Preserving Privacy and Traceability in Car-sharing Blockchain Based on Attribute Cryptosystem

*Tzu-Hao Chen, Chit-Jie Chew, Jung-San Lee**

Department of Information Engineering and Computer Science, Feng Chia University, Taiwan
wilsonchen.tzuhao@gmail.com, cjie723@gmail.com, leejs@fcu.edu.tw

Abstract

A car-sharing system has been considered the most promising solution for mitigating the waste of natural resources, traffic congestion, and greenhouse gas emission in the city. However, conventional car-sharing method relies on a trusted third party, which is facing the challenge of maximizing the benefits of C2C model and privacy disclosure risk. This work aims to design a brand-new car-sharing version based on blockchain network and attribute-based cryptosystem. The demander and supplier can use the smart contract to share the vehicle without the help of a centralized node; thus, avoiding the collusion manipulation to reach the optimal profit. In particular, even if the vehicle has been damaged, the supplier can trace the responsibility by accessing the order information stored in the blockchain. Security analysis has demonstrated the confirmation of robustness and privacy essentials, while experimental outcomes have shown the satisfactory feasibility of the new method.

Keywords: Attribute-based cryptosystem, Blockchain, Car-sharing, Sharing economy, Vehicular ad-hoc networks

1 Introduction

The explosion development of vehicular ad-hoc networks (VANET) have brought huge convenience for people, making vehicles inseparable from human life. According to the statistics in 2022, there were 1.446 billion vehicles in the world [1]. However, vehicles stay idle at 95% of the time [2], meaning that a vehicle is only used for 1.2 hours a day on average. No doubt that it has contributed parts of resource waste and led to severe environment problems. This could even affect economic growth and damage the surroundings [3]. In order to improve the deteriorating situation, car-sharing services have become a promising solution worldwide [4].

Sharing economy could enhance utilization to lower down the idle capacity, which making the vehicle in a high utilization to the end of lifespan [5]. People can rent vehicles from suppliers and have the convenience without affording the high budget. In addition, it can reduce the number of vehicles in the city, thereby mitigating the traffic congestion and greenhouse gas emission [6]. Moreover, the statistical data on the number of car-sharing users worldwide from 2017 to 2024 is illustrated in Figure 1. The data before 2022 have been gathered from the real world, while the rest are predicted. The total number of demanders has increased from 36 million in 2017 to 48.5 million in 2022, which is explosively risen by 10 million users in 5 years. Subsequently, it is predicted that there will be 56.3 million demanders at the end of 2024 [7]. Also, researchers have offered the statistics in 2019 that the market value of the car-sharing economy has approached 2.5 billion, and this value will reach 9 billion by 2026 [8]. All the statics have indicated that the market value and user numbers of the car-sharing economy rise continually.

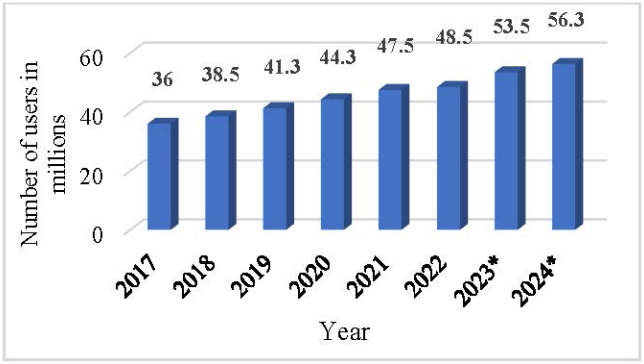


Figure 1. Number of car-sharing users worldwide from 2017 to 2024

Normally, the car-sharing economy could be classified into Business-to-Consumer (B2C) and Consumer-to-Consumer (C2C) [9]. Regarding B2C mode, a demander rents vehicles from car-sharing companies, which is the one-way sharing mode. The current mode can only meet the car demands, but the idleness of vehicles has not been improved [2]. As to the C2C mode, a supplier can share vehicles through the car-sharing platform, demanders can rent the vehicles on the platform through mobile devices to achieve a cycle of sharing economy. Not only the idleness of vehicles can be solved, but also the utilization of vehicles can be increased.

Without loss of generality, traditional C2C car-sharing economy creates a win-win situation for both the supplier and demander. However, security issues have been challenged due to the fact that all personal information and sharing records are kept in a centralized facility [10]. Once the centralized

*Corresponding Author: Jung-San Lee; E-mail: leejs@fcu.edu.tw
DOI: 10.53106/160792642024032502001

server suffers from malicious attacks, the user privacy is no longer safe. Moreover, there is a fairness issue in the centralized car-sharing system. Suppose a dispute occurs, including a car accident or vehicle breakdown. Collusion between server and user might compromise the relevant order information stored in the central node so that the actual driving status is difficult to be tracked. Therefore, a secure decentralized car-sharing system proposed by Kim et al. [9] has effectively addressed collision attacks between malicious users and the centralized platform. However, this system faces challenges in accounting for responsibility when cars are damaged, as there is no mechanism to record the driving status of the vehicle while it is being used by a demander. In case of a dispute, the owner of the vehicle faces difficulty in clarifying responsibility for the accident because there is no evidence to prove whether the damage to the shared vehicle was caused by the customer.

To solve the abovementioned problems, a blockchain-based car-sharing platform (BCSP) has been figured out in this article. A user uploads order information to the blockchain via VANET so that the C2C car-sharing can run smoothly in the new framework without a centralized node. The supplier and demander cooperate to establish a car-sharing smart contract without paying the tax to a centralized platform. Even a dispute happens, the supplier can track the information stored in the blockchain to acquaint the incident. Furthermore, the user privacy could be guaranteed by the attribute-based cryptosystem, in which only qualified users can disclose the location of the car. The followings are the achievement essentials of the new method.

