Date of publication: April 24, 2025.

A Secure Parking Navigation System for Autonomous Vehicles Communication

ABDULRAHMAN ALAMER[1], SULTAN BASUDAN[1]
[1]Computer Science Department, Engineering and Computer Science College, Jazan University, Jazan, KSA
Corresponding author: Sultan Basudan (e-mail: sbasudan@jazanu.edu.sa).

ABSTRACT This work suggests that sharing data about parking spaces between autonomous vehicles (Aut-Vs) will enhance parking navigation systems and congestion avoidance. For example, if a number of Aut-Vs are ready to share their parking spaces with others before leaving their spots, this will promote parking navigation services' efficiency, reduce time and energy consumption. However, sharing data will result in various challenges, including incentive and security as well as latency issues. For instance, Aut-Vs may not wish to share their data with zero benefit since doing so will incur them more computation and communication efforts and security issues. Therefore, this paper aims to propose a novel security incentive mechanism for improving the parking navigation system for the Aut-Vs paradigm. However, even with low latency and minimal cost, data sharing between Aut-Vs still has mobility issues. For this reason, the fog caching (FC) system has been created to boost data sharing effectiveness while maintaining high levels of mobility and flexibility. This paper has designed a secure incentive mechanism based on an FC network to proposed a secure parking navigation (SPN) system for the Aut-Vs paradigm. The proposed SPN combines auction methodology with attribute-based encryption algorithm to design a secure incentive mechanism which guarantees the security and privacy of sharing parking data. Security analysis shows that our work is able to achieve sharing parking with full guarantee of privacy protection. Performance evaluation also shows that the proposed scheme for the SPN system is highly feasible and scalable.

INDEX TERMS Autonomous vehicles communication, security, privacy, parking navigation system, smart application.

I. INTRODUCTION

Autonomous vehicles (Aut-Vs) are part of the artificial intelligence field that has created the potential for new intelligent driving behaviors [1]. For instance, fully Aut-Vs have the ability to improve our driving by taking the driver out of the loop by relying on navigating itself through reading traffic road data [2]. However, with the growing of vehicle numbers in our cites, Aut-Vs could be facing a serious issue related to finding a vacant parking space in a crowded area, such as malls and sport centers [3]. Due to this annoying situation, Aut-Vs are now forced to circle around parking lots or drive on the road in search of empty spots. In congested places, these vehicles account for 20% of all traffic on average [4]. Serious societal issues, including air pollution, fuel waste, vehicle accidents, and traffic congestion, are caused by this increased traffic [5]. Therefore, many studies have proposed smart parking navigation applications [6] operating on a cloud-based system. Typically, in these applications, an Aut-V that is seeking for a parking area will send a query to the cloud server to discover available parking areas in its destination. However, these studies build their parking application based on a cloud computing system, which it is not recommended for most applications that require real-time services. In fact, parking data have high sensitivity in terms of time expired, where obtaining the data in real time is the key factor for successful parking navigation systems in Aut-Vs. Thus, adopting a cloud system in an Aut-V parking navigation system could lead to the following issues:

- A latency issue. Since the communication traffic between the cloud server and the Aut-V requires a high bandwidth, this will lead to a latency issue. For example, when a number of Aut-Vs are requesting parking data at peak time, the communication between the cloud server and the Aut-Vs could be result in a significant traffic backhaul, which may result in a delay in delivering data to the requester Aut-V. Therefore, a latency issue may lead Aut-Vs to make an inappropriate decision.
- A redundancy issue. For example, the parking space data that are sent to the cloud server could be stored for a long time, by which the server may send it multiple times for

every requester Aut-V without considering the occupied situation of the parking space, especially when a large number of Aut-Vs are requesting parking navigation at a same geographic area (e.g. downtown). The cloud server may then send the same parking spot data to all requester Aut-Vs, by which this may mislead most of them.

- A privacy issue. A cloud server is considered as a not trusted entity, whereby it could be able to identify the requester Aut-V's location and its trajectory. Although numerous works have proposed privacy-preserving parking systems [7] [8] based on cryptography, these schemes require very high computation costsin terms of cryptography algorithms, which will result in a latency issue. For example, the time taken in encrypting data and sending to the cloud server, and then the time taken in requesting and decrypting the ciphertext will exceed the time in finding a vacant parking space.

