Dwivedi et al, 16% lower compared to Javed et al and 18% lower compared to Shi et al. The communication cost has reduced due to use of less number of messages communicated for authentication and event sharing in proposed solution. Most of the information is stored in IPFS and only notification is shared in VANET. This reduced the packet payload and hence the communication cost reduced.

The storage cost is measured, and the result is given in **Fig10.**

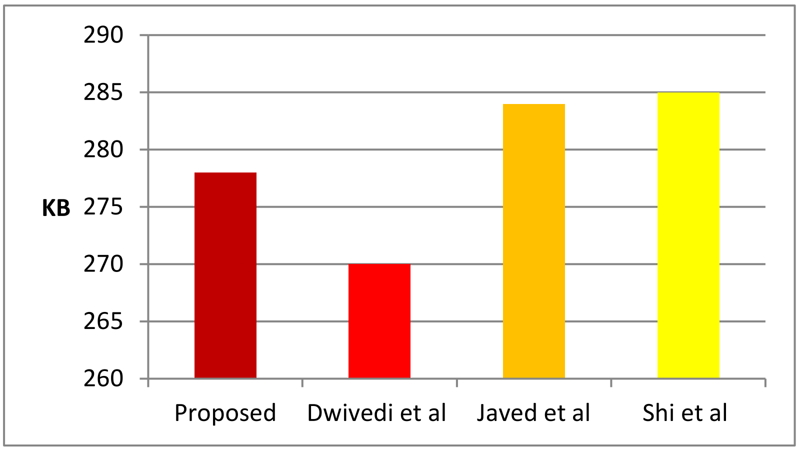

Fig10. Comparison of Storage Cost

The storage is proposed solution is 2.8% higher compared to Dwivedi et al but it is 2.1 lower compared to Javed et al and 2.5% lower compared to Shi et al. Due to storage of fine grained access privilege information apart from events, the storage cost is 2.8% higher in proposed solution compared to Dwivedi et al. But the storage cost is lower compared to Javed et al and Shi et al due to storage of only private information in IPFS compared to entire event information in Javed et al and Shi et al.

The fake event detection accuracy in proposed solution for different density of vehicles is measured and compared against reputation based fake message detection approach proposed by Lu et al [17].

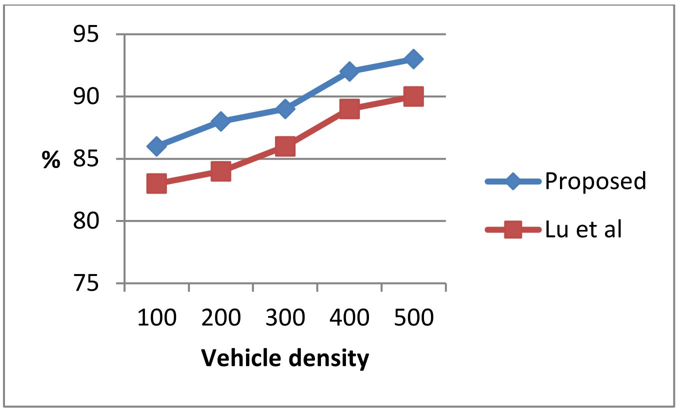

Fig 11. Comparison of Vehicle Density

The average fake event detection accuracy **Fig 11** in proposed solution is at least 3% higher in proposed solution. The event confidence model used in proposed solution can provide clear separation between real and fake events due to it continuous monitoring and scoring the nodes. The temporal nature of event source behavior is better capture due more neighbor considered for collaborative event validation in proposed solution. This has increased the fake detection accuracy in proposed solution.

V. CONCLUSION

An integrated blockchain IPFS based framework is proposed for authentication, validation and secure event sharing in this work. The proposed solution differed from existing works through a collaborative event confidence model to detect fake events, fine grained access control over the events, and revocation of vehicle on misbehavior. The proposed solution reduced the event authentication time by atleast 6%, communication cost by atleast 14% compared to existing works. The event confidence model proposed in this work is able to achieve atleast 3% higher fake message detection accuracy compared to existing works.

Data Availability

No data were used to support this study.

Conflicts of Interest

The author(s) declare(s) that they have no conflicts of interest

References

[1]. Y. J. Li, “An overview of the DSRC/WAVE technology,” International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. Springer, Berlin, Heidelberg, 2010: 544-558

[2]. S. Nikolidakis, D. Kandris, D. Vergados, and C. Douligeris, “Energy Efficient Routing in Wireless Sensor Networks Through Balanced Clustering,” Algorithms, vol. 6, no. 1, pp. 29–42, Jan. 2013, doi: 10.3390/a6010029.

[3]. R. G. Engoulou , “VANET security surveys,” Computer Communications, 2014, 44: 1-13.