- Data security: BCSP construct a C2C car-sharing system based on blockchain, which guarantees three properties, confidentiality, integrity, and availability. Firstly, the confidentiality means that only the authorized user can access the information stored in the system. Secondly, the integrity is to keep the order information consistent after being transmitted in a public channel. Finally, the feature of availability is to confirm that the system could be available anytime and anywhere.
- Collusion-free: BCSP leverages the distributed consortium blockchain. Thus, specific users cannot collude with the vehicle-sharing platform to tamper with the order information to escape responsibility in an accident or a dispute.
- Tamper-free: All information is stored synchronously in all nodes of BCPS. Therefore, all car-sharing related information shall not be tampered with after being uploaded to the blockchain.
- Traceability: BCSP has designed a driving status information storage mechanism while the sharing car is used. Obviously, vehicle driving statuses could be tracked through the data recorded on the blockchain. It provides the ability to track the car status by the supplier when the car is shared.
- Accountability: Driving status information is signed by the exclusive key of the vehicle, which undoubtedly can not be impersonated by a malicious user. Apparently, driving behavior able to be accountable so that the order information can be used to arbitrate disputes even if the vehicles are damaged.

The rest of the paper is organized as follows. Related backgrounds are introduced in section 2. The detail of BCSP is presented in section 3, followed by the experimental results and analysis in section 4. Finally, conclusions are made in section 5.

2 Related Works

The car-sharing has received much attention, thus, we introduce the research progress of the car-sharing topic in subsection 2.1. In addition, the blockchain has been adopted to build the sharing platform, and the smart contract is used to complete the deal. Thus, we first introduce the techniques of blockchain and smart contract in subsections 2.2.

2.1 Car-sharing

Car-sharing has gained significant attention in recent times, both in the industry and academia. In order to guarantee the security to the user. The privacy of users needs to be protected in the car-sharing platform. In the existing studies [9-10], the privacy of the user has been fulfilled. More precisely, the order information of the user cannot be linked to the user's identity to cause the leakage of user privacy. However, the previous researches [9-10] primarily concentrate on enhancing the efficiency and privacy of the service. However, if the supplier shares the car with others in the platform, they should have the ability to track the driving status of the vehicle when the vehicle is damaged in order to clarify the responsibility of the accident. Thus, traceability and accountability need to be fulfilled. Moreover, the car-sharing platform needs to ensure fairness among users, the car-sharing system needs to address potential issues such as vehicle damage. However, if the system relies on a centralized maintenance party, there is a risk of malicious users bribing the centralized facility to manipulate driving status information to evade responsibility for accidents. Therefore, careful consideration must be given to the design and implementation of the system to mitigate such risks of car-sharing services. Therefore, the collusion-free of users should be guaranteed in the system.

2.2 Blockchain and Smart Contract

Blockchain leverages asymmetric encryption, digital signature, and one-way hash function, which achieves the properties of decentralization, tamper-free, traceability, and transparency [11]. It is a distributed ledger technology maintained by all nodes in the blockchain network. Each block is constructed with the hash value of the previous block, timestamp, merkle root, and nonce. A brief structure is depicted in Figure 2. The timestamp is the time when the block was established, the block header is calculated from the previous block header with hash function SHA256, and the merkle root is generated from the hash values of all previous transaction.

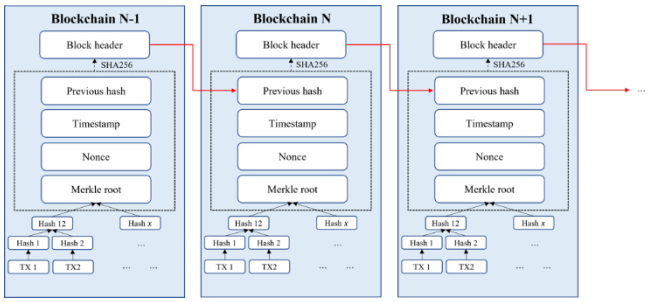


Figure 2. Blockchain structure

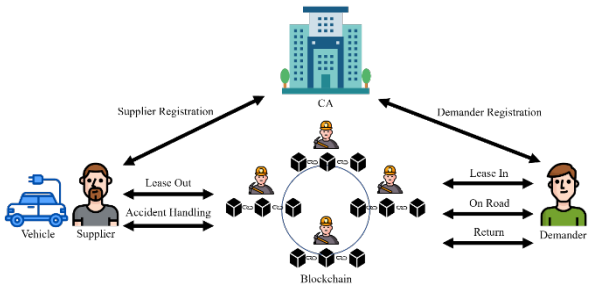


Figure 3. Car-sharing system blockchain framework

The blockchain technique can be organized into three categories, public blockchain, private blockchain, and consortium blockchain [11]. In the public blockchain, all of the members in each node keep ledgers and participate in consensus, which makes the consensus faster but has heavier loading. Besides, all of the nodes in the blockchain can join or leave the blockchain easily without permission. On the other hand, the private blockchain is managed by a private enterprise, and it has centralized characteristics [12].

On the contrary, consortium blockchain is suitable for the car-sharing system, only the member of the alliance can access the information stored in the blockchain, and thus user privacy can be improved. In addition, the consensus efficiency of the consortium blockchain is higher than public blockchain. It accommodates the higher transaction throughput in the car-sharing platform.

The concept of the smart contract is proposed by Szabo [13] in 1997, which is the contract automatically executed without a third party. The smart contract is the code stored in the blockchain, it will trigger via address and specific regulation, such as the values and status of users. When all of the conditions in the smart contract are satisfied, the transaction will automatically execute. For example, the vending machine will automatically supply different beverages when customers press the button and put a dollar in. To reduce the tax while sharing the vehicle in the centralized platform, it is necessary to remove the centralized manager from the system. Thus we leverage smart smarts intending to execute the contract automatically to achieve a decentralized car-sharing platform.

3 Blockchain-based Car-sharing Platform: BCSP

The car-sharing framework is shown in Figure 3. All the suppliers and demanders are the users in our framework. In the beginning, both the supplier and demander have to provide relevant information to the certificate authority (CA) to complete the registration, such as the user e-wallet, driving license, car registration, and identification. Hereafter, suppliers can rent out their vehicles publicly, while demanders can rent the vehicles through the blockchain. Once the demander completes the rental, it returns the right of use to the supplier. If the vehicle is damaged, the order information stored in the blockchain can be used as the basis for the arbitration of disputes. Notations used in the BCSP are defined in Table 1.

