IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 30 June 2022, accepted 1 August 2022, date of publication 18 August 2022, date of current version 26 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3199874

RESEARCH ARTICLE

Cross-Domain Self-Authentication Based Consortium Blockchain for Autonomous Valet Parking System

LEI HUA[1,4], HAOBIN JIANG[2], JIAN XIAO[3], AND MOHAMMAD SAMIE[4]

[1]School of Automotive and Traffic Engineering, Jiangsu University, Zhenjiang 212013, China
[2]Automotive Engineering Research Institute, Jiangsu University, Zhenjiang 212013, China
[3]School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China
[4]Integrated Vehicle Health Management (IVHM) Centre, School of Aerospace, Transport and Manufacturing (SATM), Cranfield University, Bedford MK43 0AL, U.K.

Corresponding authors: Lei Hua (Lei.Hua@cranfield.ac.uk) and Haobin Jiang (jianghb@ujs.edu.cn)

This work was supported in part by the Graduate Research and Innovation Projects of Jiangsu Province under Grant KYCX20_2862, and in part by the China Scholarship Council under Grant 202008690005.

ABSTRACT This paper proposed a cross-domain self-authentication scheme to address the ''information isolated island'' problem of users' identities storage in servers and the ''redundant registration problem'' of users' identities for Autonomous Valet Parking (AVP). This scheme adopts a decentralized anonymous authentication method to relieve the authentication center's service load. Users are segregated into two categories to increase authentication efficiency: inexperienced and regular users. For the former, the paper explores a self-authentication mechanism based on verification parameters. Then, its valid personal information, pseudonym and public key, were stored in a consortium blockchain (PseIDChain) as the transaction records so that they can be securely shared among servers located in different domains. For the latter (regular users), an efficient authentication mechanism, searching users' personal information on PseIDChain by the smart contract, was proposed. Security proof and simulation results show that the designed scheme has superior security to the existing schemes. Its authentication efficiency is 80.29% and 50.45% higher than the traditional anonymous and batch authentication schemes.

INDEX TERMS Autonomous valet parking, privacy protection, cross-domain authentication, consortium blockchain, pseudonym.

I. INTRODUCTION

Two significant challenges associated with parking spaces are ''parking difficulty'' and ''difficult to park''. The first challenge refers to cases where few parking spots are available, while the other refers to narrow parking spaces in congested areas. They are already crucial problems in crowded places such as shopping malls, hospitals, and the city centres, which causes conflicts, especially during peak hours [1], [2], [3]. As a result, looking for an available parking spot takes more time and effort for drivers, increasing the likelihood of collisions in narrow parking spaces [4], [5]. Automated Valet Parking (AVP) has evolved and been developing rapidly to address these problems.

AVP is a driverless system in the field of autonomous parking that locates a free space in the parking garage and parks the car in an unmanned manner using various connected communication technologies [6]. As illustrated in Fig. 1, AVP enables drivers and passengers to leave their vehicles at the drop-off area (e.g., workplace, shopping mall, park, shown in red) with a command ordered to the AVP system for parking the vehicle at nearby parking lots. Drivers benefit from the Internet of Things (IoT) technology to set such commands to the AVP system via their mobile phones. AVP is equipped with a set of functions, including Short- and Long-range AVP functions (S-AVP and L-AVP) for driving in and parking at local (basement parking) or nearby parking lots

The associate editor coordinating the review of this manuscript and approving it for publication was Razi Iqbal.

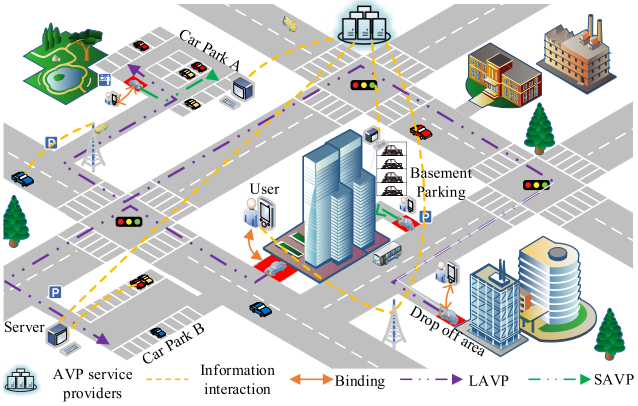

FIGURE 1. AVP echograph.

(car park A or B) while satisfying feasible routes (shown by the purple or green dotted line in Fig. 1). The entire process is autonomously done with intelligent tools, intending to achieve safer and more efficient parking capability and further improve users' last-mile driving experience. Additionally, the application of AVP could increase parking resource utilization, save parking time, and decrease energy consumption. Considering all such advantages, the AVP has been the best-recognized automated parking solution to date [7], [8], [9], [10], [11], [12], [13].

Recently, major players in the automotive industry put efforts into formulating AVP standards, e.g., intelligent transport systems - Automated Valet Parking Systems (AVPS) (ISO 23374-1) [14] and General technical requirements of automated valet parking systems (T/CSAE 156-2020) [12]. There is now a broad range of well-known companies (e.g., Bosch, BMW, Baidu, etc.) proceeding to promote the commercialization of AVP supported internationally by governments and organizations, including, but not limited to, the International Organization for Standardization (ISO), German's Verband der Automobilindustrie (VDA), and China Industry Innovation Alliance for the Intelligent and Connected Vehicles. In addition, two AVP demonstration areas have been built in Beijing, China, serving as AVP verification sites.

In common with the IoT-based system, the downside of AVP is that it suffers from various security and privacy threats, especially concerning storing and processing of users' sensitive information [15]. The threats are broad and include users' locations and identity information in parking space reservations, vehicle parking and recalling, authentication between the local server and the customer, intelligent payment, and data storage and process, see Fig. 2. The main elements are the authentication and the privacy protection of users' locations and identities. First of all, authentication is necessary for all entities in each query (e.g., reserve a vacant parking spot, recall clients' parked vehicle, etc.) to ensure only legitimate ones enjoy AVP services and guarantee service suppliers' benefits (e.g., charge parking fee) [2], [15]. Next, unlike the traditional parking system, AVP requires drivers to submit their vehicles' real-time locations accurately, which is used for vehicle parking navigation [1]. Therefore, the lack of an efficient security scheme leads to AVP being exposed to various cyber-attacks such as eavesdropping attacks, identity fraud attacks, and so on. Finally, local servers store members' privacy information, including their identities, home addresses, places of work, daily travel habits (e.g., time, travel routes, parking preference), and so on. It is straightforward for an unauthorized server or adversary to infer unprotected sensitive data [16]. As a result, the performance of the AVP system will be compromised if such critical issues remain uncared, leading to safety issues for vehicles exposing dangers to drivers and passengers.

Most of AVP's existing works have been mainly directed to constructing functional requirements involving critical technologies in engineering. It includes multi-domain engineering practices e.g., system model [17], [18], [19], [20], parking path planning and tracking [21], [22], vehicle control [23], indoor positioning [24]. On the other hand, the security and privacy issues have been left with less attention until recent years [1], [6], [15]. Industrial trends in advancing the privacy and security of AVP's users, in general, are to employ electronic signature, zero-knowledge, and one-time keys to handle the private leakage problem in the process of AVP's intelligent payment, vehicle recall, and parking space reservation respectively [2], [6], [10], [15]. Moreover, the work presented in [1] demonstrates a privacy-preserving smart parking navigation scheme for protecting privacy in parking spot queries and retrieving the encrypted navigation results from Road-Side Units (RSU). Alqazzaz *et al*. [25] propose a secure and privacy-preserving framework for smart parking systems ensuring the security of real-time information by the Elliptic Curve Cryptography (ECC) and a secured communication channel. These schemes considered an AVP system in one parking lot and did not pay enough attention to the secure storage and sharing problem of AVP users' privacy information. Specifically, users' identities are independently stored in local servers (e.g., the terminal of different shopping malls), and service providers are not pleased to share them due to the differences in parking charge systems and their business profits. Such the mutually independent storage way makes each system to be an ''information island'' so that resources cannot be shared across domains. Therefore, users' information will not be shared with other parking suppliers [26]. These limitations cause customers to repeatedly submit their identities for registering with various suppliers while using the same AVP service, which is an additionally annoying task. It is known as the redundant identity registration problem, a common phenomenon in our daily life. Thus, resolving the ''information island'' problem and the ''redundant identity registration'' problem are the key points this paper intends to address.

