Journal of Theoretical and Applied Information Technology
15th February 2025. Vol.103. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PRIVACY-PRESERVING AND EFFICIENT DATA SHARING FOR BLOCKCHAIN-BASED INTELLIGENT TRANSPORTATION SYSTEMS WITH INTERNET OF VEHICLES (IOV)

[1*]SHAIK MOHAMMAD RAFI, [2*]Dr. R. YOGESH RAJ KUMAR

[1*]Reasearch scholar, Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India.
[2]Professor, Department of Information Technology, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India.
[1*]Corresponding Author E-mail: shaikmohammadrafi956@gmail.com
[2]Co Author Email: ryogeshrajkumar081@gmail.com

ABSTRACT

Recent years have witnessed the development and adoption of blockchain technology in intelligent transportation systems (ITS) because of its authenticity and traceability. However, increasing ITS devices imposes grand challenges in privacy-preserving and efficient data sharing. Recent research has demonstrated that integrating searchable symmetric encryption in blockchain enables privacy-preserving data sharing among ITS devices. However, existing solutions focus only on single-keyword searches over encrypted ITS data on the blockchain and suffer from privacy and efficiency issues when extended to multi-keyword scenarios. This work proposes a bloom filter-based multi-keyword search protocol for ITS data with enhanced efficiency and privacy preservation. We design a bloom filter to select a low-frequency keyword from the multiple keywords input by the ITS data owner. The low-frequency keyword can filter out a large portion of the ITS data from the search result, thus significantly reducing the computational cost. Furthermore, each identifier-keyword pair is attached with a pseudorandom tag that enables the completion of a search operation in only one round. To make changes in ITS data, include protocols for dynamic data updates, including addition and deletion, to the proposed system. Vehicle nodes' anonymity, data ownership, and secure communication during voting are supported by the blockchain foundation. The protocols allow for a fast, scalable, and privacy-preserving multi-keyword search for blockchain-based ITS, according to a comprehensive performance test. To ensure anonymity, traceability, and unlinkability of data sharing among vehicles. A comprehensive performance evaluation of the protocols was conducted.

Keywords: *Blockchain, Privacy-Preserving, Data Sharing, Intelligent Transportation Systems (ITS). Internet Of Vehicles (IOV).*

1. INTRODUCTION

In the past decades, intelligent transportation systems (ITS) [6] have emerged, integrating the technologies of computer vision, sensing, wireless communication, etc., to reduce traffic accidents and improve transportation efficiency. To provide quick and safe decision-making in ITS, autonomous cars must exchange massive amounts of data with the infrastructure (i.e., base stations and units placed along the route) [14]. For instance, adjacent cars may get incident information fast, which improves course planning and allows for more precise arrival time prediction [4]. To optimize traffic flow, traffic lights may also be meticulously timed using road traffic data [5]. The traditional ITS data-sharing approaches can be categorized into data hosting-based [19] and data aggregation-based [3]. In data hosting-based approaches, the roadside units and base stations serve as the data hosting center storing data and responding to the search queries from the vehicles [13]. Concerns about privacy and efficiency arise from the large volume and sensitivity of the uploaded data. The cars transmit just the metadata, or descriptions, to the roadside devices and base stations in data aggregation-based methods, rather than the actual data itself [12]. Under these conditions, it is very difficult to guarantee the presence of raw data matching the metadata, which leads to problems with authenticity. Data hosting and

data aggregation methods rely on a centralized server, either a roadside unit or a base station, which is insufficient. Research has highlighted blockchain technology as a key enabler for safe ITS data exchange to address centralization [11]. Specifically, automobiles, roadside equipment, and base stations function as both blockchain nodes and users. They run a blockchain and peer-to-peer network. Vehicle data is encrypted and saved on the blockchain. Smart contracts allow other cars, roadside equipment, and base stations to query this data privately [18].].

In ITS data-sharing systems that use blockchain technology, searchable symmetric encryption is often used to encrypt data and search queries before they are saved and performed on the blockchain [7]. One positive aspect is that privacy is maintained as the questioned party is unaware of much of the data. The whole blockchain network, on the other hand, executes the search queries using smart contracts, guaranteeing that the results are sound and comprehensive. Consequently, ITS devices may share data securely and privately by combining blockchain technology with searchable symmetric encryption.

Despite its importance, the most recent searchable encryption methods over blockchains [14] only take a single term into account. The methods may be made to work with more than one keyword by processing each one separately and then finding their intersection [17]. To be more specific, the blockchain nodes will be exposed to the intermediate results, which include the ITS data linked to every keyword. Several individuals are concerned about the security and privacy of their information due to this data leak [12]. The blockchain nodes also need to handle search requests with a single phrase in sequential order. An additional set of keywords is associated with some of the identifiers, so bear that in mind. As a result, handling several keywords comes with a hefty computational cost and time overhead. The need for the search smart contract to store the intermediate discoveries results in a substantial financial investment.