Table 1. Notations used in BCSP

Sign	Definition
i	User i-th which i is the supplier S_i, $0 \le i \le n$.
j	User j-th which j is the demander D_j, $0 \le j \le n$.
k	Vehicle k-th, $0 \le k \le n$.
LQ_{role}	Leasing qualification such as rental per hours, mileage fee, region and fraction of $role$.
SK_{role} / PK_{role}	The private/public key of $role$.
$E_{SK_{role}}$ / $D_{PK_{role}}$(.)	The asymmetric encryption and decryption with SK_{role} and PK_{role} in elliptic curve cryptography, respectively.
ID_{role}	The identification of $role$.
DL_{D_j}	The driving license of D_j.
VIN_k	The vehicle identification number of k.
VR_{s_i}	The vehicle registration of S_i, including VIN_k, brand, expiration of the vehicle registration, etc.
DDL_{D_j}	The digital driving license of D_j.
DVR_{S_i}	The digital vehicle registration of S_i.
$address_{role}$	The address of the virtual wallet of $role$.
A_{role}	The access structure in attribute-based encryption of $role$.
APK_{role}/ASK_{role}	The attribute-based public/private key of $role$.

3.1 Registration Phase

In this phase, the supplier vehicle registration and the demander driving license are bound to the corresponding virtual wallet.

3.1.1 Supplier Registration

Supplier S applies to CA for the vehicle and virtual wallet registration. The flowchart of the supplier registration phase is displayed in Figure 4.

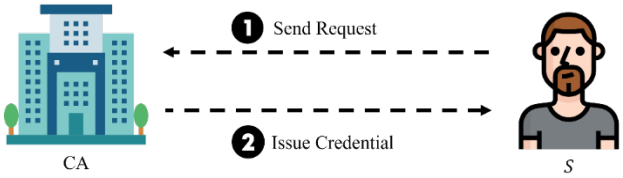


Figure 4. Supplier registration flowchart

Step 1. Send Request: S defines A_S by LQ_S by ciphertext-policy attribute-based encryption [14], then offers VR_S, ID_S, $address_S$, PK_V and A_S to CA through the secure channel.

Step 2. Issue vehicle credential: CA computes and issues the cipher-text policy attribute-based encryption key APK_S and $DVR_S = E_{SK_{CA}}$ ($address_S$, VIN_K) to S.

3.1.2 Demander Registration

Demander D registers the driving license and virtual wallet to CA. The flowchart of the demander registration phase is shown in Figure 5.

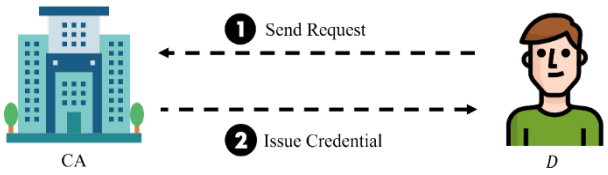


Figure 5. Demander registration flowchart

Step 1. Send Request: D provides DL_D, $address_D$, and LQ_D to CA based on the secure channel.

Step 2. Issue Credential: CA generates and sends the cipher-text policy attribute-based decryption key ASK_D and $DDL_D = E_{SK_{CA}}(address_D)$ to D.

3.2 Lease-out Phase

Lease-out phase is for the supplier to publish the rental contract to the blockchain. The supplier checks the rule block and creates a rental contract, which is verified by the miners and published in the blockchain. The flowchart of the lease-out phase is shown in Figure 6.

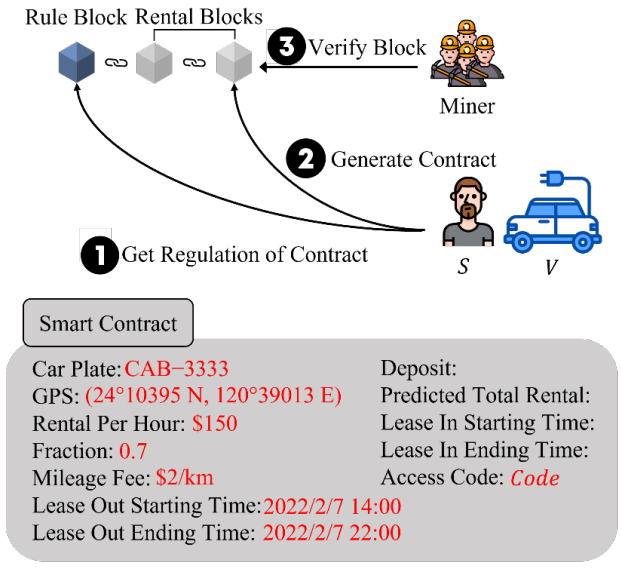


Figure 6. Lease-out phase flowchart

Step 1. Get regulation of contract: S acquires the rule of blockchain and completes the required information of the rental block for the formulation of the smart contract. The smart contract table is displayed as Figure 7.

Step 2. Generate contract: S defines A by GPS, rental fee, mileage fee, lease out starting time, and lease out ending time. Then it encrypts the rental information $CLO_S = E_{APK_S}(LO_S)$ by ciphertext-policy attribute-based encryption [14]. Later, S signs E_{SK_S} (DVR_S, CLO_S) and publishes $M_1 = (E_{SK_S}$ (DVR_S, CLO_S), DVR_S, CLO_S, $address_S$, VIN_k) to the blockchain. Afterward, the V_j updates the access code and stores it in the memory.

Step 3. Verify block: Miners verify whether the rental information CLO_S complies with the rule block and verifies if S is eligible for leasing out the vehicle by DVR_S. Finally, the contract is published in the blockchain.

3.3 Lease-in Phase

The lease-in phase is for the demander who has transportation requirement. The flowchart of the lease-in phase is shown in Figure 7.

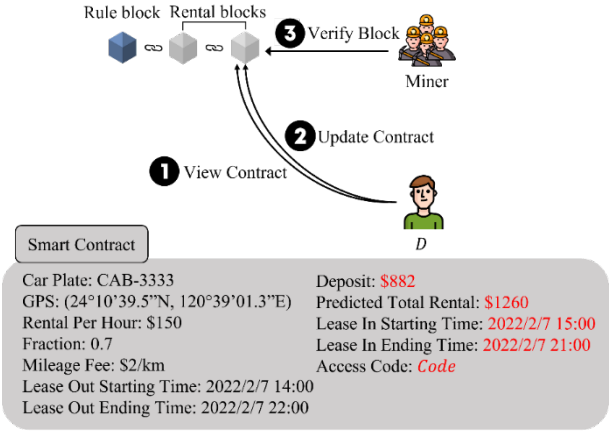


Figure 7. Lease-in phase flowchart

Step 1. View contract: D views the rental information broadcasted on the car-sharing blockchain.