Generally, the cross-domain data sharing mechanism is recommended to address the two problems mentioned earlier. In this approach, the key points are the unified management of users' sensitive information and methods for dealing with

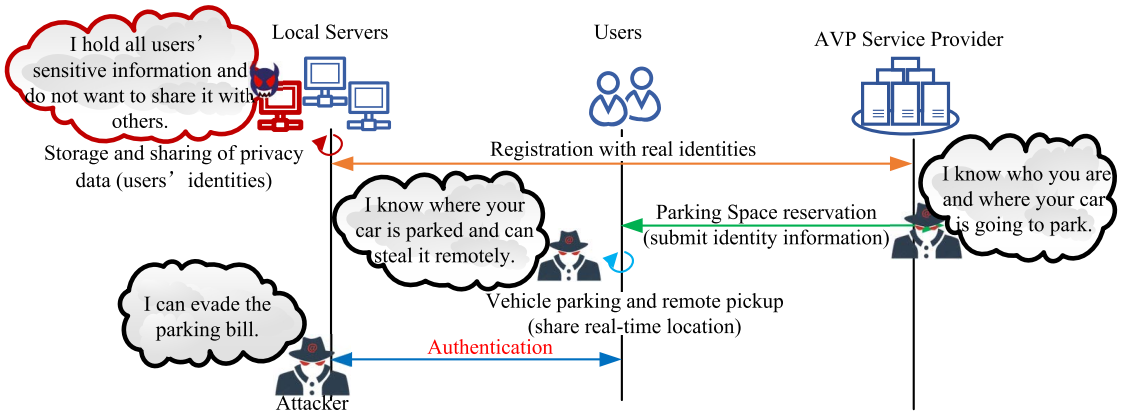

FIGURE 2. Security threats to information interactions of AVP.

different servers verifying the legitimacy of users' identities [26]. Moreover, existing AVP systems have a centralized architecture traditionally adopted. Such an AVP system will suffer from a considerable response time when the number of service requests reaches a certain level. Meanwhile, the service center is usually heavily burdened when demand increases. So it is unsuitable for AVP with many users.

This paper proposes a cross-domain self-authentication scheme based consortium blockchain for AVP to address the following problems:

1) Information isolated island problem of users' identities storage in servers;
2) Redundant registration problem of users' identities;
3) Privacy leakage problem during the process of users' authentication;
4) Low efficiency of authentication for centralized architecture.

The main contribution of this paper is outlined as follows.

1) Develop a secure and decentralized model for AVP by exploiting pseudonym-based anonymity technique and edge computing to solve the problem of users' privacy leakage problem while satisfying real-time requirements.
2) Deploy the vehicle-anonymous-based consortium blockchain (PseIDChain) to realize the sharing of the user's identity information among cross-domain servers. It facilitates building smart contracts for registration, management, and cross-domain efficient authentication for users' identities.
3) Evaluate the proposed scheme extensively from security and efficiency aspects. Experimental results illustrate the superiority and the effectiveness of the proposed scheme.

The remainder of this paper is organized as follows. Section II reviews the relevant works within the context of AVP. Section III formalizes the AVP architecture, attack model, and design goal. Then Section IV presents our cross-domain self-authentication scheme, followed by security analysis in Section V and performance evaluation in Section VI.

II. RELATED WORK

This section analyzes the closest works for the information security of AVP.

Alqazzaz *et al.* [25] proposed a secure and privacy-preserving framework for smart parking systems based on the publish/subscribe messaging model, which provides various services to the user, including real-time parking information dissemination, car park navigation, and parking reservation, and employed ECC algorithm to guarantee the confidentiality of users' privacy. However, the broker (the heart of this framework) is the only entity to verify users' identities. Moreover, users' certifications issued by the trusted authority do not update, which means any attackers can impersonate legitimate users to enjoy services. Besides the study of AVP frameworks, researchers make much effort into the security of specific phases, including parking space reservation, vehicle recall, and navigation. Firstly, the reserved parking space is an essential factor of AVP systems. Pseudonym-based reservations can protect users' identity privacy, but it is easy for a malicious user to launch multiple reservation attacks. To handle this issue, a privacy-preserving reservation scheme for securing AVP system was reported in [15]. This scheme resisted the "double-reservation attack" by zero-knowledge proofs and proxy signatures. Based on this, an improved scheme, the secure and privacy-aware framework of the parking reservation scheme [6], was designed. It added the differential privacy scheme and the deep reinforcement learning algorithm to prevent multiple reservation attacks and enhance the reservation rate. Secondly, AVP requires users to remotely start engines which significantly increases the risks of vehicle theft [10]. Ni *et al.* [10] designed a two-factor authentication between vehicles and smartphones based on one-time passwords, ensuring vehicle security in the remote pickup. NI's research group also explored location privacy protection problems during vehicles to vacant parking spaces in the destinations [1], [27]. A cloud-based privacy-preserving parking

TABLE 1. Contribution to the information security problem of AVP.

Research Study	Research Focus	Techniques for Privacy and Security	Privacy protection
[1] and [27]	The cloud-based privacy-preserving parking navigation system on the way to a vacant parking space in the destinations (centralization).	◆ The anonymous credential	location privacy
[6]	The multiple reservation attack in the parking spaces reservation.	◆ Anonymity and zero-knowledge proof (users' identity privacy) ◆ Deep reinforcement learning algorithm (enhance the reservation rate)	Identity and location privacy
[10]	Authentication between vehicles and smartphones.	◆ One-time passwords	Identity privacy
[15]	The double-reservation attack in the parking spaces reservation.	◆ Zero-knowledge proofs of knowledge ◆ Proxy signature	Identity privacy
[25]	Secure and privacy-preserving framework (centralization).	◆ the publish/subscribe messaging model (provides various services) ◆ Elliptic curve cryptography (real-time parking information) ◆ Certifications (uses' identities)	None
This work	Cross-domain self-authentication between users and servers	◆ Pseudonym-based anonymity (users' identity and location privacy) ◆ Consortium blockchain and smart contract (the users' identity management and secure sharing)	Identity and location privacy

TABLE 2. Closest works on component's security problem of AVP.

Components of AVP	Research Study
Parking reservation	[6], [15]
Vehicle parking and remote pickup	[10]
Self-authentication between local server and users	This work
The storage and sharing of users' privacy information among multiple servers	This work
Security architecture	[25] and this work

Notes: Both this work and Ref. [25] proposed the security architecture for AVP, but they are different. The security architecture proposed in [25] is centralized. However, our proposed architecture is a decentralized model based on edge computing, which can better meet AVP's real-time requirement.

navigation system proposed in [1] utilized the anonymous credential to protect the location privacy of vehicles on finding accessible parking spots for vehicles. Its extended version [27] analyzed the navigation performance in detail. The comparison of these related works and this paper is shown in TABLE 1 and TABLE 2. As shown in TABLE 2, the closest works do not pay enough attention to the AVP's decentralized security architecture, self-authentication between local servers and users, and the storage and sharing of users' privacy information among multiple servers. These are the research focus this paper does.

III. PROBLEM FORMULATION

A. AVP ARCHITECTURE

Fig. 3 describes AVP system architecture which consists of four components, namely, Trusted Authority (*TA*), AVP service provider (*AVPpro*), local server (*Serv*), and user. The details are as follows.

