Blockchain-Based Outsourcing Shared Car Risk Prediction Scheme Design

Haonan Zhai, Song He, Zeyu Wei, and Yong Xie(✉)

Department of Computer Technology and Applocation,
Qinghai University, Xining 810016, China

Abstract. With the widespread use of shared cars, the security of cars and user data sharing have become increasingly important. To prevent the leakage of data and damage or non-return of shared cars, researchers have put forward many proposals of shared cars. But there are some problems in these schemes such as security, low precision. Therefore, we propose a shared car risk prediction scheme by using support vector machine (SVM) learning and blockchain, homomorphic encryption. First of all, this scheme adopts blockchain technology to ensure that the data can not be tampered with. ln addition, the homomorphic encryption algorithm is used to realize the machine learning calculation in the ciphertext state. Finally, the SVM learning algorithm is used to make the risk prediction results of shared cars more accurate. Through performance analysis and comparison, the scheme is proved to have higher accuracy and security.

Keywords: Support vector machine learning · Blockchain · Homomorphic encryption · Multi-key conversion protocol

1 Introduction

In recent years, with the rise of shared bikes, more and more cities begin to use shared bikes, which means that shared cars will enter our lives right away. Car-sharing is an emerging development direction with brand-new development prospects. The function of car-sharing is to realize the reasonable and effective distribution of vehicle resources and cease the flooding and waste of vehicles. Therefore, the number of private cars and caused problems can be reduced to some extent, such as air pollution, energy shortage, traffic congestion, and parking difficulties can be alleviated. Some questions about shared cars have gradually emerged simultaneously. For example, shared cars will have problems such as not returning them in time after renting, and vehicle damage.

Designing a special scheme combined with machine learning predictive models can improve the car sharing problem. Machine learning prediction can accurately and effectively use the user and vehicle encrypted information in the car-sharing platform to predict the security risks of renting a car, so as to avoid

W. Shi et al. (Eds.): SPNCE 2021, LNICST 423, pp. 1–14, 2022.
https://doi.org/10.1007/978-3-030-96791-8_1

as much as possible the situation where the shared car is damaged or cannot be returned. At present, many machine learning training prediction models have been proposed. Among all machine learning training prediction models, the support vector machine training prediction model can effectively analyze data and make predictions. In this paper, SVM supervised learning method is used to predict the security of car-sharing platform rental by training a predictive model. SVM machine learning has a wide range of applications. In addition to predciting the security of shared cars, it can also be used in smart healthcare, smart cities, and smart grids. The training of the support vector machine learning algorithm model requires the transmission of a large amount of data information. The traditional method is to directly transmit sensitive data information of users and vehicles to a third-party computing party and use support vector machine learning algorithms for model training, which will lead to the leakage and dissemination of private data information of users and vehicles. Therefore, during the transmission process, the privacy protection of the data transmission and training calculation process needs to be improved.

In order to solve the problem of shared cars systems' data privacy protection for users and used vehicles, we urgently need to introduce a scheme that combines privacy protection and blockchain to protect our private data in the shared cars systems. In our scheme, the shared car information and the user's information are encrypted, and then the encrypted data is transmitted and stored. This method can ensure that the personal information of the user and the rented vehicle information data will not be leaked. However, there is a risk of data information leakage during the transmission process, the adversary cannot decrypt the content of the data information after receiving the encrypted data information. In our shared car risk prediction scheme, data information can be encrypted with confidential multiple keys by using the Paillier homomorphic encryption algorithm and multi-key conversion protocol. Computing service provider (CSP) and Cloud platform(CP) adopt a multi-key conversion protocol to convert ciphertext data encrypted by multiple keys into ciphertext encrypted by a unified key. The information analysis and prediction node processes the unified key ciphertext data for SVM learning and calculation.

The immutable and decentralized nature of blockchain is particularly suitable for car-sharing scenarios. We use consortium blockchain storage to ensure that metadata cannot be tampered with in our scheme. Even if the metadata representing the ciphertext data on a blockchain node is modified, the blockchain can also periodically update the synchronized data to make it invalid through the consensus protocol. Not only does the metadata representing the ciphertext data will never be revised, but it can also be traced back to the party that modified the data.

2 Relate of Work

There are many applications of blockchain and privacy protection in domestic and foreign, such as medical treatment and smart grid. Blockchain technology in these applications can solve the problem of improving entity trust and data storage security.