This study presents a reliable and secure ITS data-sharing system with database setup, dynamic updates, and multi-keyword search. Our database consists of various pairings of IDs and keywords. Each identifier has many keywords connected with it. The ITS data owner may change data by dynamically adding or removing certain identifier-keyword combinations after setup. ITS data owners may use multi-keyword searches to identify identifiers associated with certain keywords. The unique bloom filter-enabled technique in this study enables fast and cost-effective execution of multi-keyword search queries. Like blockchain nodes, ITS devices rent data and compute capabilities to profit. Blockchain smart contracts integrate database creation, dynamic updating, and multi-keyword search protocols. This study presents a bloom filter-enabled multi-keyword search protocol for blockchain-based ITS data exchange to save time and cost. It prevents smart contract cost restriction breaches using cost estimates. Real-world ITS dataset trials prove the methods' viability and efficacy.

Current Internet of Vehicles (IoV) systems suffer privacy risks from fraudulent communications, centralized trust dependencies, vehicle hijacking, and illegal monitoring. Single points of failure, delayed alerts, and intruder-broadcast false messages plague centralized methods. An authentication technique that protects vehicle identification, location privacy, non-repudiation, authenticity, and message traceability is needed.

Blockchain's decentralized structure and consensus algorithms provide a reliable and transparent environment for IoV data exchange Blockchain’s immutability, decentralization, and transparency ensure transaction confirmation, protecting against malicious nodes. Blockchain privacy-preserving solutions use cryptography to secure sensitive data. Permissioned blockchain architecture Hyperledger Fabric improves privacy with secret transactions and leader selection in its consensus method.

•

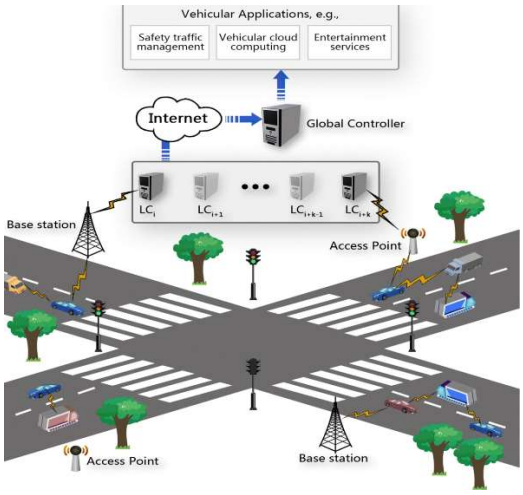

Figure 1: A System Model for Cloud Computing Based Privacy-Preserving Authentication Scheme

2. Research Gap

Current methods for conducting blockchain-based data sharing in ITS are limited to searches involving a single term, which is insufficient for the complicated needs of searches involving several keywords, even if these systems have shown possibilities for privacy-preserving data sharing in general. In addition, there is a lack of scalability, significant processing cost, and sufficient dynamic update methods for ITS data records in the present systems. Due to these restrictions, research must be conducted to share data efficiently and securely, allowing for simultaneous searches with multiple keywords.

3. RELATED WORK

The authors in [8] proposed a Conditional Privacy-Preserving Authentication (CPPA) scheme for vehicular ad hoc networks that uses Schnorr's signature. The secret key is pre-loaded on the vehicle but a long-term secret key can be accessed by an adversary when it has physical access. This compromises the scheme's privacy and security. In another study [9], the authors presented an Efficient, Anonymous Authentication with Conditional Privacy (EAAP) scheme based on a bilinear pairing technique, using anonymous certificates that are valid for short-term and public keys for IoV. In [10], the authors presented a secure authentication solution for authentication, integrity, and confidentiality. Traceability depends on a Trusted Authority (TA). This improves traceability, but a TA breach in [10] interrupts the network and creates a single point of failure The authors in [11] presented a scheme based on blockchain to protect the security and privacy of vehicle nodes. The authors proposed a Lightweight Scalable Blockchain (LSB), without traceability of the malicious vehicle nodes. The approach in [11], using Lightweight Scalable Blockchain (LSB), has limited scalability and efficiency because of the absence of batch verification and authentication features. The approach uses an Overlay Block Manager (OBM), which acts as a cluster head. It also did not provide batch verification or batch authentication. The proposed model is also affected by the issues of key management, caching data, and mobility.