1) *TA* (*Fully trusted*): *TA* is a trusted third party with extensive communication and computation capabilities that will not compromise with any entities. It is responsible for system initialization, the registration and management of system entities' identities (users, service providers, and local servers), smart contract deployment, and malicious vehicle revocation. In this paper, all local servers and users must be registered with their real identities to be legitimate ones.
2) *AVPpro* (*Fully trusted*): *AVPpro* is in charge of providing parking services to users, such as releasing parking space status, making parking space reservations, etc. The corresponding services are only available to AVP registered users.
3) *Serv* (*Semi-trusted*): *Serv* is the local server of the parking lots (provide AVP service from different providers), which can perceive the status of each parking spot by its deployed geomagnetic sensors and upload them to *AVPpro* in real-time. Based on that, users can reserve their favorite parking spots.
4) *User* (*Untrusted*): Each user has a phone to reserve parking spaces, issue parking and recall instructions to a paired Autonomous Vehicle (AV). AVs can communicate with *Serv* and phones by their equipped communication model (like On-Broad Units, OBU). They can store sensitive information (e.g., session keys, temporary anonymities, etc.) and parking-related information (e.g., high-precision maps, feasible routes to parking spaces, etc.).

The flow of AVP implementation in this paper is as follows:

1) **Registration**: There are two phases to the registration process for this paper. First, it is indispensable for the AVP system's *User* and *Serv* to obtain system parameters (temporary anonymity, session key, ID, certificates, etc.) through the registration work using their real identities before the system implementation. Second, using the temporary anonymity to enjoy AVP service without revealing their personal information.
2) **Publication of parking space status**: Each parking space is equipped with a geomagnetic sensor and

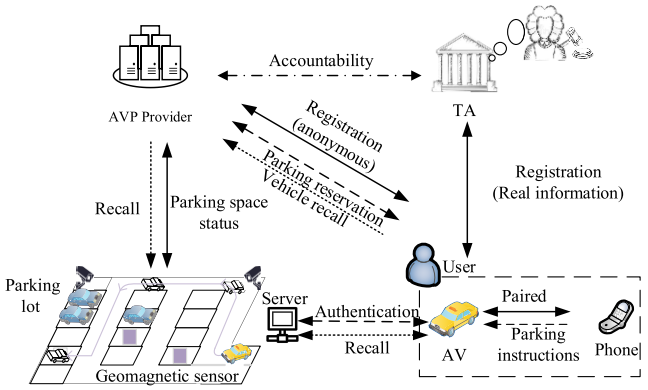

FIGURE 3. AVP architecture.

wireless communication unit that monitor and upload the status to *AVPprov* for publication.

3) **Parking space reservation**: *User* could use the phone (more specifically, an app) to preview the parking space's status of the target parking lot and book a favorite one.
4) **Parking**: *User* sends parking instructions and the location of a reserved parking space to its AV by the linked phone. Then, the AV will reach the target parking lot and authenticates with *Serv*. Finally, parking will be done based on the necessary information provided by *Serv*, like high-precision maps, feasible driving paths, and so on.
5) **Recall**: If *User* wishes to recall its vehicle, submit a recall request to the *AVPprov* and complete the payment of bills (e.g., parking fee, car washing fee, electricity charge, etc.).
6) **Accountability**: If a malicious event occurs in any processes from 1) to 5) (e.g., remote vehicle theft, users deliberately booking several parking spaces, etc.), *TA* will investigate and arbitrate.

B. ATTACK MODEL AND DESIGN GOAL

To execute an AVP service, the four components of the AVP system must communicate mutually (wired or wireless). Users who apply for AVP services, for example, require wireless connectivity with *Serv* to complete authentication and acquire a high-precision map. In this process, malevolent attackers try to steal users' legal identities by monitoring the network and launching counterfeit attacks [26]. Furthermore, *AVPprov* and *Serv* could employ data analysis to sniff users' location privacy, although they are fully trusted (honest and curious) in this paper. As a result, the AVP system is vulnerable to internal and external threats. This paper focuses on solving the information island problem of data storage in local servers, the users' redundant registration problem, and their privacy leakage problem during the authentication process. In this sense, we primarily analyze the types of network attacks exposed to entities throughout the authentication process rather than the physical attacks each entity faces.

1) **Privacy attack**: Attackers are endowed with the ability to analyze users' genuine identities. Daily whereabouts can be interpreted by eavesdropping on users' sensitive information or attacking the server database, such as users' home addresses, daily travel schedules, etc. These enable attackers to launch more precise privacy attacks furtherly.
2) **Impersonation attack**: Through the Sybil attack, the eavesdropping attacks, or the replay attacks, attackers or even malicious legitimate users premeditated to obtain several identities to establish a more convenient and comfortable driving environment for their benefit. They can also impersonate a legal member reserving one parking space to evade paying bills like parking fees, energy transaction bills, etc., and even remotely steal a target vehicle by the recall instruction.
3) **Repudiation attack**: AVP users try to evade legal responsibility by hiding their misconduct with their pseudonyms, which is unavoidable for an anonymous authentication scheme. A malicious user, for example, uses its anonymity to send a vehicle recall order but then claims that its vehicle was stolen and did not do that behavior and files a claim with *AVPpro*.

This research aims to develop a cross-domain and self-authentication scheme for user identity in AVP, which can realize a secure and efficient authentication process between users and servers. Meanwhile, this scheme can tackle the redundant registration problem of users' identities and the information isolated island of local servers, as well as the users' privacy and location privacy leakage problem during the authentication process, thereby resisting the three attacks above consequently.

IV. PROPOSED SCHEME

This paper designed a pseudonym-based user anonymous authentication scheme to protect users' identity and location privacy. Even if an attacker can eavesdrop on the network information, it cannot analyze the real identity of users and cannot grasp a specific one's location privacy consequently. At the same time, the decentralized and secure sharing of user anonymized identity among servers can be realized by consortium blockchain. This method makes it impossible for honest but curious *AVPpro* and *Srev*, and malicious attackers who try to attack server databases to analyze and grasp users' private information.

A. DEPLOYMENT ON VEHICLE-ANONYMOUS-BASED CONSORTIUM BLOCKCHAIN (PseIDChain) AND SMART CONTRACT (PseIDContract)

We designed a system model based on edge computing for AVP, as shown in Fig. 4, to allow *Serv* to monitor and publish all parking spots' status to users in real-time. Users can book, modify and even cancel their orders with minimal delay. The system, from top to bottom, is divided into three layers: cloud layer, edge layer, and terminal layer. The

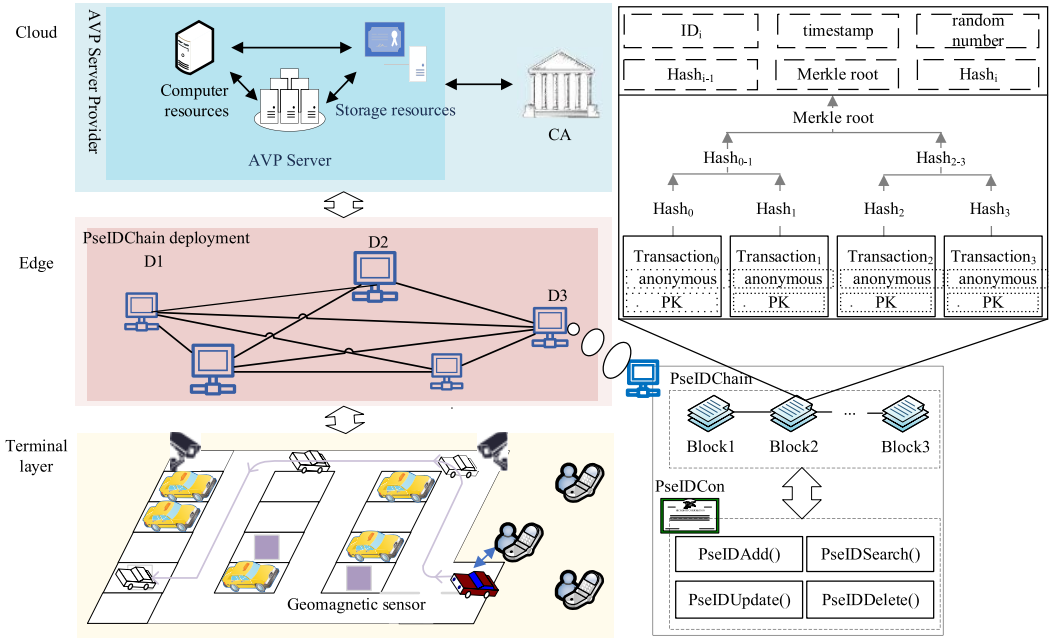

FIGURE 4. System model.