In the field of car-sharing, Viktor Valaštín et al. [1] have used blockchain technology to build a decentralized car-sharing scheme. A decentralized car-sharing service created by blockchain technology ensures data integrity and anonymous identity verification. In terms of the Internet of Vehicles, messages need to be distributed more widely. So the security and privacy of the messages have higher requirements. Lei Zhang et al. [2] have proposed a Blockchain-based secure data sharing scheme that solves the challenges of security and privacy on the internet of vehicles. In terms of data privacy protection based on homomorphic encryption, Parmar PV et al. [3] have published an Overview of different homomorphic encryption algorithms. In our article, we use the Paillier homomorphic encryption algorithm. Shen M et al. [4] have published a smart city based on Paillier homomorphic algorithm, support vector machine (SVM), and blockchain. Wang Ruijin et al. [5] have established a privacy protection program for the internet of vehicles based on homomorphic encryption and blockchain technology. The scheme can achieve private data is distributed, shared, and calculated in the state of ciphertext.

In terms of multi-key conversion protocols, there was the privacy-preserving outsourced support vector machine design for secure drug discovery researched by Liu et al. [9] which realizes privacy protection through the combination of SVM, multi-key conversion protocol, homomorphic encryption.

There are also much researches on data processing SVM machine learning. Among them, Byvatov et al. [6] used the support vector machine (SVM) for the classification of drug and non-drug. Secondly, Lin and Chen [7] have considered solving the privacy problem of the dataset in SVM training and the encryption problem of SVM information for classification. The contributions of this paper:

1. Use the consortium blockchain and SVM machine learning to realize a secure and reliable shared car risk prediction that can try to avoid the damage and long-term borrowing from happening in the shared car application scenario.
2. Solve the problem of privacy in shared car data protection. With the help of blockchain and homomorphic encryption, the confidentiality, immutability, and traceability of data in storage are realized. The plaintext information can not be obtained even if the ciphertext state data is leaked during transmission.
3. The privacy-protected SVM machine prediction scheme uses multi-key conversion protocol and homomorphic encryption technology to implement the SVM model training and prediction calculations while data are all in encrypted status.

This paper introduces related work in Sect. 2; introduces basic knowledge of SVM and blockchain in Sect. 3; Sect. 4 introduces the structure model of the shared car risk prediction scheme and the process of data prediction; Sect. 5 is analysis and comparison; Sect. 6 is a summary.

3 Preliminaries

In this section, we outline the definition of blockchain, Paillier Homomorphic Encryption, SVM, which are the basic in our proposed scheme. Table 1 summarizes the key notations used in this paper.

Table 1. Summary of notations

Notations	Definition
pk_a/sk_a	Party a' public key or private key
$sigk_{KGC}/verk_{KGC}$	Strong unforgeable signature/verification key
$SK^{(1)}/SK^{(2)}$	Partial Strong private key of our scheme
$[x]_{pk_a}/x$	The ciphertext $[x]_{pk_a}$ is the plaintext x encrypted by the public key of a
CET_i/REC_i	Certificate/revocation for domain i
M_{re}	car'/user' node data and authentication in encrypted state
$\overrightarrow{x}, \overrightarrow{w}$	Parameters of SVM
g, N	Group generator, plaintext domain of our scheme

3.1 Blockchain

The blockchain is essentially a distributed database, using p2p communication technology and consensus protocol to allow multiple databases to maintain the same ledger at the same time. So the blockchain data is immutable, decentralized, and secure. Blockchain can be combined with encryption algorithms to make all the nodes invisible to the content of the ledger and realize the confidentiality of the data in the ledger.

Blockchains can be divided into three types: public chains, consortium chains, and private chains.

(1) For public chains, all users can join the blockchain network at any time to maintain or update the ledger, such as Bitcoin and Ethereum.
(2) For the consortium chains, only nodes that have been authenticated can apply to update the blockchain.
(3) For private chains, they are generally used in enterprises and institutions.

The shared car risk prediction scheme designed in this paper adopts the consortium blockchain.

3.2 Paillier Homomorphic Encryption

The Paillier homomorphic encryption algorithm can ensure that the processor does not need to know its corresponding plaintext information, allowing the

processor to process the ciphertext and map the processing to the corresponding plaintext processing. So the ciphertext is processed directly, and the result of the processing after the plaintext is encrypted at the same.