In regard to the above issues, the sharing paradigm is considered the best methodology for achieving real-time data parking navigation [9]. Thus, for enhancing sharing data systems, recent studies have proved that sharing real-time data is better implemented by a fog caching (F-cache) paradigm [10] [11]. With its temporary data storage, computing, and processing features, F-cache can perform caching techniques to cache the important content data in its cache memory in order to speed up the data communication between two Aut-Vs, at the same time reducing the high bandwidth and the traffic backhaul between the requester device and the cloud server [12]. The basic idea of using F-cache techniques in the parking navigation system is to enable a provider Aut-V to upload its parking space to be cached in the F-cache node's memory in order to directly serve a requester Aut-V in real-time service. Therefore, sharing data with the F-cache system will eliminate the latency issue as well as the data redundancy issue, whereby the F-cache stores the data for just a short time period. Thus, this work exploits the F-cache paradigm in order to design a secure parking navigation (SPN) system with the attribute of a rapid sharing data (RSD) for the purpose of improving the parking navigation paradigm in the Aut-V network system. However, designing a PS with RSD features means having to cope with several challenges. First, in implementing an incentives technique for encouraging sharing data among Aut-Vs, significant investigation is needed in order to find an efficient way of inventively encouraging Aut-Vs to share their parking spaces data with other Aut-Vs. Particularly, when a provider Aut-V feels that sharing parking data with another Aut-V seeking for a parking spot without receiving any compensation is unfair. As a result, incentive mechanisms are significant and require in-depth study. The second major issue with the F-cache paradigm is that it raises issues related to security, trustworthiness, and privacy invasion during sharing data. Finally, the authorized requester Aut-V must not be able to disclose the confidential data of the provider Aut-V, such as vehicle model type, identity, etc. Therefore, significant work needs to be done to ensure that rapid parking data sharing in the designed SPS system doesn't compromise security or violate privacy. Motivated by the challenges above, an auction-based theory is exploited to model a selling parking (sp-auction) mechanism for producing advantageous proprieties such as rapid sharing data with profitability as well as designing an encryption-attribute-based homomorphic matching key (EHMK) to protect driver's privacy during sharing parking data. Based on the sp-auction mechanism and EHMK protocol, this work proposes a secure parking navigation (SPN) system for the Aut-V communication paradigm with RPD feature.

- An auction mechanism is designed as a selling parking (sp-auction) mechanism for encouraging Aut-Vs to profitably share their parking data. In the sp-auction model, the seller Aut-V will draw its strategy for selling its parking space based on its location and leaving time. In contrast, the buyer Aut-V will draw its strategy for buying the parking place based on its budget and time of arriving. Thus, both seller and buyer Aut-Vs are bidding according to their best strategies.
- An encryption-attribute-based homomorphic matching key (EHMK) scheme is designed as a privacy-preserving scheme to protect the seller and buyer Aut-Vs' privacy from being disclosed during sharing parking data. The proposed scheme enables the seller Aut-V to encrypt its parking data with a searchable keyword, which can be selected from a list of predefined searchable keywords. The parking data and keyword ciphertexts will be stored in the F-cache node. The buyer Aut-V can then search for a particular parking space using a corresponding predefined searchable keyword.
- Based on the sp-auction mechanism and EHMK protocol, a secure parking navigation (SPN) system is proposed as an efficient and secure rapid sharing parking data solution to the Aut-V communication paradigm.
- To demonstrate the proposed SPN system's efficiency, an inclusive validation is carried out through performance evaluation and security analysis to demonstrate the capabilities of the proposed sp-auction model and EHMK scheme.

The paper is arranged as follows. Related Work is demonstrated in Section II. Section III provides preliminaries required in this work. In Section IV provides a detailed description of the proposed scheme. Section V then goes with security analysis. Subsequently, the performance is assessed in terms of computational, communication overhead, and security attributes in Section VI. Finally, Section VII concludes the work.

II. RELATED WORK

Finding a parking spot is one of the road transportation activities in the Aut-V paradigm that wastes time and energy, particularly in urban areas. To the best of our knowledge, not much research has been done on the issue of parking spot search methodology in the Aut-V communication system [13]. The majority of literature research have examined parking systems for all non-Aut-V levels.

Numerous parking guidance systems that are not Aut-V have been suggested by VANET-based systems that employ various technologies including image segmentation, deep learning, machine learning, etc. [14] [15] [16]. In addition, since the security and privacy are the key issues that must be handled with during parking navigation exchange. Nonetheless, a number of VANET-based privacy-preserving navigation systems have been put forth to help cars go where they need to go as quickly as possible by taking the right routes.