consortium blockchain is a specific blockchain that maintains a distributed shared database through nodes authorized by the system. Only more than half of the consortium members can reach a consensus to generate new blocks [28]. Compared with public and private chains, it benefits from a more negligible overhead and lower cost features which are better suited to the real-time requirement of AVP. Thus, we deployed PseIDChain at the edge layer to securely store temporary pseudonyms and public keys of users, addressing the secure sharing problem of users' privacy information as well as the "information isolated island" problem of different local servers in various car parks. Meanwhile, we also developed a smart contract named PseIDContract with four functions, adding function *PseIDAdd*, searching function *PseIDSearch*, deleting function *PseIDDelete* and an updating function *PseIDUpdate* to realize the users' identities management of PseIDChain.

B. PROPOSED CROSS-DOMAIN SELF-AUTHENTICATION SCHEME

The proposed cross-domain self-authentication scheme mainly includes three parts (see system flowchart Fig. 5): 1) system initialization, 2) decentralized authentication based on authentication parameters for "*Inexperienced Users*", and 3) cross-domain authentication based on consortium blockchain for "*Regular Users*". The details are as follows, and the symbols' definition is listed in TABLE 3.

1) SYSTEM INITIALIZATION

Before the system implementation, all entities (servers and users) must register with their real identities at TA to be legitimate and consequently obtain their own unique identities, key pairs, signatures, and certificates (see Fig. 6).

TABLE 3. Symbols and definition.

Symbols	Definition
p	prime number
a, b	constant, $a, b \in Z_q^*$
G	The base point of the elliptic curve
n	The order of the base point from the infinity point
SK_x, PK_x, AP_x	Public key, private key, authentication parameters of entity x (include servers and users)
ID_x, PID_x	Real and anonymous identity of entity x
$Sign(\cdot), Cert(\cdot)$	Signatures and certificates by SK_x
Key	Symmetric key
TS	Timestamp
$Ecc(\cdot)$	Encrypt message by elliptic curve cryptographic algorithm
$AvailPL$	Available parking space information
$HMAC(\cdot)$	Message authentication code

1) **TA**: TA generates its public and private key pairs $SK_{TA} = x_{Serv}, PK_{TA} = SK_{TA}G$ by the elliptic curve cryptography (ECC) (x_{TA} is a random number, and $x_{TA} \in Z_q^*$). Then, it chooses two hash functions $H : \{0,1\}^* \rightarrow \{G_1, +\}$ and $h : \{0,1\}^* \rightarrow Z_q^*$, and publishes system parameters $Para : (p, a, b, G, n, h.PK_{TA}, h(\cdot), H(\cdot), ECC(\cdot))$.
2) ***Serv* registration**: with the help of TA, first, *Serv* downloads system parameters and obtains a unique identity ID_{Serv}, private key $SK_{Serv} = x_{Serv}(x_{Serv}$ is a random number, and $x_{Serv} \in Z_q^*)$, public key $PK_{Srev} = SK_{Serv}G$, *Serv*'s location Loc_{Serv}, certification $Cert_{SK_{Serv}}(h(PK_{Srev}, Loc_{Serv}))$ and authentication

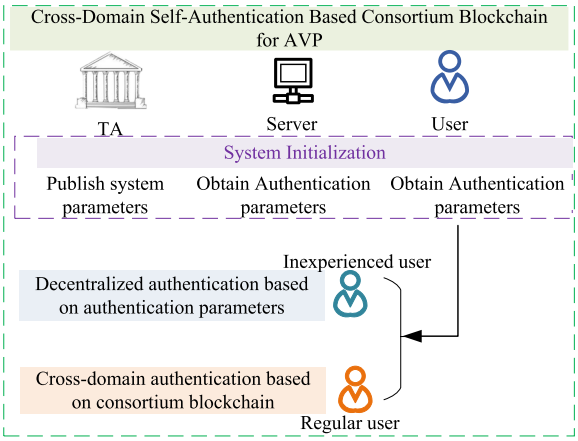

FIGURE 5. System flowchart.

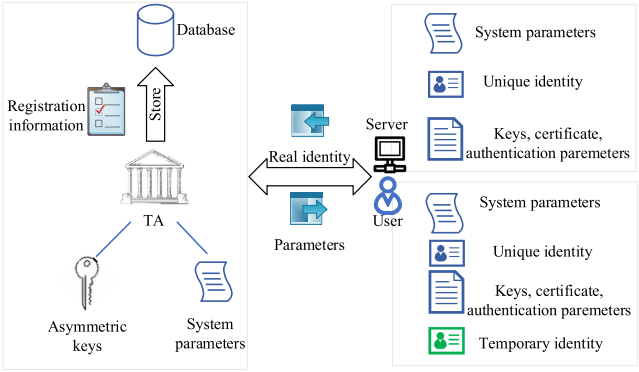

FIGURE 6. System initialization.

parameters for the first identification AP_{Serv} and AP'_{Serv} ($AP_{Serv} = SK_{TA} \cdot AP'_{Serv} \cdot G, AP'_{Serv} = h(ID_{Serv})$).

3) ***User* registration** (Consistent with *Serv*'s registration process): The *User* downloads system parameters and obtains a unique identity ID_{User}, private key $SK^1_{User} = x^1_{User}$ ($x^1_{User}$is a random number, and $x^1_{User} \in Z^*_q$), public key $PK^1_{User} = SK^1_{User}G$, temporary identify $PID^1_{User} = ID_{User}SK^1_{User} \cdot PK_{TA}$, and authentication parameters for the first identification AP_{User} and AP'_{User} ($AP_{User} = SK_{TA} \cdot AP'_{User} \cdot G, AP'_{User} = h(ID_{User})$.

2) CROSS-DOMAIN SELF-AUTHENTICATION SCHEME

In order to improve the users' authentication efficiency, we divided users into two types, "*Inexperienced users*" (the user has never registered and enjoyed AVP services) and "*Regular Users*" (the user has enjoyed AVP services). For the former, we designed decentralized authentication based on authentication parameters. For the latter, we proposed cross-domain authentication based on the consortium blockchain. Both strategies employed the decentralized authentication architecture, decreasing the heavy burden of the authentication center and the considerable authentication delay of systems. It is worth emphasizing that users' identities used for

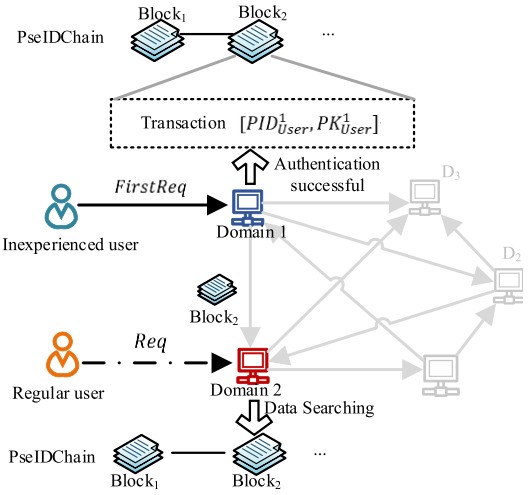

FIGURE 7. Cross-domain self-authentication scheme for AVP.

authentication with servers, except for TA, are anonymous to protect users' privacy and identity privacy better. At the same time, users who have used the same pseudonym for a long time are more vulnerable to guessing attacks while enjoying AVP services in different geographical regions. Hence, users should replace their pseudonyms regularly.