The encryption function defined by Paillier cipher is defined as $E_{pk}(...)$, Paillier cipher system is defined as follows:

$$E_{pk}(m, r) = g^m * r^N \bmod N^2 \tag{1}$$

The above parameter $m \epsilon Z_n$ is the homomorphically encrypted plaintext information, N is the product of two prime numbers p, q. From the above formula, the following additive homomorphic formula and multiplicative homomorphic formula can be derived:

$$E_{pk}(a + b) = E_{pk}(a) * E_{pk}(b) \bmod N^2 \tag{2}$$

$$E_{pk}(a * b) = E_{pk}(a)^b \bmod N^2 \tag{3}$$

3.3 SVM Support Vector Machine Algorithm

The support vector machine algorithm is a machine learning training model of supervised learning. The algorithm classifies data after predicted by calculating the maximum edge hyperplane of the data. The formal formula of the hyperplane: $y = w^T x + b$, and $w^T x + b > 0, y = +1; w^T x + b < 0, y = -1$, the relevant optimizations are as follows:

$$\min_{w,b} \frac{1}{2} \left\| w^2 \right\|, s.t., y_i(w^T x + b) \geq 1, i = 1, 2..., m \tag{4}$$

4 Scheme Mechanism

In this part, we introduce the model design, design goals, and critical steps of the scheme design. In detail, the scheme model in Sect. 4.1, designed goal in Sect. 4.2, the data authentication and key distribution in Sect. 4.3, smart contracts in blockchain in Sect. 4.4, secure multiple-key transform protocol in Sect. 4.5, the request query process analysis in Sect. 4.6.

4.1 Scheme Model

From Fig. 1, we can see the shared car risk prediction scheme model structure designed in this paper. This system model includes an improved IBE cryptographic system that can realize user authentication and signature. There are eight types of entity in the scheme model structure as follows:

Key Generation Center (KGC): KGC is a fully trusted authority whose job is to allocate and manage public and private key pairs and generate keys that can be signed and authenticated.

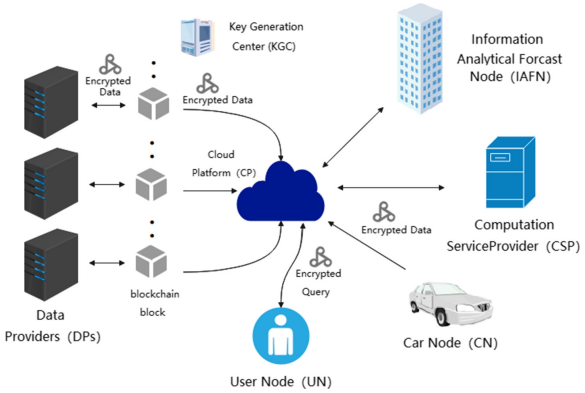

Fig. 1. The model structure of shared car risk prediction scheme

Data providers (DP): Each data provider can be an independent car-sharing platform company and each data provider can be regarded as a blockchain accounting node in the blockchain. The car rental data is encrypted and forwarded to CP is used for storage.

Data Blockchain: The blockchain stores the hash value information of the user node or vehicle node data information in multiple data providers. The data provider plays the role of the blockchain accounting node in the blockchain. Blockchain can invalidate any data provider's tampering with data. Our solution uses the alliance blockchain.

User Node (UN): The user node encrypts the relevant information data of renting a shared car and sends it to CP for storage. Once the user node receives the encrypted data, it can decrypt the result and obtain the prediction result.

Car Node (CN): After the car-sharing node is rented, it encrypts the relevant information data of its car-sharing and sends it to the CP for storage.

Cloud Platform (CP): There is almost unlimited storage space in the cloud platform which can store all the encrypted registered participants' information data in the scheme and perform partial decryption calculations on the ciphertext.

Computing Service Provider (CSP): It can partially decrypt the semi-decrypted information sent by the CP to obtain the information.

Information analytical Forecast Node (IAFN): The information-analytical forecast node is a commercial company that is used to provide security

forecasts for users to rent shared cars. The Information analytical forecast node can predict the security of car rental behavior under the premise of ensuring information security.

4.2 Design Goals

Confidentiality: Homomorphic encryption ensures data is invisible. Data providers, the cloud platform, computing service provider, and information-analytical forecast node are invisible to data. The data of user nodes and shared car nodes are kept in the form of encryption during the transmission process.