The authors in [15] presented a seven-layer architecture for transportation systems. This paper also presented delegated proof-of-stake (DPOS), which is appropriate for vehicular communication because it establishes blockchain-based vehicular networks. The authors in [16] presented a distributed trust management scheme for a clustering mechanism for IoV based on blockchain technology. In this paper, block validation is performed by proof of work and roadside units function as miners performing POW for the consensus mechanism. The DPOS and POW techniques in [15] and [16] add computational cost. Roadside devices used as resource-heavy miners may cause delays and system strain. 6. Latency and Computational Overheads In [17], the authors proposed a Byzantine fault tolerance consensus algorithm for IoV. This algorithm provides a privacy-preserving incentive announcement network. The authors used a multi-weight subjective logic model and contract theory to prevent internal collision among miners. The authors in [20] recognize the difference between correct and fake transactions. In addition to increasing accuracy, this recognition prevents double-spending problems in which someone may be able to create multiple correct transactions and thus combine them to create a fraudulent transaction. The third phase is the latency of the system and computing power, which is needed to enable the correctness and agreement processes. These unforeseen consequences show that

vehicle network authentication methods confront complicated trade-offs and practical issues notwithstanding research improvements.

3.1 Blockchain-Based Intelligent Transportation Systems

With the popularity of blockchain technology, its applications in intelligent transportation systems have been attracting intensive attention from academia and industry. There are a bunch of survey papers about blockchain-enabled intelligent transportation systems [14, 11, 15]. As early as 2016, Yuan and Wang conducted a pioneering study of blockchain-based ITS and designed an ITS-oriented seven-layer blockchain conceptual model [43]. Mollah et al. presented the first comprehensive survey of blockchain-based ITS, covering the applications, architectures and frameworks, challenges, and future research opportunities [31]. More recently, Dibaei et al. focused on the security of vehicular networks and surveyed the blockchain and machine learning-based approaches to tackle security issues [7].

The research community has identified a bunch of critical applications of blockchain-based ITS, including data protection and trading, resource sharing, content broadcasting, and traffic control [13]. Many challenging issues arise and remain to be addressed, such as incentive mechanism design [28,19] and high-performance consensus [26]. For example, Li et al. proposed CreditCoin facilitating content broadcasting [28]. In particular, CreditCoin is a blockchain-based ITS incentivizing vehicles to share surrounding traffic information while guaranteeing its anonymity and authenticity.

3.2 Data Sharing in Intelligent Transportation Systems

Data sharing is essential for ITS because it enriches individual vehicles' knowledge, achieving higher road safety and better path planning [15]. Most existing data-sharing approaches derive from the requirement of ITS applications, e.g., content broadcasting and dissemination [12] and vehicular mobile social networks [16]. As an example, in a study conducted by Ko et al. [16], it was suggested that roadside units could arrange data services more easily if vehicles could share data. By creating a data-sharing method based on blockchain technology that is immune to manipulation, Sun et al. created safe and flexible vehicular social networks [9]. To a similar extent, Kong et al. [13] suggested a practical and effective method for enabling cars to exchange multi-dimensional sensory data while protecting user privacy. Furthermore, Gosman et al. considered the trustworthiness of information shared by vehicles and devised an approach to quality assessment concerning spatial accuracy, temporal closeness, and vehicle reputation [10].

3.3 High-Performance Search over Blockchain

In recent years, blockchain-based search has garnered a lot of attention [1,2]. One simple method involves a user sending a search query to a full node on the blockchain, and the node processing the query transaction by transaction. However, such an approach incurs low efficiency, integrity, and efficiency. Notably, it is time-consuming to scan the whole blockchain, a single full node can be malicious, and the data and search queries are transparent to the public. To this end, the researchers have been designing blockchain search protocols guaranteeing integrity and privacy and enhancing efficiency.

Smart contracts and verifiable computation are two mainstream approaches to enhancing search integrity. In smart contract-based methods, the requests from users are executed by all the blockchain nodes rather than a single one [17]. As long as a blockchain system is secure, the search results will be honourable because most blockchain nodes agree on the results. Such methods are convenient to be adapted to all kinds of blockchain data but are time and computation-intensive. Regarding verifiable computation, the full node returns not only the results but proof as well [19]. The returned proof is essential to verify the search results' integrity, i.e., soundness and completeness. Such an approach enjoys high efficiency owing to the design of subtle data structure for verification [21]. However, no universal data structure can handle every kind of data.

3.4 Secure and Efficient ITS Data Sharing

Autonomous vehicles enjoy privacy-preserving and efficient data-sharing services by sending the encrypted data and operations to and receiving encrypted query results from the

roadside infrastructure. On the other hand, the roadside infrastructure, including roadside units and base stations, maintains a blockchain and responds to the vehicles' operations by invoking pre-defined smart contracts.