As shown in Fig. 7, an *inexperienced user* must send the first request to a local server located in Domain 1 (the blue one) and pass the identification process when it would like to enjoy AVP service. This local server, then, will store its pseudonym and public key on PseIDChain and share them with other servers. If this user becomes a regular one and will enjoy AVP service again, local servers (the red one) only need to search its pseudonym and public key on PseIDChain to verify it. The details are as follows.

➢ **Preparation**

1) **Information Distribution**: The AVP service provider publishes the real-time status of each parking spot. Available parking space message is M^i_{Serv}, $M^i_{Serv} = PK^i_{Serv}, Loc_{Serv}, AvailPL, Cert_{Serv}$ ($h(PK^i_{Serv}, Loc_{Serv}, AvailPL)$).
2) **Service selection**: The user selects a target parking spot with their demand, and then he/her is authenticated with the local server of this parking spot to submit an AVP service request. The detail is that the *User* chooses a favorite parking lot based on the available parking space message M^i_{Serv}, and verify its validity by certification ($Cert_{Serv}$).

- **Cross-domain self-authentication scheme for AVP**:

The first request of "inexperienced users": decentralized authentication based on authentication parameters

The authentication steps of "inexperienced users" is shown in Fig. 8, and the details are as follows.

1) ***User***: Inexperienced user sends the first request (*FirstReq*) on AVP service, $FirstReq = (TS, Ecc(Key, PK^1_{User}, PID^1_{User}, Sign(Key, PK^1_{User}, PID^1_{User}))$,

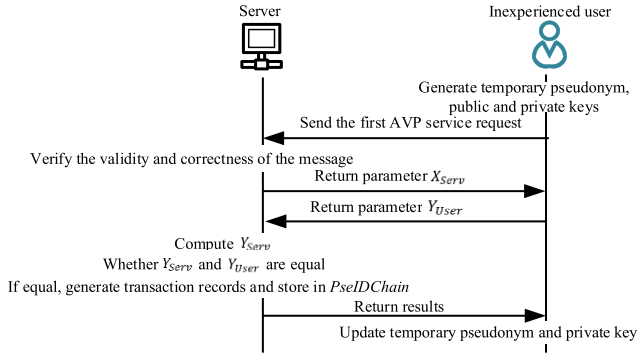

FIGURE 8. Decentralized authentication based on authentication parameters.

$HMAC(\cdot)$, in which $HMAC(\cdot) = HMAC(TS, Ecc(Key, PK^1_{User}, PID^1_{User}, Sign(Key, PK^1_{User}, PID^1_{User})))$.

2) ***User***: Inexperienced user sends the first request ($FirstReq$) on AVP service, $FirstReq = (TS, Ecc(Key, PK^1_{User}, PID^1_{User}, Sign(Key, PK^1_{User}, PID^1_{User})), HMAC(\cdot)$, in which $HMAC(\cdot) = HMAC(TS, Ecc(Key, PK^1_{User}, PID^1_{User}, Sign(Key, PK^1_{User}, PID^1_{User})))$.
3) ***Serv***: $Serv$ verifies the validity and integrity of $FirstReq$ based on TS and $HMAC(\cdot)$. If successful, it encrypts $FirstReq$ to obtain and store related parameters $(Key, PK^1_{User}, PID^1_{User})$. Then, choose a random number $\alpha \in Z^*_q$ and compute $X_{Serv} = \alpha G$. Finally, send a message $M_1 : (TS, E_{key}(X_{Serv}, Key \cdot AP'_{Serv}, HMAC(TS, E_{key}(X_{Serv}, Key \cdot AP'_{Serv},))))$ to User.
4) ***User***: $User$ computes $X_{User} = \beta G$ (β a random number, $\beta \in Z^*_q$) and Y_{User}(see formula 1). Then, it sends a message $M_2 : (TS, E_{key}(X_{User}, Key \cdot AP'_{User}, Y_{User}, HMAC(TS, E_{key}(X_{User}, Key \cdot AP'_{User}, Y_{User}))$ to $Serv$.
5) ***Serv***: $Serv$ computes Y_{Serv} according to formula (2) and compare it with Y_{User}, if they are equal, this user is a valid one (more specifically, the identity of this user is valid.)
6) ***User***: $User$ updates its public key and pseudonym, from $[PK^1_{User}, PID^1_{User}]$ to $[PK^2_{User}, PID^2_{User}]$.

$$Y_{User} = e(\beta \cdot Key \cdot AP'_{Serv}, PK_{TA}) \times e(Key \cdot AP_{User}, X_{Serv}) \quad (1)$$

$$Y_{Serv} = e(\beta \cdot Key \cdot AP'_{User}, PK_{TA}) \times e(Key \cdot AP_{Serv}, X_{User}) \quad (2)$$

The request of "regular users": cross-domain authentication based on the consortium blockchain

The authentication steps of "regular users" is shown in Fig. 9 and the details are as follows.

1) ***User***: Regular $User$ sends the request (Req) to $Serv$ by their updated public key and pseudonym, $Req = (TS, Ecc(PK^2_{User}, PID^2_{User}), Sign(PK^2_{User}, PID^2_{User}), HMAC(TS, Ecc(PK^2_{User}, PID^2_{User}), Sign(PK^2_{User}, PID^2_{User})))$.
2) ***Serv***: $Serv$ obtains PK^2_{User} and PID^2_{User} by Req, and searching them on PseIDChain by the developed $PseIDSearch()$ of PseIDContract. If PK^2_{User} and PID^2_{User} exist on PseIDChain, that is, this user is a valid one and is approved to enjoy AVP service; otherwise, refuse it.

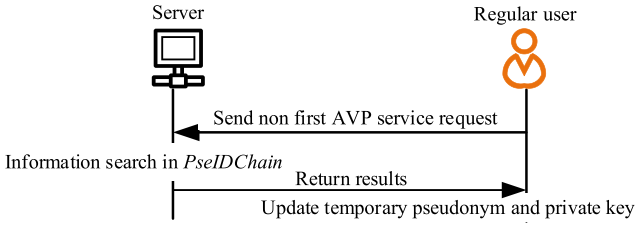

FIGURE 9. Cross-domain authentication based on the consortium blockchain.

➢ **The management of users' pseudonyms on PseIDChain**: The target server will save the user's public key and pseudonym $[PK^1_{User}, PID^1_{User}]$ as a transaction of PseIDChain, if this user is a valid one. Meanwhile, $Serv$ regularly packages transactions to generate blocks and updates PseIDChain with other consortium members by the auditing mechanism. After completing one authentication, the user must update the public key and pseudonym to reaccess the AVP service and against the guessing attack. Following are the specifics:

1) ***User***: $User$ regenerates its temporary public key and pseudonym $[PK^2_{User}, PID^2_{User}]$ according to the related process described in Section IV. B, and sends update requests (Update), $Update = (TS, Ecc(h((PK^1_{User}, PID^1_{User}, PK^2_{User}, PID^2_{User})), Sign(\cdot), HMAC(\cdot))$.
2) ***Serv***: Servupdates the record from $[PK^1_{User}, PID^1_{User}]$ to $[PK^2_{User}, PID^2_{User}]$ by $PseIDSearch()$ and $PseIDUpdate$

V. SECURITY ANALYSIS

This subsection will analyze the security of the proposed approach from cross-domain authentication, anonymity, traceability of user identities, and data storage confidentiality. These can resist the privacy attacks, impersonation attacks, and repudiation attacks described in Section III. B. The paper then continues by comparing the proposed technique against existing solutions.