Immutable: The hash value of the data of user nodes and shared car nodes will be stored on the data servers of multiple data providers through the blockchain consensus protocol PBFT. The data on blockchain will be shared in the form of blocks and synchronized. Any tampering of the data by the data provider will be invalid.

Synchronization: By using the consensus protocol PBFT of the blockchain, data providers act as blockchain accounting nodes that can update the data synchronously within a certain period of time and make the data more secure and stable on the storage side.

Anonymity: Through the light-node privacy protection identity verification scheme, data providers, cloud platforms, computing service providers, and the information-analytical forecast node can obtain encrypted data of user nodes and shared car nodes. But they cannot track and determine the identity of the user node and the car node.

Predictability: Through the support vector machine learning and prediction on the encrypted user node data and the encrypted shared car node data, the information-analytical forecast node calculate an SVM machine learning model by the encrypted data in CP. The model can predict the rental situation and return situation of the shared car by using the user node data and the shared car node data.

4.3 Certificate Authentication and Key Distribution

Certificate Assignment and Revocation
The improved IBE cryptographic system can enable KGC nodes to authenticate and sign user or car identities. If one participant P (e.g., IAFN) wants synchronously compute some encrypted data from other parties (e.g., DPs). P must get DPi's authorization time (AT) for party P from DPi, then sends the DPi's authorization time (AT) to KGC. KGC will generate

a certificate sequence (CS) for everyone certificate and uses the DPi's authorization time (AT), domain area (DA) to make a new certificate $CET_i = <cet = (CS, DA, DP_i, AT, pk_{DPi}); Sig(cet, sigk_{KGC})>$ or a revocation certificate $REC_i = <rec = (revoke, CS); Sig(cet, sigk_{KGC})>$, then send to CP and CSP for storage.

Key Distribution
To distribute keys in this shared car risk prediction scheme, the KGC generates public parameters $pp = (N, g)$, randomly select $sk_s = \Theta_x \epsilon Z_N$ (include all $x\epsilon\{DP_1, DP_2, \cdots DP_n, UN, CN, IAFN\}$), then computes $Pk_i = g^{\Theta_i} (i = 1, \cdots, n)$, on the same N and g. KGC generates CET_i for DP_i, CET_{UN} for UN, CET_{CN} for CN,CET_{IAFN} for IAFN and sends these authentications to both CP and CSP for storage. KGC also generates and sends the private keys $sk_x = \Theta_x (x = 1, \cdots, n), sk_{UN} = \Theta_{UN}, sk_{CN} = \Theta_{CN}, sk_{IAFN} = \Theta_{IANN}$ to DP_x, UN, CN, IAFN via a secure channel, respectively. KGC sends the verification key $verk_{KGC}$ to both CP and CSP. There is no one external adversary or internal party to decrypt the DP_i's ciphertexts because these parties can not get the corresponding private key sk_x by one way.

4.4 Smart Contracts in Blockchain

Smart Contract of Adding Requesting Data
All the data is divided into two sorts. One is car rental users' information, the other one is cars' information. The data is all in the ciphertext state. The blockchain will use the smart contract to detect whether the data is in requesting forecast state. When the data is sent to CP for forecasting whether the user can lend the car, CP will send hash value of these data to the main data provider node. The main data provider node will obey the adding new message of smart contract, then broadcast the hash value to all the data provider nodes in the blockchain. At last, all the data provider nodes store the hash value and add in the last blockchain's block data segment.

Smart Contract of verifying All Stored Dataset
When the IAFN needs to train the SVM model, it will send a request of needing datasets to CP. CP receives the request and sends the request of verifying all stored datasets to the main data provider node of the blockchain. The main data provider node will use the smart contract of verifying all stored datasets, then the blockchain will send all the hashes to the CP. When the CP verifies that the data corresponds to the hashes, the CP will make some processes in CP and CSP before sending encrypted data to IAFN. The process will be explained in Sect. 4.5.