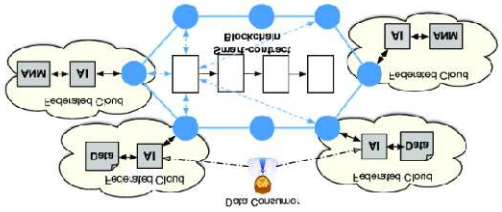

Figure 2: Blockchain Data Sharing System In A Federated Cloud (AI Stands For Anonymisation Interface, While ANM Stands For Anonymisation Service)

4. DESIGN AND DEVELOPMENT OF BLOCKCHAIN-BASED IOV IN CLOUD

In this section, we present an efficient, secure, decentralized, and anonymous network model for IoV to overcome the above limitations of security issues and authentication for data sharing. The proposed scheme provides traceability to identify malicious vehicle nodes. The proposed reputation scheme is based on the Hyperledger Fabric leader selection process. The scheme also satisfies the security and authentication requirements.

4.1 Network Model

The proposed scheme uses the Fabric Certificate Authority (CA) for the registration of identities. It has sufficient capabilities, such as high computation, fast communication, and enough storage. CA is also responsible for the generation of certificates for vehicles and roadside units. Additionally, once their registration is complete, the TA produces the initial security parameters for all vehicles and roadside units (RSUs) and sends them to the vehicles via TLS. Issuance of Enrolments Certificates (ECerts) is an enrolment process whereby the Fabric CA issues a certificate key-pair, comprised of a signing certificate and a private key that forms the identity [25]. The private and public keys are first generated locally by the Fabric CA client, and then the public key is sent to the CA, which returns an encoded certificate, the signing certificate for certificate renewal, and revocation. Orderers are stationary nodes deployed on the roadside. These orderers act as the RSUs. The orderer maintains the list of the organizations that can create and configure the channel and is responsible for ordering and packaging the transactions. The orderer also obtains the certificates that represent identities, and the Membership Service Provider (MSP) contains the permission identities. The orderer utilizes a dedicated short-range communication protocol for V2V and V2R wireless communications. The MSP authenticates traffic messages from vehicles and processes them locally or forwards them to the TA. The law enforcement department may request the CA to revoke the real identity of the message sender if malicious activity is detected. Vehicle nodes are embedded with high processing, storage, and wireless communication modules. The vehicle-to-vehicle and vehicle-to-RSU communications are conducted through wireless networks. The figure shows the layers of the proposed solution.

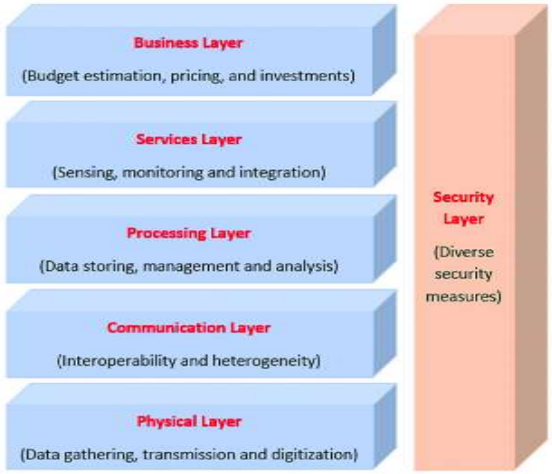

Figure 3: Layers Architecture Of IOV

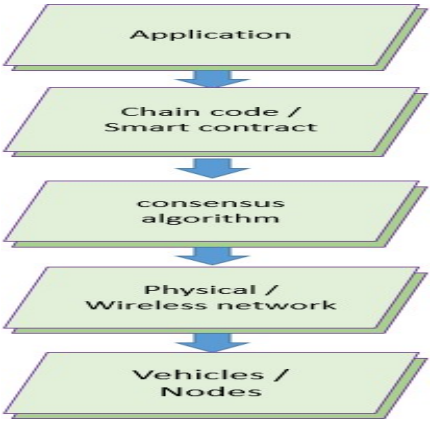

Figure 4: Layers Of The Proposed Network

The figure shows the different layers of the proposed network, comprising the application layer, chain code/smart contract layer, consensus layer, physical/wireless network, and ground vehicular nodes. Smart contracts are blockchain-based programs that execute when certain criteria are met. The contracts are decentralized applications that respond to events by executing business logic. These are often used to automate contract execution so that all parties immediately know the outcome without the need for any intermediaries.