A. AUTHENTICATION

As previously stated, the cross-domain self-authentication scheme designed in this paper is divided into two parts: 1) decentralized authentication based on authentication parameters for inexperienced users; 2) cross-domain authentication based on consortium blockchain for regular users.

Decentralized authentication based on authentication parameters for inexperienced users: Authentication

TABLE 4. Security comparison.

Scheme	Decentralization	Cross-domain authentication	The secure storage and sharing of users' privacy information	Anonymity	Traceability	Data confidentiality
[6]	×	×	—	×	×	✓
[10]	—	—	—	✓	✓	✓
[15]	—	—	—	✓	✓	✓
[25]	×	—	—	×	×	✓
[29]	×	×	—	✓	✓	—
[30]	✓	×	—	✓	✓	—
This work	✓	✓	✓	✓	✓	✓

Note: "✓"indicates meet this security, "×" indicates do not meet, and "—" indicates no consideration

parameters $[AP_{User}, PK^1_{User}]$ supplied by TA during the system initialization phase are used to authenticate users' identities.

- **Theorem**: Assuming H is a random oracle and meets both DL and CDH assumptions, the proposed scheme has IND-CCA2 authentication.
- **Proof**: Assuming that the adversary can compute a legitimate user's authentication parameters AP_{User} by hash queries for $q_i(i = 1, 2)$ times, that is, the DL and CDH problems are computable.

Game 1 (*DL Problem*):

- **Initialization**: Generate system parameters $Para : (p, a, b, G, n, h.PK_{TA}, h(\cdot), H(\cdot), ECC(\cdot))$.
- **Query**: First, the attacker interrogates the challenger about the target user's identity (ID_{User}). Then, compute $y = h(ID_{User}) \cdot G$ and return.
- **Challenge**: The attacker computes SK_{TA} based on G and PK_{TA}, $h(ID_{User})$ based on y, and $AP_{User} = SK_{TA} \cdot h(ID_{User}) \cdot G$ consequently. That is, G and PG are known, calculate P.

Game 2(*CDH Problem*):

- **Initialization**: Generate system parameters $Para : (p, a, b, G, n, h.PK_{TA}, h(\cdot), H(\cdot), ECC(\cdot))$.
- **Query**: First, the attacker interrogates the challenger about the target user's identity (ID_{User}). Then, compute $y = h(ID_{User}) \cdot G$ and return.
- **Challenge**: The attacker computes $AP_{User} = SK_{TA} \cdot h(ID_{User}) \cdot G$ based on G, $PK_{TA} = SK_{TA}G$ and $y = h(ID_{User}) \cdot G$. That is, G, PG, and QG are known, calculate P.

Cross-domain authentication based on consortium blockchain for regular users:

If the user is a regular one, *Serv* only needs to identify it by indexing the user's current public key and pseudonym $[PK^1_{User}, PID^1_{User}]$ on PseIDChain. (PseIDChain is a consortium blockchain, its security is recognized). Therefore, the adversary cannot determine the authentication parameters of the legitimate user because the chance of solving DL and CDH problem in polynomial time is negligible, hence the user's identity in this article is valid.

B. ANONYMITY AND TRACEABILITY

Users' sensitive information during their authentication process is a temporary pseudonym PID_{User}, $PID_{User} = ID_{user} \oplus h(SK_{User} \cdot PK_{TA})$. Since SK_{User} and ID_{user} are issued by TA and are held by themselves only. Besides, attackers cannot compute the user's private key (SK_{User}), despite public key $(PK_{User} = SK_{User}G)$ is easy to grasp (DL Problem). Therefore, attackers and curious servers cannot grasp users' real identities, meaning the scheme has anonymity.

Besides, users must anonymize their real identities to protect their identity privacy and location privacy. Meanwhile, in disputes and culpability determination events, law enforcement agencies must be able to track down the real identity of the malicious user. That is, allowing the user to communicate anonymously and tracking the user's real identity if necessary. For example, a user recalls his/her vehicle by its pseudonym, but it claims another user stole it. The sent message in this paper contains users' pseudonym PID_{User} and public key PK_{User}. Based on that, TA can trace the real identity of the malicious user by formula (3). Thus, the proposed scheme is traceable.

$$\begin{aligned} ID_{user} &= PID_{User} \oplus h(SK_{TA} \cdot PK_{User}) \\ &= ID_{user} \oplus h(SK_{User} \cdot PK_{TA}) \oplus h(SK_{TA} \cdot PK_{User}) \end{aligned} \tag{3}$$

C. DATA CONFIDENTIALITY

We take users' anonymities and public keys as the transaction data to create a particular consortium blockchain, PseIDChain, which allows for the secret sharing and storage of users' identities among servers. That is, data confidentiality is ensured. For servers and attackers, even if they got a target user's anonymity and public key (the user proactively sends his/her anonymity and public key to servers or the attacker illegally obtains them through eavesdropping etc.), they are unable to calculate the target user's true identity. At the same time, the security characteristics of consortium blockchain, such as distributed and data confidentiality, make it difficult for attackers to discover any encrypted information from our proposed PseIDChain, even if they control single or numerous servers. Thus, the proposed scheme ensures the confidentiality of users' sensitive data.

TABLE 5. Experimental environment.

Items	Tools and version
Operating System	Ubuntu 18.04.4 LTS
Blockchain framework	Hyperledger Fabric 1.4.4
SDK	Fabric-SDK-go 1.0.0
cURL	curl 7.75.0 (x86_64-pc-linux-gnu)
Docker	docker 19.03.6, build 369ce74a3c
Docker-compose	docker-compose version 1.17.1, build unknown
Golang	go1.16.3 Linux/amd64
Cryptography library	crypto/aes, ecdsa, elliptic, hmac, etc.

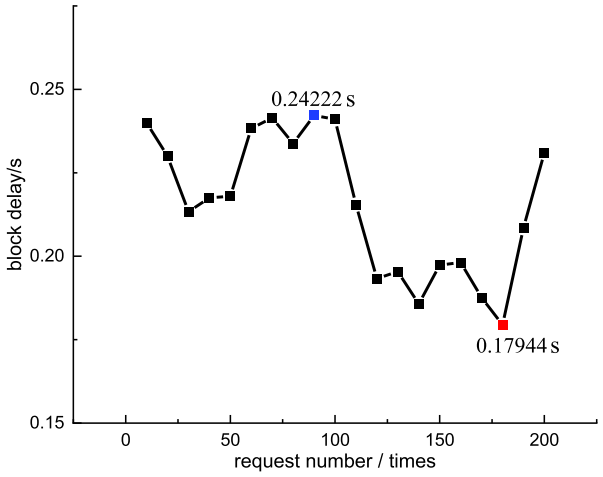

FIGURE 10. Block delay of PseIDChain.

D. SECURITY COMPARISON

The three subsections above prove that our proposed scheme has cross-domain authentication, anonymity, traceability, and data confidentiality. Meanwhile, the secure storage and sharing of users' privacy information, one of the research focuses of this paper, has been achieved by them. So, we also compared our proposed authentication scheme to representative solutions in [6], [10], [14], [25], [29], and [30]. Among them, [29] is a typical pseudonym-based scheme, and [30] is batch authentication (batch authentication and decentralized authentication are the effective methods of the efficient authentication scheme). Others are the more state-of-the-art algorithms related to the security scheme of AVP. The results demonstrate that our proposed scheme is more secure (see TABLE 4).

VI. PERFORMANCE EVALUATION

We use the Hyperledger Fabric to build the network environment of PseIDChain (a consortium blockchain based on users' identities), dockers to simulate consortium nodes (local servers), and developed PseIDContract (smart contracts) to manage users' identities. We set up 9 nodes in PseIDChain, including 2 CA nodes, 3 order nodes, and 4 peer nodes, and established 2 SDK clients, as shown in TABLE 5. Based on it, analyzing this paper's preference from the block delay, authentication time, and system throughput.