Smart Contract of Adding Result Data
When the IAFN gets the processed dataset, IAFN will use the homomorphic encryption algorithm and corresponding requesting information to complete prediction result P of request lending sharing car. The prediction result will be encrypted by authorized public key pk_B, then IAFN will send the encrypted

prediction result $[P]_{pk_B}$ to CP. CP will store it and send it's hash to the main data provider node of the blockchain. The main data provider node will use the smart contract of adding the hash, then the hash value of encrypted prediction result $[P]_{pk_B}$ will be broadcasted to all the data provider nodes in the blockchain and published in the blockchain. CP also uses the method (Sect. 4.5) to make the encrypted prediction result $[P]_{pk_B}$ transform to the encrypted prediction result $[P]_{pk_A}$, pk_A is the corresponding user's public key. CP will send the encrypted prediction result $[P]_{pk_A}$ to the corresponding user and the user can decrypt to know the prediction result P.

4.5 Secure Multiple-key Transform Protocol (SMT)

All the data which is about cars and users are encrypted, the ciphertext is encrypted by the unique different public key which is one of the cars' or the users' public keys. Because these data are encrypted by the different public keys, we can't use the homomorphic encryption algorithm to deal with these data directly. In this part, The method borrows the solution called Secure Domain Transformation (SDT) proposed by Liu et al. [8]. In the proposed way, we can transform ciphertexts in different public keys to one centralized key.

The goal of our method: make a ciphertext $[x]_{pk_A}$ with public key pk_A transform to $[x]_{pk_B}$ which is encrypted by an authorized public key $pk_B \epsilon CET_B$. The method is as the following steps:

Step 1 (in CP, CSP): Use $verk_{KGC}$ to verify whether both CET_A and CET_B are valid, and $[x]_{pk_A} \epsilon DA$ in CET_A. if valid, then do the following steps.

Step 2 (in CP): Select and choose a random integer number $r \epsilon Z_N$, then calculate $[x]_{pk_A} \cdot [r]_{pk_A} = [x + r]_{pk_A} \rightarrow X_1$ and use partial private key $SK^{(1)}$ decrypt X_1 to get $X_1^{'}$, then send X_1 and $X_1^{'}$ to CSP.

Step 3 (in CSP): Use partial private $SK^{(2)}$ decrypt X_1 and $X_1^{'}$, then obtain the data m = x + r. Then, encrypt m with an authorized public key pk_B and send $[m]_{pk_B} = [x + r]_{pk_B}$ to the CP.

Step 4 (in CP): Calculate the result that $[m]_{pk_B} \cdot ([r]_{pk_B})^{N-1} \rightarrow [m]_{pk_B}$ with authorized public key pk_B.

In a word, the method is used to transform the encrypted result $[m]_{pk_A}$ from users' or cars' public key pk_A to the encrypted result $[m]_{pk_B}$ with a domain public key pk_B. Correspondingly, It also can transform the encrypted result $[m]_{pk_B}$ from domain public key pk_B to the encrypted result $[m]_{pk_A}$ with users' or cars' public key pk_A.

4.6 Request Query Process Analysis

After the step of key distribution (Sect. 4.3), multiple data providers (DPs), user nodes (UN), shared car nodes (CN), and information-analytical forecast

node (IAFN) obtain their own public-private key pair and certification signature from The Key Generation Center (KGC) by the secure channel. The IAFN information-analytical forecast node obtains data from the cloud platform (CP), and the cloud platform (CP) obtains data from data providers (DP). The mainly accounting node in the blockchain obtains all the multi-key encrypted data by using the smart contract. After the data is transmitted to the cloud platform (CP), the multi-key encrypted data is changed to unify-key encrypted data through the computing service provider (CSP) and Secure multiple-key Transform (SMT) protocol protocols. The CP sends the unify-key encrypted data to the information-analytical forecast node (IAFN), and the information-analytical forecast node (IAFN) will perform training calculations on the data and obtain the SVM classification model before accepting the car rental query data.

In the scheme, obtaining the forecast security result of car rental requires these three processes which are respectively the car rental query data are transferred to the cloud platform (CP) and uploading to the blockchain; secure data processing and predict calculation; forecast results to be uploaded on the blockchain and returned to the user. The three processes are as follows:

Step 1: The query data is transmitted to the cloud platform and uploaded on the blockchain

The platform user node (UN) uses their mobile phones to acquire shared information of car node $Data_{CN}$, the authentication information of car node CET_{CN}, the public key of the car node $PK_{CN} = g^{\Theta_{CN}}$. After confirming automotive vehicle information and authentication information is correct, the user transmits the encrypted data of authentication and information $Enc_{PK_{UN}}(CET_{UN}, Data_{UN})$, $Enc_{PK_{CN}}(CET_{CN}, Data_{CN})$, named as M_{re}. After the cloud platform (CP) receives the information M_{re}, it determines whether the information is a car rental request query information and determines whether the data is valid information. If the information is a car rental request query information and the message is valid, through the Byzantine consensus the car rental request information will be sent to the data provider which is the main accounting node in the blockchain. Then the data provider uses the smart contract (Sect. 4.4) that adds the requested information on the blockchain and store it in the databases of multiple data providers.