4.2 Enhanced Hyperledger Fabric

Vehicles with OBU and digital networking equipment are blockchain-based IoV to communicate with neighboring RSUs, thus accessing vehicular networks. The OBU performs basic functions, collects local data, and sends it to the orderer via a communication channel. Vehicle nodes work as information providers and provide their information to data requesters. Vehicle nodes send their messages to the neighboring orderer. Orderers are stationed along roads to ensure that cars can connect with orderers. Orderers are stationary roadside nodes. According to their locations, the entire network is split into several regions. Without the help of a trustworthy third party, a group of auditors has the secret tracing key. If malicious conduct is discovered, the law enforcement department can request that group auditors revoke the true identity of the message. To retrieve the real identity of the sender, at least 't' tracers must work together. This is used to prevent misuse of power. We should mention that the CA and vehicle nodes in the scheme elect the issuers and auditors. The steps of the proposed scheme are system configuration, registration enrollment process, transaction handling, consensus process, ledger update, and traceability.

5 . PERFORMANCE EVALUATION

5.1 Experimental settings

Using the PYCRYPTODOME and PYBLOOM [1] packages, we develop the setup, addition, deletion, and search protocols in Python 3.9. These packages enable us to build the pseudorandom HMAC-SHA256 function and bloom filter, respectively. On workstations equipped with 32 GB RAM and Intel Core i9-10900 CPU, operate the ITS data owner and blockchain nodes. The operating system is Ubuntu 20.04.3. The blockchain nodes form a peer-to-peer network through the local area network and employ the proof-of-work [8] as the blockchain consensus protocol. The nodes respond to the setup, addition, deletion, and search requests from the ITS data owner by running the corresponding smart contracts. We employ proof of work as the blockchain consensus protocol and set the difficulties low to neglect the influence of the blockchain performance while focusing on the proposed data-sharing protocols only.

Table 1: Database Setup And Dynamic Update

Dataset (with Size)	Operation	No Multi-keyword Search Protocol	Multi-keyword Search Protocol
Enron Email Dataset 1, 352 MB in Size 517.0 K Identifiers 622.0 K Distinct Keywords 9.1 M Identifier-keyword Pairs	Setup	Data Owner 209 s Smart Contract 28, 219 TXs Blockchain Nodes 2.6 s Encrypted Database 378 MB	Data Owner 272 s Smart Contract 42, 356 TXs Blockchain Nodes 3.0 s Encrypted Database 532 MB
	Addition	Data Owner 1.4 s Smart Contract 1 TX Blockchain Nodes 1.2 s	Data Owner 2.0 s Smart Contract 1 TX Blockchain Nodes 1.5 s
	Deletion	Data Owner 1.0 s Smart Contract 1 TX Blockchain Nodes 1.2 s	Data Owner 1.0 s Smart Contract 1 TX Blockchain Nodes 1.4 s
Earth Surface Temperatu	Setup	Data Owner 1, 650 s	Data Owner 2, 105 s

re Dataset 572 MB in Size 10.0 M Identifiers 8.7 K Distinct Keywords 69.9 M Identifier-keyword Pairs		Smart Contract 216, 763 TXs Blockchain Nodes 20.0 s Encrypted Database 2, 903 MB	Smart Contract 325, 145 TXs Blockchain Nodes 22.2 s Encrypted Database 4, 084 MB
	Addition	Data Owner 1.7 s Smart Contract 1 TX Blockchain Nodes 2.1 s	Data Owner 2.2 s Blockchain Nodes 3.5 s
	Deletion	Data Owner 1.9 s Smart Contract 1 TX Blockchain Nodes 2.5 s	Data Owner 2.4 s Smart Contract 1 TX Blockchain Nodes 3.1 s

The experimental results of the database setup, addition, and deletion protocols on the three datasets are shown in Table 1. The setup operation takes considerable time and financial cost because of the encryption of a large amount of data and its storage on the blockchain. The number of transactions, time costs, and encrypted database size increase linearly as the number of identifier-keyword pairs increases in the original database. On the side of ITS data owners, most of the time is used in database encryption, i.e., generating $\mathcal{L}$, $\mathcal{L}$, secret keys, and bloom filter. The three databases contain large volumes of data, resulting in a large number of transactions generated. The database setup of the three databases consumes transactions whose numbers are up to 42.3 thousand, 325.1 thousand, and 3.6 million. The blockchain nodes handle the received transactions by local storage, which takes a relatively shorter time. The sizes of databases after encrypted are as large as 532 MB, 4, 084 MB, and 45, 820 MB, respectively.

The addition and deletion operations consume much less time and fewer transactions than the setup operation from the perspectives of both the ITS data owner and the blockchain nodes. For example, in the Enron Email Dataset, each data owner and blockchain node only takes around 1 s on average to complete the operation of addition or deletion. For the large dataset, e.g., the New York City Bus Dataset, such operation is still efficient and takes no more than 4 s on average.