Step 2. Update contract: D decrypts $LO_S = D_{ASK_D}(CLO_S)$ to retrieve the vehicle access code. Later, D completes the rental information LI_D including lease-in starting time and ending time. After that, D signs $E_{SK_D}(DDL_D, LI_D)$ and publishes $M_2 = (E_{SK_D}(DDL_D, LI_D), DDL_D, LI_D, address_D)$ to the car-sharing blockchain. Afterward, the V gets the DDL_D and stores it in memory for the use of identity connection with D.

Step 3. Verify block: Miners verify whether the rental information LI_D complies with the rule block and verifies if D is eligible for leasing the vehicle. Then, the contract is published in the car-sharing blockchain with the deposit detaining.

3.4 On-road Phase

The relevant vehicle information is uploaded to the blockchain every t seconds through the mobile phone of the demander, where the vehicle information is generated by the vehicle, such as GPS, vehicle speed, battery temperature, and sensing information [15]. We take 3 seconds as the example of t. The flowchart of the on-road phase is shown in Figure 8.

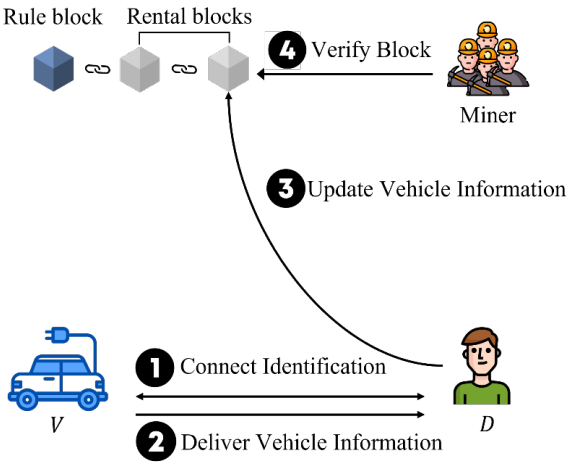


Figure 8. On-road phase flowchart

Step 1. Connect identification: V verifies the identity of D in the first time connected with D by DDL_D.

Step 2. Deliver vehicle information: V captures the vehicle information CI and signs it as $(E_{SK_V}(DDL_D, CI)$, by HSM chip [16]. It then delivers $M_3 = (E_{SK_V}(DDL_D, CI)$, $DDL_D, CI)$ to the driver D.

Step 3. Update vehicle information: D signs $(E_{SK_D}(M_3)$ and uploads $M_4 = (E_{SK_D}(M_3), DDL_D, CI)$ to the blockchain.

Step 4. Verify block: Miners verify the vehicle information CI and the identity of D by DDL_D. Then, the contract is updated to the blockchain.

3.5 Return Phase

After the demander finishes the rental, the demander updates the vehicle information to the blockchain. The contract calculates the price or returns the deposit. At the same time, the demander returns the right to use the vehicle to the supplier. The return phase is shown in Figure 9.

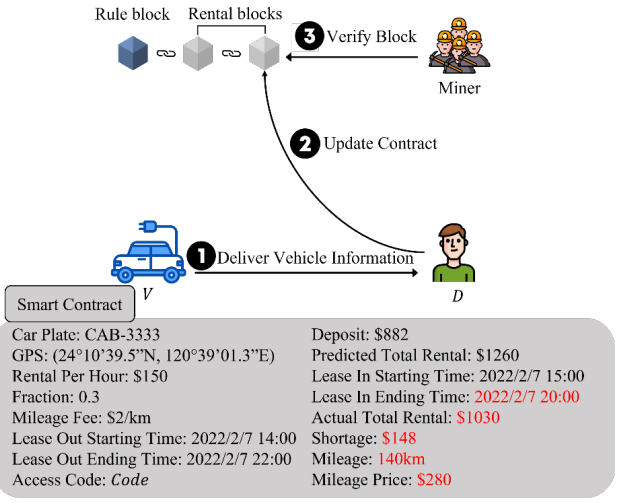


Figure 9. Return phase flowchart

Step 1. Deliver vehicle information: V captures the vehicle information RI_D. Then delivers $M_4 = (E_{SK_V}(DDL_D, RI_D), DDL_D, RI_D)$, DDL_D, RI_D is signed by SK_v to the driver D.

Step 2. Update contract: D signs $M_5 = (E_{SK_D}(M_4)$ then publishes (M_5, DDL_D, RI_D) to the car-sharing blockchain.

Step 3. Verify block: The miners verify the return information RI_D and ID_D. Then, the contract is updated to the car-sharing blockchain.

3.6 Accident Handling Phase

In the accident handling phase, when the vehicle is damaged, S requests D to check CI stored in the car-sharing blockchain. The CI stored in the blockchain can be used as the basis for the arbitration of disputes. The CI contains the speed, battery temperature, and sensor information of the V, which can be checked if D is driving improperly at the time of the accident. The schematic is shown in Figure 10.

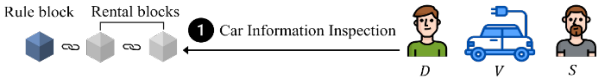


Figure 10. Accident handling phase schematic

4 Experimental Results

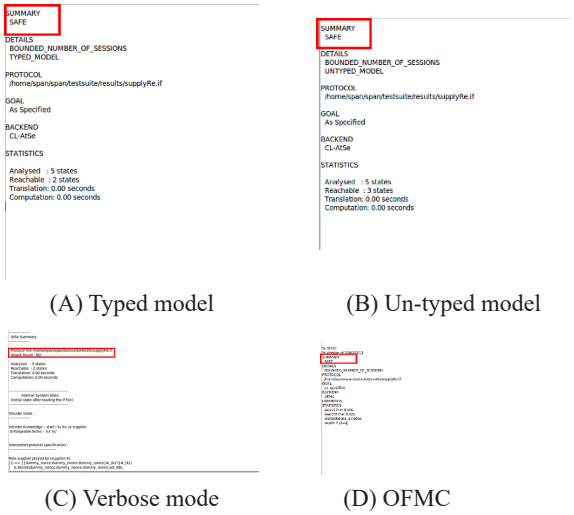
The security of BCSP is analyzed by the Automated Validation of Internet Security Protocol and Application (AVISPA) [17] in subsection 4.1, the performance and achievement are discussed in subsection 4.2, while the computational cost is displayed in subsection 4.3. The simulation environment is executed on a personal computer running Windows 10 64-bit with Python language. It is equipped with an Intel i7-12700 with 32 GB RAM.