Step 2: Secure data processing and predictive calculation

After the cloud platform (CP) receives the information, the cloud platform (CP) uses the computing service provider (CSP) and Secure multiple-key Transform (SMT) protocols to unify the secret data and send the secret request query data to the information-analytical forecast node (IAFN). After the information-analytical forecast node (IAFN) receives the encrypted request query data, the decision function of the SVM model predicts the risk assessment result of the action of the user renting the vehicle.

$$\overrightarrow{x} = (1, [x_1], [x_2], [x_3], [x_4], [x_5], [x_6], [x_7], [x_8]) \tag{5}$$

$$\overrightarrow{w} = (b, w_1, w_2, w_3, w_4, w_5, w_6, w_7, w_8) \tag{6}$$

Step 3: Uploading and returning the prediction result

The information-analytical forecast node (IAFN) finally calculates the prediction result of the request to rent a car and sends it to the cloud platform (CP) by encrypting it with the certified public key. After receiving the data, the CP uses the Secure multiple-key Transform (SMT) protocol with the computing service provider(CSP) to transform the unify-key encrypted data into encrypted data using the public key of the user node. Then the data provider uses the smart contract (Sect. 4.4) in the blockchain to add the encrypted prediction result data $[P]_{pk_A}$ on the blockchain and store it in the databases of multiple data providers. The cloud platform (CP) will also send the encrypted prediction result data $[P]_{pk_A}$ to the user node, then the user node (UN) uses its private key sk_A to decrypt it to obtain the prediction result P.

5 Performance Analysis

5.1 Experiment Preparation

The experimental code runs on a PC. The configuration of the PC is a 6-core Intel i5-9400 processor at 2.90 GHz and 16 GB RAM. The experiment uses the real car rental information dataset CarrentalData and the real personal clothing information dataset Personal-fashion for data simulation, and simulates a dataset named SharedcarData suitable for car sharing scenarios. The CarrentalData and Personal-fashion datasets are publicly available on the Kaggle machine learning dataset resource website. The shared car dataset SharedcarData is divided into two parts proportionally, one part is the training set to train the model, and the other part is used as the test set to test the performance of the model. Table 2 is the basic situation for all the datasets.

Table 2. Basic situation of datasets Table

Dataset name	Example number	Attribute number
CarrentalData	5851	15
Personal-fashion	204	6
SharedcarData	204	9

5.2 Analysis of Experimental Results

When changing scale of the dataset to predict, the accuracy of the model is not drop significantly, indicating that the scale of the test basically has no effect on the accuracy. In order to test the impact of the scale of the test dataset on the

prediction accuracy of the shared car SVM method, we set the maximum number of iterations of the SVM training parameter to 1000 and select 20, 40, and 80 samples from the SharedcarData dataset as the experimental test dataset. The experimental results are shown in Table 3.

Table 3. Accuracy statistics table

Number of test dataset samples	Training time/ms	Accuracy/%
20	63774	84.9
40	62949	83.9
80	63883	84.0

According to the accuracy in the table, the accuracy of SVM machine learning for this shared car is basically around 85%.

5.3 Time Analysis

Calculate the time from the beginning of data generation to the information-analytical forecast node receiving the data encrypted by the unified key, as shown in Table 4:

Table 4. Time calculation analysis table

Step	Step name	Homomorphic multiplication	Encryption	DSecryption
1	Data generation	0	0	1
2	SMT-step1-2	1	1	0
3	SMT-step2	0	1	1
4	SMT-step3	1	0	0

According to the data in the table, it can be seen that this section needs a total of two encryption times, two decryption times, two homomorphic multiplication times. When the prediction result is to be converted from pk_B to the personal user public key pk_A, the time required is the same as steps 2, 3, and 4 in the Table 4.