Three RSUs are able to find open parking places for cars arriving at huge parking lots thanks to a privacy-preserving parking system that proposed in [17]. This parking lot concept is a small-scale project. A VANET-based secure and privacy-preserving navigation strategy was developed by Chim et al. [18]. In this scheme, RSUs placed on highways gather real-time road data and work together to guide vehicles to destinations in a distributive manner. Sadly, because the master key is shared by all vehicles, this technique is susceptible to internal vehicle attacks. Cho et al. [19] suggested a better privacy-preserving navigation protocol to thwart this attack and do away with the need to share the master secret key. As a result, Sur et al. [20] showed that the protocols [19] and [18] are built on the firm presumption that every RSU is completely trustworthy and that the cars would not improperly communicate their credentials with other parties. Therefore the authors [20] in suggested a secure navigation protocol based on proof of knowledge and one-time credential to address these shortcomings.

Nevertheless, the techniques [19], [18] and [20] rely on the premise that a moving vehicle can complete a query with an RSU, which is actually very difficult, especially when the vehicle is traveling at a very high speed.

Thus, in light of our observations, we disprove this presumption and suggest a unique smart parking navigation system that will enable vehicles to access parking services without compromising their privacy. Therefore, in order to obtain the navigation result, we proposed a secure navigation system based on auction method that enable Aut-V to request a parking available information while en route. This approach is better than the current ones navigation systems based on VANET technology in [21] and cloud application system in [22] since it can increase the likelihood that navigation results will be retrieved.

III. PRELIMINARIES

Methodology that are needed for this work are illustrated in this section.

A. BILINEAR MAPS.

It is an admissible bilinear map such that $\hat{e} : G_1 \times G_1 \to G_2$ where G_1 is an additive cyclic group and G_2 is a multiplicative cyclic group that are generated by the same prime order p_o. The $\hat{e}$ has the various properties as illustrated below:

- Bilinear: $\forall\ g_1, g_2 \in G_1$ and $k, y \in \mathcal{Z}^n_{p_o}$, there is $\hat{e}(kg_1, yg_2) = \hat{e}(g_1, g_2)^{ky} = \hat{e}(yg_1, kg_2)$.
- Symmertic: $\hat{e}(g_1, g_2) = \hat{e}(g_2, g_1)$.
- Non-degenerate: $\hat{e}(g_1, g_2) \neq 1_{G_2}$.
- Computable: $\hat{e}$ is computable.

B. COMPLEXITY ASSUMPTION.

The proposed cryptography scheme is designed based on following discrete logarithm problem.

Assumption 1 Computational Diffie—Hellman (CDH) Problem, which is defined as:

Definition 1: Given $(kg, yg, zg) \in G_1, \forall k, y, z \in Z^n_{p_o}$, the CDH assumption holds if an adversary $\mathcal{S}$ has a function $\mathcal{F}$ with a negligible advantage Dv^{DBDH} and a polynomial time *tim* in successfully computing $h = kyz \in Z^n_{p_o}$ and then decides the following problem:

$$Dv^{DBDH}_{\mathcal{S}}(\mathcal{F}) = \left| \begin{matrix} Pr[\mathcal{S}(kyzg = 1)] \\ -Pr[\mathcal{S}(hg = 1)] \end{matrix} \right| \geq tim \tag{1}$$

Assumption 2 Decisional Bilinear Diffie–Hellman (DBDH) Problem, which is defined as:

Definition 2: Given $(kg, yg, zg) \in G_1$, the DBDH assumption holds if an adversary $\mathcal{S}$ has a function $\mathcal{F}$ with a negligible advantage Dv^{DBDH} and a polynomial time *tim* in successfully computing $h = kyz \in Z^n_{p_o}$ and then decides the following problem:

$$Dv^{DBDH}_{\mathcal{S}}(\mathcal{F}) = \left| \begin{matrix} Pr[\mathcal{S}(\hat{e}(g, g)^{kyz} = 1)] \\ -Pr[\mathcal{S}(\hat{e}(g, g)^{h} = 1)] \end{matrix} \right| \geq tim \tag{2}$$

1) Searchable keyword mechanism

This work designed a searchable keyword (SKW) mechanism for improving parking navigation. The proposed SKW defines set of keys $\mathcal{W}$ that are used as a searchable key for each parking location in oder to enable seller Aut-V to offer its location and enable buyer Aut-V to find a particular parking spot in a secure manner. However, SKW mechanism is designed based of a polynomial fitting mechanism that is defined as below.