4.1 Formal Proof Analysis

Here, the famous verification tool AVISPA [17] has been adopted to ensure the security of the protocol. The version of the AVISPA is simulated by Security Protocol Animator version 1.6 (SPAN 1.6) on Ubuntu10.10-light.

AVISPA [17] uses the High Level Protocol Specification Language (HLPSL) for protocol security analysis and divides the protocol into the environment, role, session, and goal. The environment complies with the transmission environment in Subsections 3.1 to 3.6, and the role corresponds to the supplier, the demander, the CA, and the blockchain. In the security analysis, AVISPA simulates the replay attack, user impersonation attack, and server spoofing attack through different security modules to determine whether the protocol satisfies the verification. Without loss of generality, two modules are used in BCSP verification, namely Constraint-Logic-based Attacker Searcher (CL-AtSe) and On-the-Fly-Model-Checker (OFMC). CL-AtSe analyzes the deniability and verification of the protocol in a limited session [18]. The modularity design only allows easy integration of operator properties, such as exclusive-or and exponentiation [19]. More precisely, CL-AtSe includes the Typed model using all parameters, the Untyped model using generic parameters, and the Verbose mode for a detailed description of possible attacks. On the other hand, OFMC is the one for analyzing security protocols based on a lazy, demand-driven search. As a result of the lazy intruder technique, all the attacks would

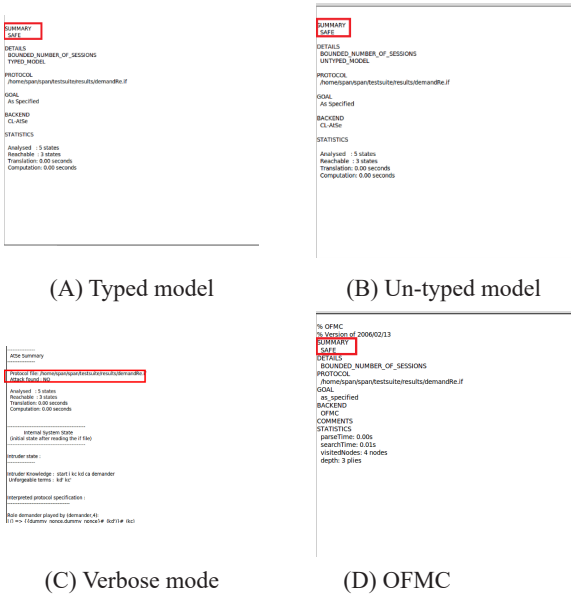
be found. Moreover, the constraint differentiation technique is a general search technique that could reduce the search time of the analysis [18]. According to the result shown in Figure 11 (A-D) to Figure 16 (A-D), the protocol security at each phase can been verified separately. These figures show the test results in different verification models, namely the Typed model, Un-typed model, Verbose mode, and OFMC model. The red frame part in the figures represents whether the test results are secure or not. Obviously, all the results guarantee the security of the protocol in each phase. In other words, the car-sharing blockchain is able to against man-in-the-middle attacks, replay attacks, and type-flaw attacks.



(A) Typed model (B) Un-typed model

(C) Verbose mode (D) OFMC

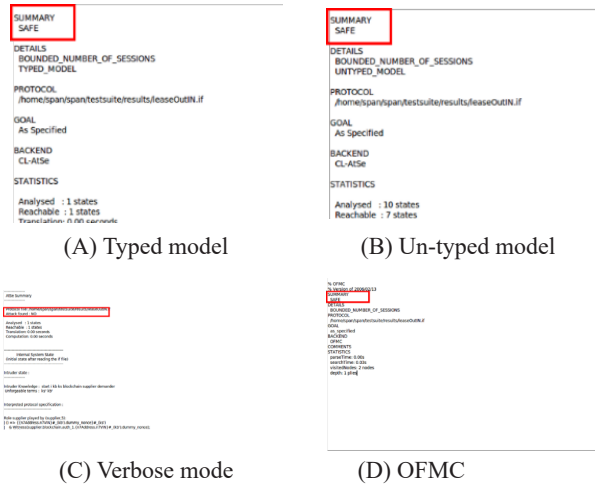
Figure 11. The result of security analysis in the supplier registration phase



(A) Typed model (B) Un-typed model

(C) Verbose mode (D) OFMC

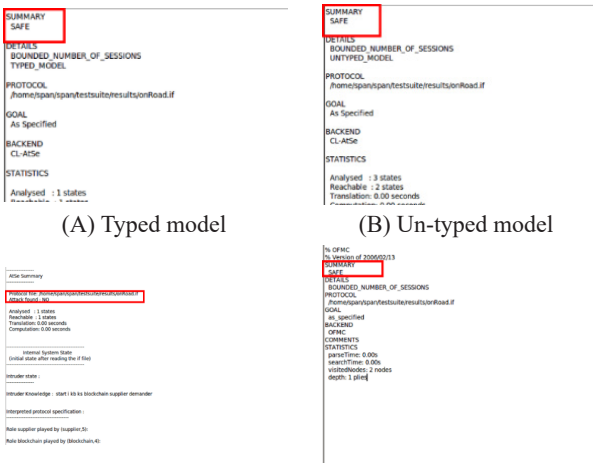
Figure 12. The result of security analysis in the demander registration phase



(A) Typed model (B) Un-typed model

(C) Verbose mode (D) OFMC

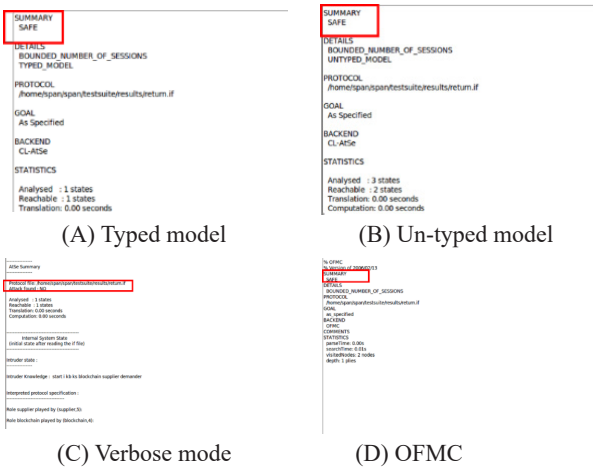
Figure 13. The result of security analysis in the lease in and lease out phase