5.4 Performance Comparison

In this part, we summarize the comparison of the proposed shared car risk prediction scheme with other privacy-preserving SVM classification or blockchain schemes. All the schemes can be divided into two sorts, one is using homomorphic encryption and multi-key conversion protocol to make data more secure,

the other one is the no-using privacy-preserving scheme. The no-using privacy-preserving scheme is less time consuming than the proposed privacy-preserving scheme. In order to support multiple keys situations and the strong security level, our scheme pays little time-consuming to for more security. For prediction accuracy, there is almost no dataset directly suitable for car sharing scenarios, the SharedcarData dataset generated by our simulation will reduce the accuracy of the SVM machine learning algorithm, and thus cannot reach more than 90%. We used the logistic regression algorithm and the SVM machine learning algorithm to calculate the accuracy of the SharedcarData dataset. Experiments show that the accuracy of our SVM machine algorithm (85%) is higher than that of the logistic regression algorithm (72%).

The comparison of method and Algorithm between our scheme we designed and other schemes about the secure machine learning solution is shown in Table 5.

Table 5. Time calculation analysis table

Method/Algorithm	[7]	[8]	[9]	[10]	[11]	Proposed
Support multiple keys	✗	✗	✓	✗	✓	✓
Distributed storage	✗	✗	✗	✓	✓	✓
Data synchronize	✓	✓	✓	✓	✗	✓
Support SVM training	✓	N.A.	✓	✗	✗	✓
Security Level	Weak	Strong	Strong	Weak	Weak	Strong

6 Conclusin and Future Work

In this paper, we propose a blockchain-based shared car risk prediction scheme with the following advantages: (1) Blockchain technology provides a solution for the secure and confidential storage of metadata. The blockchain realizes distributed storage, synchronization, and sharing of metadata. (2) With the use of homomorphic encryption algorithm and multi-key conversion protocol, the multiple entities' shared car, user data can be more secure and prediction can be more accurate. The scheme can provide some valuable solutions and ideas in the data privacy of SVM machine learning. In the future, we can learn and refer to more multiparty secure computing privacy protection methods to optimize the data privacy protection in SVM machine learning as much as possible. Secondly, the privacy algorithm of the shared car risk prediction platform scheme can be popularized and applied in more applications.

Acknowledgment. The work was supported in part by the National Natural Science Foundation of China (61862052), and the Science and Technology Foundation of Qinghai Province (2019-ZJ-7065).

References

1. Valaštín, V., Košt'ál, K., Bencel, R., et al.: Blockchain based car-sharing platform. In: 2019 International Symposium ELMAR, pp. 5–8. IEEE (2019)
2. Zhang, L., Luo, M., Li, J., et al.: Blockchain based secure data sharing system for internet of vehicles: a position paper. Veh. Commun. **16**, 85–93 (2019)
3. Parmar, P.V., Padhar, S.B., Patel, S.N., et al.: Survey of various homomorphic encryption algorithms and schemes. Int. J. Comput. Appl. **91**(8) (2014)
4. Shen, M., Tang, X., Zhu, L., et al.: Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. IEEE Internet Things J. **6**(5), 7702–7712 (2019)
5. Ruijin, W., Yucheng, T., Weiqi Zhang, F.Z.: Privacy protection scheme for internet of vehicles based on homomorphic encryption and block chain technology. Chin. J. Network Inf. Secur. **6**(1), 46 (2020)
6. Byvatov, E., Fechner, U., Sadowski, J., et al.: Comparison of support vector machine and artificial neural network systems for drug/nondrug classification. J. Chem. Inf. Comput. Sci. **43**(6), 1882–1889 (2003)
7. Lin, K.P., Chen, M.S.: Privacy-preserving outsourcing support vector machines with random transformation. In: Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 363–372 (2010)
8. Liu, X., Choo, K.K.R., Deng, R.H., et al.: Efficient and privacy-preserving outsourced calculation of rational numbers. IEEE Trans. Dependable Secure Comput. **15**(1), 27–39 (2016)
9. Liu, X., Deng, R.H., Choo, K.K.R., et al.: Privacy-preserving outsourced support vector machine design for secure drug discovery. IEEE Trans. Cloud Comput. **8**(2), 610–622 (2018)
10. Yao, Y., Chang, X., Mišić, J., et al.: BLA: blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. IEEE Internet Things J. **6**(2), 3775–3784 (2019)
11. Vaidya, J., Yu, H., Jiang, X.: Privacy-preserving SVM classification. Knowl. Inf. Syst. **14**(2), 161–178 (2008)