Definition 3: Polynomial fitting mechanism (PF). Define a set of parking locations as a list of keywords $\mathcal{W} = \{w_1, ..., w_n\}$, the PF function for each $\Gamma(w_i)$ is computed with order n, as follows:

$$\begin{aligned} \Gamma(w_i) &= \left(\frac{\sum_{0 \leq i}^{n} w_{-i} - w_{i+1}}{\sum_{0 \leq i}^{n} w_i - w_{i+1}}\right) \\ &= \tau_1 + ... + \tau_n \end{aligned} \tag{3}$$

For each $\Gamma(w_i)$ will produce a coefficient vector as $\upsilon(w_i) = [\tau_1, \tau_2, ..., \tau_n]$. Based on the SKW and PF mechanism, this work proposed a polynomial searchable keyword (PSK) protocol, which is defined below.

Definition 4: Polynomial searchable keyword (PSK) protocol. Given $\upsilon(w_i)$, vector $\mathbf{W}_i = [w_i, ..., w^n_i]$ and a query keyword $\hat{w}_j$, the PSK function $\Lambda(w_i)$ is achieved as follows:

$$\begin{aligned}\Lambda(w_i) &= \hat{w}_j[\mathbf{W}_i \sum_{i=1}^{n} \upsilon(w_i)] \\ &= \hat{w}_j(\tau_1 w_i) + \hat{w}_j(\tau_2 w_i^2) + ... + \hat{w}_j(\tau_n w_i^n)\end{aligned} \tag{4}$$

Therefore, $\Lambda(w_i) = 1$ if $\hat{w}_j = w_i$. Otherwise $\hat{w}_j$ is not matching and will be rejected.

C. EHMK FRAMEWORK

In this work, we exploit an encryption-attribute-matching key with homomorphic methodology to design the encryption-attribute-based homomorphic matching key (EHMK) as a security and a privacy-preserving scheme. The proposed EHMK is used to protect seller and buyer Aut-Vs private data from being disclosed during performing s-auction model. In the proposed EHMK scheme, a keyword w_i is selected from $\mathcal{W}$ that is defined for the parking area data a dat_i. The keyword w_i will be encrypted with attributes of homomorphic function, which enable buyer Aut-v to performing a matching process between a searchable key w_i and a parking spot while they are encrypted. The proposed EHMK is implemented according to the following four algorithms.

- **KeyG($\Game$):** Given $\Game$ as a security system parameter and return a public and private key (X_i, x_i).
- **HKS ($\Game, w_i$):** Given the security system parameter $\Game$ and a parking searchable keyword w_i, return a parking location ciphertext $\mathcal{P}_i$ for w_i.
- **Searching ($x_j, \hat{w}_j$):** Given a private key x_i and a parking keyword $\hat{w}_j \in \mathcal{W}$, return a searchable keyword $\mathcal{S}_j$, where $(\hat{w}_j = w_i) \in \mathcal{W}$.
- **Matching($\mathcal{P}_i, \mathcal{S}_j$):** Given the parking location ciphertext $\mathcal{P}_i$ and the searchable keyword $\mathcal{S}_j$, return "1" if $(\hat{w}_i = w_i$ and "0" otherwise.

D. AUCTION MODEL

The auction system is a model in which a buyer can buy offers a higher price to obtain a required service from a single vendor.

In the navigation parking system, it is

Obviously, Aut-Vs are more economical vehicles, which they are not interested reservation their parking spot data to other Aut-Vs during its time checking out without any compensation.

Thus, in the effort to optimize payment system and to make Aut-Vs more interactive, this work design a parking selling auction (ps-auction) model for encourage Aut-Vs to sell their parking data before they are leaving to the other buyer Aut-Vs. The proposed ps-auction is defined as follows:

Definition 5: (ps-auction). In the ps-auction, through the auctioneer u_i, a seller Aut-V_i can reserve its a parking data dat_i to an interested buyer Aut-V_j who is offering a higher price pr_i. Indeed, each buyer Aut-V_j has n number of price strategies as $\mathcal{P}r = \{pr_1, ..., pr_n\}$. Each $pr_i \in \mathcal{P}r$ is an optimal strategy $\varphi_i(pr_i)$ for an optimal action of provided dat_i. Therefore, the action function F_a for each strategy $pr_i \in \mathcal{P}r$ guarantees that the price of buying the park data should not exceed the buyer Aut-V_j budget Bdg_j that is defined as:

$$F_a(dat_i) = \begin{cases} 1, & ifpr_i \leq Bdg_i \\ 0, & otherwise \end{cases}$$

Definition 6: (Monotone Equilibrium Strategy [MES]). In the propose *system*, the auction rule F_a is designed as a MES to ensure that a buyer Aut-V_j's price pr_i is monotonically selected as its pest strategy $\varphi_i(pr_i)$.