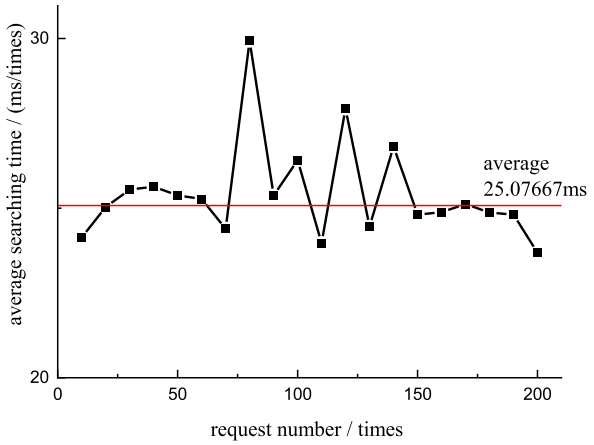

FIGURE 11. Authentication delay.

- Block delay: The block latency of PseIDChain is examined in this subsection since it directly impacts the overall efficiency of the AVP system. As demonstrated in Fig. 10, the block delay of PseIDChain is less than 0.25 s, and it does not increase linearly with the increasing number of requests.

➢ **Authentication delay**: The authentication delay in this article is divided into two parts, authentication delay for inexperienced and regular users.

1) *Serv* authenticate an inexperienced user based on authentication parameters issued by TA; thus, the authentication delay of it is the sum of three main operation costs, point multination $T_{mul} = 0.6$ms, MapToPoint hash $T_{mtp} = 2.7$ ms and bilinear maps pairing $T_{par} = 1.6$ ms [31]. So, authentication delay for inexperienced users is $8T_{mul} + 4T_{par} = 11.2$ ms.
2) The authentication to regular users is completed by searching their public key and anonymous identity $[PK^1_{User}, PID^1_{User}]$ on PseIDChain. As shown in Fig. 11, the number of requests has less impact on the authentication delay of the regular users. The average single query time is about 25.08 ms, which meets the requirements of rapid authentication on the internet of vehicles.

➢ **System throughput**: As shown in Fig. 12, the median of this work's system throughput is 46.65 TPS, and its maximum value is 55.72 TPS.

➢ **Average delay**: Furthermore, we also analyze the average delay of this paper. Due to related works on the information security problem of AVP did not focus on the privacy protection of the authentication between users and multiple local servers. Meanwhile, improving authentication efficiency is one of the research focus in this paper, and batch authentication and decentralized authentication architecture are effective strategies for it. So, the authentication delay of this scheme is compared with a typical pseudonym-based authentication scheme

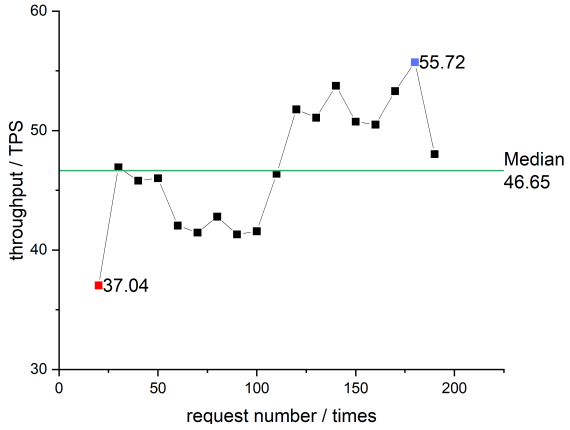

FIGURE 12. System throughput.

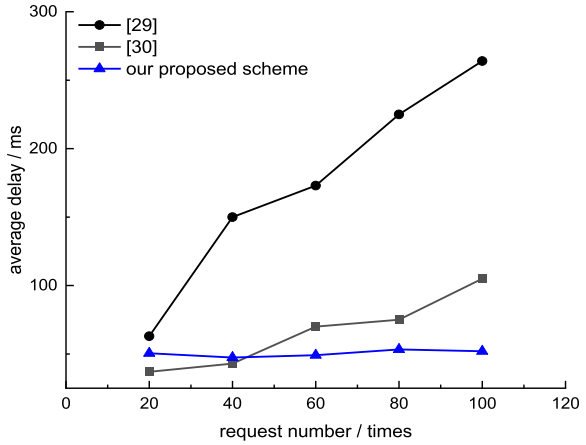

FIGURE 13. Average delay.

reported in [29] and a representative batch authentication solution reported in [30]. Fig. 13 illustrates the comparing results. Taking 100 service requests as an example, the authentication efficiency of our scheme is 80.29% and 50.45% higher than that of [29] and [30], respectively.

VII. CONCLUSION

This paper proposes a cross-domain self-authentication scheme for AVP based on the consortium blockchain, in which users are classified and different decentralized authentication strategies are designed, respectively. Additionally, PseIDChain (a consortium blockchain based on users' identities) and PseIDContract manage all legitimate users' privacy information. Consequently, this strategy solved the ''information isolated islands'' problem of different service providers' servers, decreased the burden of centralized concurrent queries, and enhanced the authentication efficiency of users. This scheme is feasible based on the comprehensive safety and performance analysis results.

In the future, we will implement a prototype smart parking system in the real world based on our proposed secure AVP framework, cross-domain self-authentication method, and the storage and sharing mechanism of users' privacy information to evaluate the proposed scheme's performance metrics more precisely and improve it. Moreover, considering that electric vehicles are an inevitable trend in the future, however, range anxiety has always been the main reason consumers buy. The integration of AVP and the intelligent charging system may achieve unmanned electric vehicles to autonomously drive to the charging pile for charging, which will solve the range anxiety issue to a certain extent. This is a meaningful future research direction.

REFERENCES

[1] J. Ni, K. Zhang, Y. Yu, X. Lin, and X. Shen, ''Privacy-preserving smart parking navigation supporting efficient driving guidance retrieval,'' *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6504–6517, Jul. 2018.

[2] L. Zhu, M. Li, Z. Zhang, and Z. Qin, ''ASAP: An anonymous smart-parking and payment scheme in vehicular networks,'' *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 4, pp. 703–715, Jul. 2020.

[3] M. Aljohani, S. Olariu, A. Alali, and S. Jain, ''A survey of parking solutions for smart cities,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 10012–10029, Aug. 2022, doi: 10.1109/TITS.2021.3112825.

[4] R. Ke, Y. Zhuang, Z. Pu, and Y. Wang, ''A smart, efficient, and reliable parking surveillance system with edge artificial intelligence on IoT devices,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 4962–4974, Aug. 2021.

[5] F. Al-Turjman and A. Malekloo, ''Smart parking in IoT-enabled cities: A survey,'' *Sustain. Cities Soc.*, vol. 49, Aug. 2019, Art. no. 101608.

[6] S. R. Pokhrel, Y. Qu, S. Nepal, and S. Singh, ''Privacy-aware autonomous valet parking: Towards experience driven approach,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5352–5363, Aug. 2021.

[7] S. Jiang, C. Zhao, Y. Zhu, C. Wang, and Y. Du, ''A practical and economical ultra-wideband base station placement approach for indoor autonomous driving systems,'' *J. Adv. Transp.*, vol. 2022, pp. 1–12, Mar. 2022.

[8] M. Khalid, Y. Cao, N. Aslam, M. Raza, A. Moon, and H. Zhou, ''AVPark: Reservation and cost optimization-based cyber-physical system for long-range autonomous valet parking (L-AVP),'' *IEEE Access*, vol. 7, pp. 114141–114153, 2019.