Improved performance of multi-keyword search queries is achieved by using additional data structures. The bloom filter, tag secret key, and tag list are the additional data structures. Achieving this goal requires about half the time, number of transactions, and storage space of the old protocol in comparison to the suggested one. Nevertheless, the proposed approach only influences the database setup operation, making itself acceptable in that the setup protocol will be invoked only once in the whole life cycle of data usage.

4Single-keyword search

Regarding single-keyword search, the time overhead from the perspective of the ITS data owner is low. The reason is that it only precedes a small number of symmetric encryption steps. As far as the blockchain nodes are concerned, they are required to pass through the dictionary *Dori* twice and with a large number of writing operations, incurring relatively high time overhead. We perform experiments on single-keyword searches varying the keywords with different appearance times. The results are shown in Fig. 4. We can see that 5.1 s, 37.5 s, and 86.3 s are needed for the three datasets with no matched identifiers. The search time grows exponentially as the number of identifiers in the query result rises. The single-keyword search times for the three datasets are 14.6 s, 76.92 s, and 140.61 s when there are up to 500 matched identifiers, respectively. Search time per identifier decreases as the number of identifiers in the results increases. This is because an increase in the number of identifiers might lead to a decrease in the average time overhead required to traverse the dictionary. In particular, when there are 500 matched identifiers, the search times per identifier are lower than 0.4 s for all three datasets.

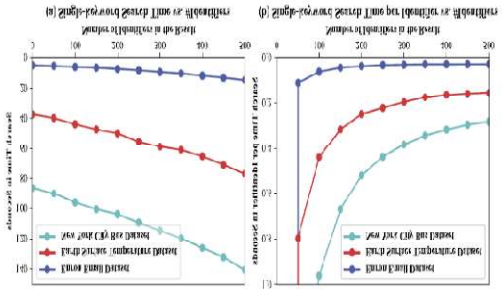

Figure 4: Experimental Results Of The Single-Keyword Search. (A) The Search Time With Increasing Identifiers In The Results. (B) The Search Time Per Identifier With Increasing Identifiers In The Results.

5.2 Local Opinions for Ordering Services

Suppose a peer (Vi) and an ordering service (RUj) interact with each other. The vector defined for the local opinion of Vi to RUj is $\omega_{i\to j}$:= $b_{i\to j}$, $d_{i\to j}$, $u_{i\to j}$, $k_{i\to j}$ where $b_{i\to j}$ represents trust, di j represents mistrust, ui j represents uncertainty, and ki j is a constant which shows a willingness to trust ordering services and is less than 1 (0.5). The values of $b_{i\to j}$, $d_{i\to j}$, and $u_{i\to j}$, in addition to the relationships between them, are particularly important. Hence, $b_{i\to j}$, $d_{i\to j}$, $u_{i\to j} \in \{0,1\}$, $b_{i\to j} + d_{i\to j} + q_{i\to j} = 1$.

$$u_{i\to j} = 1 - q_{i\to j}$$

$$b_{i\to j} = (1- u_{i\to j})\ \alpha\iota / \alpha\iota + \beta$$

$$d_{i\to j} = (1- u_{i\to j})\ \beta\iota / \alpha\iota + \beta\iota$$

αι and βι are the number of good and bad experiences, respectively. qi→j is the communication quality of a link between vehicle i and RSUj. The reputation according to ωi→j xi→j denotes the expected trust of vehicle Vi that RSU is trustworthy and behaves appropriately throughout a consensus period, represented as xi→j = bi→j + kiβjui→j.

5.3 Multi-Weight Local Opinions for Subjective Logic

Different dynamics affect local opinions by utilizing the subjective logic model [26]. Both reputation logics are handled similarly in standard subject logic. However, different reputation logic originating from different sources must be weighted correctly to be aggregated with greater precision. If the vehicle has existing experience of and maintains more recent ratings for, the RSU, the accuracy of the reputation will be significantly improved. Regarding weighing operations, this model progresses into "multi-weight subjective logic".We use the following weights.

5.4 Rate of Experiences

The rate of experience shows how much the vehicle knows about RSU. If the rate of experience is large, it indicates that the vehicle (VA) knows a significant amount about RSUj. The ratio of the number of times that vehicle (VA) communicates with RSU (RSUj) to the total amount of times that the vehicle communicates with other RSUs during some time 'T' is the rate of experiences between them.

$$f_{i\to j} = M_{i\to j} / M_i$$

Where $M_{i+j} = (\alpha\iota + \beta\iota)$, and $M_i = 1 /|Q|\sum M_{i\ q}$. Q is the ordering service (group of RSUs) interacting with vehicle Vi during the time window. A high rate of experience indicates a high reputation value.