(A) Typed model (B) Un-typed model

(C) Verbose mode (D) OFMC

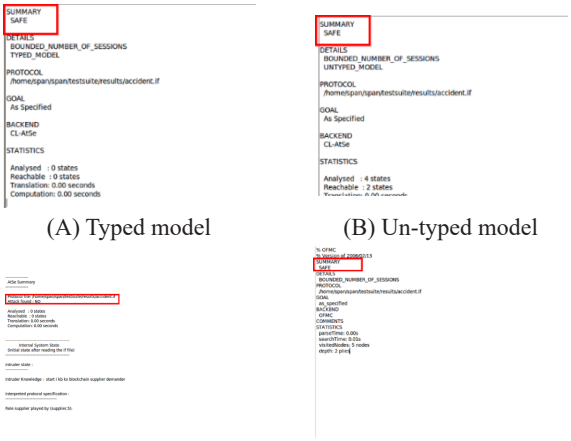
Figure 14. The result of security analysis in the on-road phase



(A) Typed model (B) Un-typed model

(C) Verbose mode (D) OFMC

Figure 15. The result of security analysis in the return phase



(A) Typed model (B) Un-typed model

(C) Verbose mode (D) OFMC

Figure 16. The result of security analysis in the accident handling phase

4.2 Performance and Achievement

To highlight the contribution, a centralized car-sharing system [10] is compared with BCSP to emphasize the obstacles faced by the traditional car-sharing system. Moreover, a decentralized car-sharing system [9] adopting blockchain is involved in the comparison to point up the outstanding effect. The performance comparisons are depicted in Table 2.

Table 2. Performance comparisons

Feature \ Type		[10]	[9]	Ours
Data security	Confidentiality	V	V	V
	Integrity	V	V	V
	Availability	X	V	V
Collusion-free		X	V	V
Tamper-free		X	V	V
Traceability		X	X	V
Accountability		X	X	V

- **Data security**: In order to preserve a secure C2C platform, data security plays an essential role in the car-sharing system. Data security considerations include confidentiality, integrity, and availability.
- **Confidentiality**: Confidentiality means that unauthorized users cannot access driving information to hazard user privacy. In the centralized car-sharing system [10], data transmission between PD-KSApp, KS-OBU, and KSMS is protected based on an asymmetric cryptosystem, thus, [10] achieves confidentiality. In the decentralized car-sharing system [9], the user information is encrypted by ECDH keys, therefore fulfilling confidentiality.

  As to BCSP, the secure channel is leveraged while the user registers at the car-sharing qualification with CA, which ensures the fact that the user sensitive information is not exposed. In addition, each phase of the driving information is stored in the consortium blockchain. Therefore, BCSP can guarantee that only authorized agencies can access sensitive information. Besides, the supplier needs to expose the vehicle information to share the car with the demander in the car-sharing system, thus jeopardizing user privacy. However, the system leverages the attribute-based cryptosystem to preserve the order information to confirm the privacy of the user. Moreover, ID_{role} is bound with the $address_{role}$. Although the malicious user may camouflage as an authorized agency, they have to face the difficulty of knowing the true ID_{role} of the user through massive data analysis. Since malicious attackers cannot directly link the with the ID_{role} of the user, the new framework can ensure the confidentiality of the user.
- **Integrity**: Integrity refers to the consistency between the demander and blockchain after transmitting order information. In the centralized car-sharing system and decentralized car-sharing system [9-10], the transmission of the message is operated by the hash function. Therefore, the user can verify the integrity of information.

  In BCSP, the order information is secured based on asymmetric encryption. All data are signed with the sender private key, and the complete information is sent simultaneously. After the receiver obtains the message, he/she decrypts it with the sender public key to check the consistency of the message. The integrity of each phase is examined as below.

  In the lease-out phase, miners verify the ID_S. If $D_{PK_S}(E_{SK_S}(DVR_S, CLO_S))? = (DVR_S, CLO_S)$ and $D_{PK_{CA}}(DVR_S)\ ? = address_S, VIN_k$ hold, it means that the lease-out information is secured. It is due to the fact that the only supplier S has his/her own private key SK_S to achieve the integrity checking.

  In the lease-in phase, miners verify the ID_D. In case that $D_{PK_D}(E_{SK_D}(DDL_D, LI_D))? = (DDL_D, LI_D)$ and $D_{PK_{CA}}(DDL_D)\ ? = address_D$ hold, it means that the lease in information is secured, in which the main basis is the same as the return phase. The miners verify the return information RI_D and the ID_D. If $D_{PK_D}(E_{SK_D}(DDL_D, RI_D))? = (DDL_D, RI_D)$ holds, the lease-in and return phases have the ability to achieve integrity due to the fact that only the legal demander D has his/her own private key SK_D. Hence, the data integrity of BCSP can be guaranteed.
- **Availability**: Availability refers to the car-sharing system that shall no longer be bounded by space, time, and scale [20]. That is the BCSP shall ensure that its service is always available to the user. In the centralized car-sharing system [10], the service might be interrupted if the centralized node suffers from a single point of failure by a malicious attacker, such as DoS and DDoS attacks [21]. In the decentralized car-sharing system [9], the system is designed using blockchain to store the service information. Moreover, the stations maintain the blockchain by acting as a blockchain node, which can avoid the system from encountering the single point of failure. Thus, the system achieves availability.

  As to BCSP, we leverage the consortium blockchain to prevent the single point of failure. The vehicle and roadside unit contribute computing

power to maintain the car-sharing blockchain. Even if a single node has been compromised, services can be provided generally. Except for more than 51% of node abnormalities, the system will not be broken down. In fact, it is difficult to disrupt 51% of the user because of the characteristic of the blockchain. Thus, the BCSP is able to achieve the availability.

- **Collusion-free**: The meaning of collusion-free indicates that no one can collude with the system, thereby affecting overall fairness. In the centralized car-sharing system [10], a centralized management architecture has been adopted. In the aspect of users, they can bribe the system to adjust their reputation values to increase the willingness of other users to rent vehicles, which raising the probability of a collusion attack. In the decentralized car-sharing system [9], the system is designed by the distributed storage structure, which is blockchain. Therefore, the system can avoid such collusion because the malicious user cannot bribe the car-sharing service provider to tamper with the service information.