[9] X. Zhang, X. Xia, S. Liu, Y. Cao, J. Li, and W. Guo, ''An integrated framework on autonomous-EV charging and autonomous valet parking (AVP) management system,'' *IEEE Trans. Transport. Electrific.*, vol. 8, no. 2, pp. 2836–2852, Jun. 2022.

[10] J. Ni, X. Lin, and X. Shen, ''Toward privacy-preserving valet parking in autonomous driving era,'' *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2893–2905, Mar. 2019.

[11] M. Khalid, K. Wang, N. Aslam, Y. Cao, N. Ahmad, and M. K. Khan, ''From smart parking towards autonomous valet parking: A survey, challenges and future works,'' *J. Netw. Comput. Appl.*, vol. 175, Feb. 2021, Art. no. 102935.

[12] *General Technical Requirements of Automated Valet Parking Systems*, Standard T/CSAE 156–2020, China Society of Automotive Engineers, China Communications Industry Association, China, Nov. 2020.

[13] H. Banzhaf, D. Nienhuser, S. Knoop, and J. M. Zollner, ''The future of parking: A survey on automated valet parking with an outlook on high density parking,'' in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Redondo Beach, CA, USA, Jun. 2017, pp. 1827–1834.

[14] *Intelligent Transport Systems-Automated Valet Parking Systems (AVPS)*, Standard ISO 23374–1, International Organization for Standardization, Under development, Feb. 2022. [Online]. Available: https://www.doc88.com/p-37287878695478.html

[15] R. Huang, C. Lu, X. Lin, and X. Shen, ''Secure automated valet parking: A privacy-preserving reservation scheme for autonomous vehicles,'' *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11169–11180, Nov. 2018.

[16] S. Woo, H. J. Jo, and D. H. Lee, ''A practical wireless attack on the connected car and security protocol for in-vehicle CAN,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 993–1006, Apr. 2015.

[17] K. An, J. Choi, and D. Kwak, ''Automatic valet parking system incorporating a nomadic device and parking servers,'' in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Las Vegas, NV, USA, Jan. 2011, pp. 111–112.

[18] Daimler. *Driverless in the Parking Lot. Automated Valet Parking*. Accessed: Oct. 2020. [Online]. Available: https://www.daimler.com/innovation/case/autonomous/driverless-parking.html
[19] E. Biba. *What the World Will Look Like Without Drivers*. Accessed: Jan. 2016. [Online]. Available: http://www.newsweek.com/2016/01/22/driverless-cars-and-futuregetting-around-415405.htm
[20] M. C. P. Ferreira, L. M. M. Damas, H. M. F. Da Conceição, P. M. De Andrade De Albuquerque D'Orey, P. Steenkiste, P. E. R. Gomes, and R. J. Fernandes, "Device and method for self-automated parking lot for autonomous vehicles based on vehicular networking," U.S. Patent 2017/0 212 511 A1, Jul. 27, 2017.
[21] H. Shin, M. J. Kim, and C. Crane, "A research on path generating and tracking algorithm for auto valet parking system based on improved sensor performance," *J. Electr. Eng. Technol.*, vol. 2022, pp. 1–12, Jan. 2022, doi: 10.1007/s42835-021-00983-3.
[22] G. G. Varga, A. Kondakor, and M. Antal, "Developing an autonomous valet parking system in simulated environment," in *Proc. IEEE 19th World Symp. Appl. Mach. Intell. Informat. (SAMI)*, Herl'any, Slovakia, Jan. 2021, pp. 373–380.
[23] M. Kneissl, A. K. Madhusudhanan, A. Molin, H. Esen, and S. Hirche, "A multi-vehicle control framework with application to automated valet parking," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 9, pp. 5697–5707, Sep. 2020.
[24] J. Lei, J. Huang, L. Kong, G. Chen, and M. K. Khan, "DeFLoc: Deep learning assisted indoor vehicle localization atop FM fingerprint map," *IEEE Trans. Intell. Transp. Syst.*, early access, Apr. 6, 2022, doi: 10.1109/TITS.2022.3163539.
[25] A. Alqazzaz, I. Alrashdi, E. Aloufi, M. Zohdy, and H. Ming, "SecSPS: A secure and privacy-preserving framework for smart parking systems," *J. Inf. Secur.*, vol. 9, no. 4, pp. 299–314, 2018.
[26] Y. L. Mao, "Research on cross domain authentication of Internet of Things," M.S. thesis, College Comput. Sci. Technol., Univ. Chongqing Univ. Posts Telecommun., Chongqing, China, 2020.
[27] J. Ni, K. Zhang, X. Lin, Y. Yu, and X. Shen, "Cloud-based privacy-preserving parking navigation through vehicular communications," in *Proc. 12th Int. Conf. SecureComm*, Guangzhou, China, Oct. 2016, pp. 85–103.
[28] Y. Lin, J. Li, S. Kimura, Y. Yang, Y. Ji, and Y. Cao, "Consortium blockchain-based public integrity verification in cloud storage for IoT," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3978–3987, Mar. 2021.
[29] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. 27th Conf. Comput. Commun. (INFOCOM)*, Phoenix, AZ, USA, Apr. 2008, pp. 1229–1237.
[30] L. Wang, X. Li, and H. Zhong, "A revocable group batch verification scheme for VANET," *Scientia Sinica*, vol. 43, no. 10, pp. 1307–1325, Oct. 2013.
[31] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017.

LEI HUA received the B.S. and M.S. degrees in information security and computer science and technology from Jiangsu University, Zhenjiang, China, in 2015 and 2018, respectively, where she is currently pursuing the Ph.D. degree in automotive and traffic engineering. Since February 2022, she has been a Visiting Research Student with the Integrated Vehicle Health Management (IVHM) Centre, School of Aerospace, Transport, and Manufacturing (SATM), Cranfield University, Bedford, U.K. Her research interests include security and communication of vehicular networks and intelligent transportation systems.

HAOBIN JIANG received the B.S. degree in agricultural mechanization from Nanjing Agricultural University, Nanjing, China, in 1991, and the M.S. and Ph.D. degrees in vehicle engineering from Jiangsu University, Zhenjiang, China, in 1994 and 2000, respectively.

From 1994 to 1995, he was a Research Assistant with the Laboratory of Power and Energy, Faculty of Biological Resources, Mie University, Mie, Japan. In 1994, he joined Jiangsu University, where he is currently a Professor of vehicle engineering. He is also the Dean of the Automotive Engineering Research Institute, Jiangsu University. His research interests include vehicle dynamic performance analysis and electrical control technology, active safety control techniques and theories of road vehicles, and intelligent transportation technology. He is also a Steering Technology Committee Member of the Society of Automotive Engineering of China, a Steering Technology Committee Member of the National Technical Committee of Auto Standardization, China, and the Standing Director of the Society of Automotive Engineering of Jiangsu.

JIAN XIAO received the bachelor's degree in information security from Jiangsu University, Zhenjiang, China, in 2021. His research interests include blockchain and security in vehicular *ad-hoc* networks.

MOHAMMAD SAMIE received the B.Sc. degree in electronics from the Azad University of Saveh, Iran, in 1997, the M.Sc. degree in electronics from Shiraz University, Shiraz, Iran, in 2002, and the Ph.D. degree in advanced electronics from the University of the West of England, Bristol, U.K., in 2012.

He is currently working as a Lecturer with the School of Aerospace, Transport, and Manufacturing (SATM), Cranfield University, U.K. He is also leading Seretonix, a Secure, and the Reliable Electronic Systems Group, Cranfield University, focusing on the resilience and security of electronics. He has accumulated a wide and varied experience in field-programmable gate arrays (FPGAs) and ASIC design, simulation, verification, and implementation at Toumaz, Didcot, U.K. He was involved with two EPSRC-Funded Projects—NFF and SABRE, where he was responsible for creating most of the detailed designs and implementations. He has published 43 international journals, conference papers, and book chapters, two awarded as the best articles.