5.5 Recent Experiences

Due to inadequate security, widely distributed RSUs might be susceptible to breaches, and IoV gives greater weight to more recent experiences, which does not guarantee that they are trustworthy and safe. There is a constant flux in Vi's credibility and standing in Ruj's eyes. For local opinions, recent and past experiences have different weights. The parameters *g* and *d* indicate the weights of recent and past experiences, respectively. $\gamma + \delta = 1$, whereas $\gamma > \delta$.

System overview of the blockchain-based ITS data-sharing system. On the one hand, autonomous vehicles enjoy privacy-preserving and efficient data-sharing services by sending the encrypted data and operations to and receiving encrypted query results from the roadside infrastructure. We design privacy-preserving and efficient protocols based on the security model to fulfill the four actions described in the following algorithm.

6. CONCLUSION

In this research, we introduced a hard security solution, i.e., the improved Hyperledger Fabric, to implement a blockchain-enabled IoV for safe vehicle information sharing. This research comprehensively highlighted the issues related to IoV. The literature review concluded that most of the security services can be achieved by the implementation of blockchain. An

upgraded Hyperledger Fabric-based solution was proposed in this study to improve the security and privacy of blockchain-enabled Internet of Vehicles (IoV) systems. This will allow for a more efficient and secure exchange of vehicle information. Our work tackles important problems with the Internet of Things (IoT), such as privacy concerns, inefficient data exchange, and centralized trust dependencies, by using blockchain technology and the permissioned architecture of Hyperledger Fabric.

Problems with centralization, scalability, and authenticity were among the many shortcomings of conventional ITS data-sharing systems that were brought to light in the study. Using a one-of-a-kind multi-keyword search protocol based on bloom filters and searchable symmetric encryption, it suggested a new decentralized and efficient framework. This method allows for effective data exchange in real time while minimizing computing costs and preserving anonymity. The solution also handles problems like vehicle hijacking and fraudulent communication by supporting dynamic upgrades and ensuring traceability. Tests on actual ITS datasets proved the solution's efficacy in safeguarding ITS data-sharing systems, as well as its scalability and cost-efficiency. By proposing a multi-keyword search protocol via the blockchain for ITS, this study establishes a precedent and emphasizes the revolutionary potential of blockchain technology to provide efficient and secure IoV communication. First, a reputation-based scheme is utilized to calculate the accurate reputation of RSUs. Second, the research presents an anonymous and traceable CPPA approach that can be utilized in a vehicular network. We also evaluated the more effective and scalable performance of the proposed solution to increase the accuracy.

REFERENCES

[1]. Qureshi, K.N.; Bashir, F.; Abdullah, A.H. Provision of Security in Vehicular Ad hoc Networks through An Intelligent Secure Routing Scheme. In Proceedings of the 2017 International Conference on Frontiers of Information Technology (FIT), Islamabad, Pakistan, 18–20 December 2017; pp. 200–205.

[2]. Qureshi, K.N.; Din, S.; Jeon, G.; Piccialli, F. Internet of Vehicles: Key Technologies, Network Model, Solutions and Challenges with Future Aspects. *IEEE Trans. Intell. Transp. Syst.* 2020, *22*, 1777–1786.

[3]. Zhang, C.; Lin, X.; Lu, R.; Ho, P.-H. RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks. In Proceedings of the 2008 IEEE International Conference on Communications, Beijing, China, 19–23 May 2008; pp. 1451–1457.

[4]. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 11–14 December 2017; pp. 557–564.

[5]. Javed, I.T.; Alharbi, F.; Margaria, T.; Crespi, N.; Qureshi, K.N. PETchain: A Blockchain-Based Privacy Enhancing Technology. *IEEE Access* **2021**, *9*, 41129–41143.

[6]. Bonneau, J.; Miller, A.; Clark, J.; Narayanan, A.; Kroll, J.A.; Felten, E.W. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 17–21 May 2015; pp. 104–121.

[7]. Javed, I.T.; Alharbi, F.; Bellaj, B.; Margaria, T.; Crespi, N.; Qureshi, K.N. Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare. *Healthcare* **2021**, *9*, 712.

[8]. He, D.; Zeadally, S.; Xu, B.; Huang, X. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691.

[9]. Azees, M.; Vijayakumar, P.; Deboarh, L.J. EAAP: Efficient anonymous authentication with a conditional privacy-preserving scheme for vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2467–2476.