[4]. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Technical Report, Manubot, 2019.

[5]. E. Portmann, “Rezension „Blockchain: Blueprint for a New Economy “,” HMD Praxis der Wirtschaftsinformatik, vol. 55, no. 6, pp. 1362–1364, Sep. 2018, doi: 10.1365/s40702-018-00468-4.

[6]. C. Lin, D. He, X. Huang, X. Xie, and K.-K.-R. Choo, “Blockchain-based system for secure outsourcing of bilinear pairings,” Inf. Sci., vol. 527, pp. 590–601, Jul. 2020.

[7]. C. Lin, D. He, X. Huang, M. Khurram Khan, and K.-K.-R. Choo, “A new transitively closed undirected graph authentication scheme for blockchain-based identity manag ement systems,” IEEE Access, vol. 6, pp. 28203–28212, 2018.

[8]. S. K. Dwivedi, R. Amin and S. Vollala, "Blockchain-Based Secured IPFS-Enable Event Storage Technique With Authentication Protocol in VANET," in IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 12, pp. 1913-1922, December 2021

[9]. L. Zhang, M. X. Luo, J. T. Li, M. H. Au, K. K. R. Choo, T. Chen, and S. W. Tian, “Blockchain based secure data sharing system for internet of vehicles: A position paper,” Veh. Commun., vol. 16, pp. 85–93, Apr.2019

[10]. R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, “A new type of blockchain for secure message exchange in VANET,” Digit. Commun. Netw., vol. 6, no. 2, pp. 177–186, May 2020.

[11]. X. H. Zhang and X. F. Chen, “Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network,” IEEE Access, vol. 7, pp. 58241–58254, Jan. 2019

[12]. Y. T. Yang, L. D. Chou, C. W. Tseng, F. H. Tseng, and C. C. Liu, “Blockchain-based traffic event validation and trust verification for VANETs,” IEEE Access, vol. 7, pp. 30868–30877, Mar. 2019

[13]. J. W. Kang, R. Yu, X. M. Huang, M. Q. Wu, S. Maharjan, S. L. Xie, and Y. Zhang, “Blockchain for secure and efficient data sharing in vehicular edge computing and networks,” IEEE Int. Things J., vol. 6, no. 3, pp. 4660–4670, Jun. 2019

[14]. L. Li, J. Q. Liu, L. C. Cheng, S. Qiu, W. Wang, X. L. Zhang, and Z. H. Zhang, “CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles,” IEEE Trans. Intell. Transp. Syst., vol. 19, no. 7, pp. 2204–2220, Jul. 2018

[15]. Y. L. Lu, X. H. Huang, K. Zhang, S. Maharjan, and Y. Zhang, “Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles,” IEEE Trans. Veh. Technol., vol. 69, no. 4, pp. 4298–4311, Apr. 2020.

[16]. Z. J. Lu, W. C. Liu, Q. Wang, G. Qu, and Z. L. Liu, “A privacy preserving trust model based on blockchain for VANETs,” IEEE Access, vol. 6, pp. 45655–45664, Aug. 2018

[17]. Z. J. Lu, Q. Wang, G. Qu, and Z. L. Liu, “BARS: A blockchain-based anonymous reputation system for trust management in VANETs,” In Proc. 17th IEEE Int. Conf. Trust, Security and Privacy in Computing and Communications/12th IEEE Int. Conf. Big Data Science and Engineering, NY, USA, 2018, pp. 98–103

[18]. B. K. Zheng, L. H. Zhu, M. Shen, F. Gao, C. Zhang, Y. D. Li, and J. Yang, “Scalable and privacy-preserving data sharing based on blockchain,” J. Comput. Sci. Technol., vol. 33, no. 3, pp. 557–567, May 2018.

[19]. M. U. Javed, M. Rehman, N. Javaid, A. Aldegheishem, N. Alrajeh, and M. Tahir, “Blockchain-based secure data storage for distributed vehicular networks,” Appl. Sci., vol. 10, no. 6, p. 2011, 2020

[20]. K. X. Shi, L. H. Zhu, C. Zhang, L. Xu, and F. Gao, “Blockchain-based multimedia sharing in vehicular social networks with privacy protection,” Multimed. Tool. Appl., vol. 79, no. 11, pp. 8085–8105, Mar. 2020.

[21]. Mallikarjun Maratha and Virupakshappa. "An efficient vehicle traffic maintenance using roadside units in VANET." Imperial Journal of interdisciplinary research, Vol 3, no. 1, pp. 783-784, 2016.

[22]. K. A. Abbas et al., “Unsupervised machine learning technique for classifying production zones in unconventional reservoirs,” International Journal of Intelligent Networks, vol. 4, pp. 29–37, 2023, doi: 10.1016/j.ijin.2022.11.007.