  Regarding BCSP, we leverage the distributed consortium blockchain. Users can establish a car-sharing smart contract without the centralized platform, thus maximizin g the benefit between the supplier and demander. Since the car-sharing blockchain is maintained by the users in the car-sharing system, all of the transactions need to go through the consensus mechanism. Any modification to the information stored in the car-sharing blockchain will be found out immediately. Therefore, there is no collusion issue in BCSP.
- **Tamper-free**: Tamper-free refers to the order information not being tampered with by malicious users after being uploaded. In a centralized car-sharing system [10], the authorized agency can easily tamper with the user reputation value stored in the system. Moreover, the order information stored in the system might be tampered with by malicious attackers once the system has been intruded. If the vehicle is damaged, there is no reliable order information to prove the arbitration of disputes. In the decentralized car-sharing system [9], the system relies on the blockchain. Consequently, the tamper-free feature of the blockchain ensures the service information is not tampering. Therefore, the system can fulfill the tamper-free essential.

  Concerning BCSP, the order information is recorded in the blockchain. Suppose a malicious attacker attempts to tamper with the information in the blockchain, the attacker has to face the consensus characteristic, which is inherited from the blockchain kernel. Consequently, the order information will not be tampered with by the attacker.
- **Traceability**: Owing to the supplier sharing the vehicle with unknown users, it is indispensable to provide a mechanism to track the status of the vehicle. In the centralized and decentralized car-sharing system [9], vehicle information is not recorded. It is difficult to track the status of the vehicle, which leading to reduce the supplier willingness to lease out the vehicle.

  As to BCSP, the vehicle information has been uploaded to the blockchain regularly. The supplier can easily track the status of the vehicle by retrieving the information stored in the car-sharing blockchain. Hence, the car-sharing blockchain is capable of preserving traceability.
- **Accountability**: Accountability refers to all of the transactions and driving behaviors have to be accountable. In the centralized and decentralized car-sharing system [9, 10], the driving status is not recorded. Thus, there is no information to determine whether the user driving behavior or the vehicle itself has a problem. Therefore, both systems cannot achieve the accountability.

  In case of a vehicle damage happening to the BCSP, it is necessary to investigate whether the responsibility lies with the demander or the vehicle itself. In this case, the vehicle information is signed by the security chip HSM [16] of the vehicle and uploaded to the car-sharing blockchain. Hence, the behavior of the demander and vehicle status can be accounted.

4.3 Computational Cost

In order to emphasize the practicability of BCSP, the evaluation of the computational overheads in supplier registration, demander registration, lease-in, lease-out, on-road, return, and accident handling phases are demonstrated in this section.

All the execution time of operations are shown in Table 3. T_{KeyGen} is the time cost of attribute-based key generation, $T_{E_{APK_{Role}}}$ represents attribute-based encryption, $T_{D_{ASK_{Role}}}$ stands for attribute-based decryption, $T_{E_{SK_{Role}}}$ shows the encryption time with SK_{Role} in elliptic curve digital signature algorithm, and $T_{D_{PK_{Role}}}$ represents the decryption time with PK_{Role} in elliptic curve digital signature algorithm. The execution time of each phase is shown in Table 4.

Table 3. Execution time

T_{KeyGen}	$T_{E_{APK_{Role}}}$	$T_{D_{ASK_{Role}}}$	$T_{E_{SK_{Role}}}$	$T_{D_{PK_{Role}}}$
49.881ms	28.484ms	13.866ms	1.024ms	0.996ms

Table 4. Execution time of each phase

Phase	Cost
Supplier registration	50.905ms
Demander registration	50.905ms
Lease-out	31.500ms
Lease-in	16.902ms
On-road	5.036ms
Return	4.040ms
Accident handling	2.048ms

In the beginning, the attribute-based key generation and elliptic curve digital algorithm encryption are performed in the supplier and demander registration phase, which costing $T_{KeyGen} + T_{E_{SK_{Role}}} = 50.905$ms. The time cost of the registration phase is acceptable for users to register for the qualification. As to the lease-out phase, the supplier needs to execute attribute-based encryption in order to keep the lease-out information private and sign the information with elliptic curve digital algorithm encryption. Moreover, the miners need to verify the digital signature of lease-out information and supplier qualification, which using two elliptic curve digital algorithm decryptions, leading to the cost of $T_{E_{APK_{Role}}} + T_{E_{SK_{Role}}} + 2 \times T_{D_{PK_{Role}}} = 31.500$ms. After the lease-out phase, the demander executes the lease-in phase to rent the vehicle. Thus, the demander needs to perform attribute-based decryption to retrieve the lease-out information. Afterward, the demander signs the information with elliptic curve digital algorithm encryption, while the miners need to verify the digital signature of lease-in information and demander qualification using two elliptic curve digital algorithm decryptions. Totally, it requires $T_{D_{ASK_{Role}}} + T_{E_{SK_{Role}}} + 2 \times T_{D_{PK_{Role}}} = 16.902$ms. In summary, the lease-out and lease-in phases only takes $T_{E_{APK_{Role}}} + T_{D_{ASK_{Role}}} + 2 \times T_{E_{SK_{Role}}} + 4 \times T_{D_{PK_{Role}}} = 48.402$ms, which is efficient to complete a car-sharing.

In the on-road phase, the vehicle needs to upload the vehicle information to the blockchain and sign the vehicle information with elliptic curve digital algorithm encryption. After transferring the information to the demander, the miners verify the signature and demander qualification, which taking $2 \times T_{E_{SK_{Role}}} + 3 \times T_{D_{PK_{Role}}} = 5.036$ms. As the vehicle needs to upload the relevant vehicle information every three minutes during the simulation, in which the period is insignificant compared to 5.036ms. This has implied that the car-sharing blockchain has enough time to record the driving status of the vehicle to protect the right of both suppliers and demanders. Regarding the return phase, the vehicle has to upload the return information to the blockchain and sign the return information with elliptic curve digital algorithm encryption. Subsequently, the miners verify the signature and demander qualification, in which it costs $2 \times T_{E_{SK_{Role}}} + 2 \times T_{D_{PK_{Role}}} = 4.040$ms. Obviously, the execution time cost is quite efficient.