[10]. Li, J.; Choo, K.-K.R.; Zhang, W.; Kumari, S.; Rodrigues, J.J.; Khan, M.K.; Hogrefe, D. EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-

preserving authentication scheme for vehicular ad hoc networks. *Veh. Commun.* **2018**, *13*,104–113.
[11]. Dorri, A.; Steger, M.; Kanhere, S.S.; Jurdak, R. Blockchain: A distributed solution to automotive security and privacy. *IEEE Commun. Mag.* **2017**, *55*, 119–125.
[12]. Zhang, X.; Li, R.; Cui, B. A security architecture of VANET based on blockchain and mobile edge computing. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 17–19 August2018; pp. 258–259.
[13]. Arora, A.; Yadav, S.K. Blockchain-based security mechanism for internet of vehicles (IoV). In Proceedings of the 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), Jaipur, India, 9–10 May 2018; pp. 26–27.
[14]. Zhang, L.; Luo, M.; Li, J.; Au, M.H.; Choo, K.-K.R.; Chen, T.; Tian, S. Blockchain based secure data sharing system for Internet of vehicles: A position paper. *Veh. Commun.* **2019**, *16*, 85–93.
[15]. Yuan, Y.; Wang, F.-Y. Towards blockchain-based intelligent transportation systems. In Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016; pp. 2663–2668.
[16]. P.S. Almeida, C. Baquero, N. Preguiça, D. Hutchison, Scalable bloom filters, Inf. Process. Lett. 101 (2007) 255–261.
[17]. M. Autili, L. Chen, C. Englund, C. Pompilio, M. Tivoli, Cooperative intelligent transport systems: choreography-based urban traffic coordination, IEEE Trans. Intell. Transp. Syst. 22 (2021) 2088–2099.
[18]. C. Cai, J. Weng, X. Yuan, C. Wang, Enabling reliable keyword search in encrypted decentralized storage with fairness, IEEE Trans. Dependable Secure Comput. 18 (2018) 131–144.
[19]. L. Chen, W.K. Lee, C.C. Chang, K.K.R. Choo, N. Zhang, Blockchain-based searchable encryption for electronic health record sharing, Future Gener. Comput. Syst. 95 (2019) 420–429.
[20]. J. Cui, F. Ouyang, Z. Ying, L. Wei, H. Zhong, Secure and efficient data sharing among vehicles based on consortium blockchain, IEEE Trans. Intell. Transp. Syst. 23 (2022) 8857–8867.
[21]. N. Deepa, Q.V. Pham, D.C. Nguyen, S. Bhattacharya, B. Prabadevi, T.R. Gadekallu, P.K.R. Maddikunta, F. Fang, P.N. Pathirana, A survey on blockchain for big data: approaches, opportunities, and future directions, Future Gener. Comput. Syst. 131 (2022) 209–226.
[22]. M. Dibaei, X. Zheng, Y. Xia, X. Xu, A. Jolfaei, A.K. Bashir, U. Tariq, D. Yu, A.V. Vasilakos, Investigating the prospect of leveraging blockchain and machine
[23]. learning to secure vehicular networks: a survey, IEEE Trans. Intell. Transp. Syst. 23 (2022) 683–700.
[24]. A. Gervais, G.O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, S. Capkun, On the security and performance of proof of work blockchains, in: ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 3–16.
[25]. O. Goldreich, S. Goldwasser, S. Micali, How to construct random functions, J. ACM 33 (1986) 792–807.
[26]. C. Gosman, T. Cornea, C. Dobre, F. Pop, A. Castiglione, Controlling and filtering users data in the intelligent transportation system, Future Gener. Comput. Syst. 78 (2018) 807–816.
[27]. Z. Guan, N. Wang, X. Fan, X. Liu, L. Wu, S. Wan, Achieving secure search over encrypted data for e-commerce: a blockchain approach, ACM Trans. Internet Technol. 21 (2020) 1–17.
[28]. J. Guo, X. Ding, T. Wang, W. Jia, Combinatorial resources auction in decentralized edge-thing systems using blockchain and differential privacy, Inf. Sci. 607 (2022) 211–229.
[29]. V. Hassija, V. Gupta, S. Garg, V. Chamola, Traffic jam probability estimation based on blockchain and deep neural networks, IEEE Trans. Intell. Transp. Syst. 22 (2020) 3919–3928.
[30]. R.W. van der Heijden, S. Dietzel, T. Leinmüller, F. Kargl, Survey on misbehaviour detection in cooperative intelligent transportation systems, IEEE Commun. Surv. Tutor. 21 (2018) 779–811.

[31]. S. Hu, C. Cai, Q. Wang, C. Wang, X. Luo, K. Ren, Searching an encrypted cloud meets blockchain: a decentralized, reliable and fair realization, in: IEEE Conference on Computer Communications, IEEE, 2018, pp. 792–800.