In case of the vehicle being damaged, the supplier asks to execute the accident handling phase. It spends two elliptic curve digital algorithm decryptions to verify the vehicle information, which taking $2 \times T_{D_{PK_{Role}}} = 0.996$ms. Totally, it requires 161.336ms to finish a BCSP play, which is explaining that the car-sharing blockchain is an efficient system as the forward-looking traffic pattern in the future.

5 Conclusions

A blockchain-based platform, BCSP, has been laid out to achieve comprehensive car-sharing economy. A smart contract is used to avoid the collusion manipulation to reach the optimal profit among users. Specifically, the supplier can trace the responsibility by accessing the order information stored in the blockchain if a shared vehicle has been damaged. This can enhance the willingness of platform participation. Security analysis has demonstrated the confirmation of robustness and privacy essentials, while experimental outcomes have shown the satisfactory feasibility of BCSP.

References

[1] Pd.com.au, How Many Cars Are There in The World?, R Package Version 2.0-12, April, 2022.

[2] D. Shoup, The High Cost of Free Parking, *Journal of Planning Education and Research*, Vol. 17, No. 1, pp. 3-20, Fall, 1997.

[3] A. Dabbous, A. Tarhini, Does Sharing Economy Promote Sustainable Economic Development and Energy Efficiency? Evidence from OECD Countries, *Journal of Innovation & Knowledge*, Vol. 6, No. 1, pp. 58-68, January-March, 2021.

[4] M. Ritter, H. Schanz, The Sharing Economy: A Comprehensive Business Model Framework, *Journal of Cleaner Production*, Vol. 213, pp. 320-331, March, 2019.

[5] D. Demailly, A. S. Novel, The Sharing Economy: Make it Sustainable, *IDDRI Study*, pp. 1-30, July, 2014.

[6] Q. H. Zhou, Z. Yang, K. Zhang, K. Zheng, J. Liu, A Decentralized Car-sharing Control Scheme based on Smart Contract in Internet-of-vehicles, *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, Antwerp, Belgium, 2020, pp. 1-5.

[7] Statista Research *Department, Car-sharing - Worldwide*, December, 2022.

[8] Global Market Insight, *Car Sharing Market Size by Model (P2P Station-based Free-floating) by Business Model (Round Trip One Way) by Application (Business Private) Industry Analysis Report Regional Outlook Application Potential Price Trend Competitive Market Share & Forecast 2020-2026*, July, 2021.

[9] M. H. Kim, J. Y. Lee, K. S. Park, Y. H. Park, K. H. Park, Y. H. Park, Design of Secure Decentralized Car-sharing System using Blockchain, *IEEE Access*, Vol. 9, pp. 54796-54810, April, 2021.

[10] I. Symeonidis, M. A. Mustafa, B. Preneel, Keyless Car Sharing System: A Security and Privacy Analysis, *2016 IEEE International Smart Cities Conference (ISC2)*, Trento, Italy, 2016, pp. 1-7.

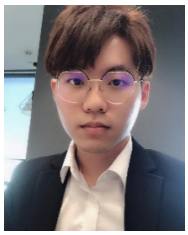
[11] Z. B. Zheng, S. A. Xie, H. N. Dai, X. P. Chen, H. M. Wang, Blockchain Challenges and Opportunities: A Survey, *International Journal of Web and Grid Services*, Vol. 14, No. 4, pp. 352-375, October, 2018.

[12] S. H. Son, J. Y. Lee, M. H. Kim, A. K. Das, Y. H. Park, Design of Secure Authentication Protocol for Cloud-assisted Telecare Medical Information System using Blockchain, *IEEE Access*, Vol. 8, pp. 192177-192191, October, 2020.

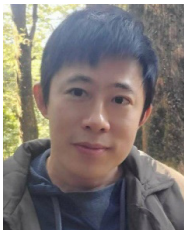
[13] D. Magazzeni, P. McBurney, W. Nash, Validation and Verification of Smart Contracts: A Research Agenda, *Computer*, Vol. 50, No. 9, pp. 50-57, September, 2017.
[14] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy Attribute-based Encryption, *2007 IEEE Symposium on Security and Privacy (SP '07)*, Berkeley, CA, USA, 2007, pp. 321-334.
[15] H. Vdovic, J. Babic, V. Podobnik, Automotive Software in Connected and Autonomous Electric Vehicles: A Review, *IEEE Access*, Vol. 7, pp. 166365-166379, November, 2019.
[16] M. Wolf, T. Gendrullis, Design, Implementation, and Evaluation of a Vehicular Hardware Security Module, in: H. Kim (Ed.), *Information Security and Cryptology - ICISC 2011*, *Vol. 7259*, Springer, Berlin, Heidelberg, 2012, pp. 302-318.
[17] European Community under the Information Society Technologies Proframme, *Deliverable D2.1: The High Level Protocol Specification Language*, Automated Validation of Internet Security Protocols and Applications, August, 2003.
[18] L. Viganò, Automated Security Protocol Analysis with the AVISPA Tool, *Electronic Notes in Theoretical Computer Science*, Vol. 155, pp. 61-86, May, 2006.
[19] M. Turuani, The CL-Atse Protocol Analyser, in: F. Pfenning (Ed.), *Term Rewriting and Applications RTA 2006, Vol. 4098*, Springer, Berlin, Heidelberg, 2006, pp. 277-286.
[20] J. S. Lee. K. S. Lin, An Innovative Electronic Group-buying System for Mobile Commerce, *Electronic Commerce Research and Applications*, Vol. 12, No. 1, pp. 1-13, January-February, 2013.
[21] T. Peng, C. Leckie, K. Ramamohanarao, Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems, *ACM Computing Surveys*, Vol. 39, No. 1, pp. 1-42, April, 2007.

Biographies

Tzu-Hao Chen is pursuing his MS degree in information engineering and computer science in Feng Chia University, Taichung, Taiwan. His current research interests include network security and blockchain applications.



Chit-Jie Chew is pursuing his PhD degree in information engineering and computer science in Feng Chia University, Taichung, Taiwan. His current research interests include information security and blockchain applications.



Jung-San Lee received his Ph.D. degree in computer science and information engineering in 2008 from National Chung Cheng University, Chiayi, Taiwan. Since 2017, he has worked as a professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. His current research interests include network management, electronic commerce, and blockchain.