Definition 7: (Best Strategy). The strategy $\varphi_i(pr_i)$ is called a best strategy if the buyer Aut-V_j's utility $\triangle_i$ is non-negative,

$$\triangle_i[\varphi_i(pr_i), \overline{\varphi_i}(pr_i)] \geq Bdg_i$$

where $\overline{\varphi_i}(pr_i)$ is not the Aut-V_j's best strategy.

E. THE PROPOSED PS-AUCTION ARCHITECTURE MODEL

The proposed ps-auction architecture model is consists of the following process:

- Auction process: The proposed ps-auction model is implemented as the following:
  - Auction entity: The F-cach node is acting as auctioneer who is responsible in initialize an auction session by publishing an available parking spot with its time availability specifications to the public through its web-platform.
  - Bidding entity: Each interesting buyer Aut-V_j selects its best price strategy pr_j based on its budget limitation to obtain the parking spot. Each buyer Aut-V_j sends its bidding value to the auctioneer, which includes its higher price cost to win the session of the auction.
- Selecting winner process: From a number of buyer Aut-V_j bidding values, the auctioneer will select Aut-V_j a higher claimed price pr_j as a winner.
- Payment process: The winner Aut-V_j will be demanding to pay the claimed price before obtaining the parking data.

F. PROBLEM STATEMENTS

For a full guarantee of trusted environment of parking navigation system, this work must addresses the following security issues.

Problem 1. Secure ps-auction: For a trusted auction process, the following two issues must be considered.

- Secure bidding. In the proposed ps-Auction system, the price value pr_i is considered a private data due to that if it is disclosed, it will lead to detect the player's best strategy, which enable other players to build their unfair prices' best strategies. Thus, a malicious buyer Aut-$V_j$may preforming a malicious action to bide with unfair price to win the auction session. For example, a malicious buyer Aut-V_j may eavesdrop on other buyer Aut-Vs price strategies to bide with a higher false price $\hat{pr}_i$ to win the auction session. This malicious behavior will result into non-trusted environment of the proposed ps-auction process.

- Blind Selecting Winner. Given number of buyer Aut-V_j $n = \{1, ..., n\}$, the auctioneer aims to select a winner $j \subseteq n$ without disclosing its price value.

Problem 2. While in the F-cach paradigm, the F-cach node is considered as a semi-trusted node, which can cause serious threat to the stored data in its cached memory. For example, when a seller Aut-V_i sends its parking data dat_i to the F-cach node in order to be perform auction process, the F-cach node has a full authorization to access to dat_i, hence it can easily disclose the Aut-V_i's private data as well as manipulating dat_i for a malicious miss leading buyer Aut-V_j. In addition, F-cach node can disclose the private data of the buyer Aut-V_j that request.

Note that, by solving the *SA* problem, we can ensure that there is no way for malicious Re-V to win the auction game by generating its strategy regarding the other participants player' price strategy $\overline{pr}_i$.

Therefore, the node's t_i^* and c_i^t values must be protected among nodes. Solving the *SP* problem will guarantee the confidentiality of the node's data.

G. SYSTEM ARCHITECTURE

This section will demonstrate the proposed security parking navigation system architecture, which consists of the following components:

- An Authority Server (A-server). It is a trust server that is in charge of generating a set of keywords $\mathcal{W} = \{w_1, ..., w_n\}$ as a predefined for parking areas. Each $w_i \in \mathcal{W}$ is a searchable key that describe a particular parking area for the requester Aut-V. In addition, the A-Server is also responsible for registering and initialization of parking navigation systems.
- A Seller Aut-V i. It is refereed to the vehicle who desire to sell its parking spot before living its spot with for Aut-V j. In fact, the Seller Aut-V i is seeking to obtain a compensation benefits from reserving its parking spot with other vehicle. However, Aut-V i need to register at the A-server first for receiving predefined parking area keywords $\mathcal{W}$ and being part of the parking navigation system as a seller vehicle.
- Buyer Aut-V j. It is refereed to one of vehicle that seeks for buying a parking spot located around its end-destination. The keywords $\mathcal{W}$ will help the buyer Aut-V j for better decision making on its states. Therefore, buyer Aut-V must be a part of the parking navigation system from registering at the A-server for gaining a list of predefined geographic parking keywords $\mathcal{W}$ that will be utilized to search for relevant parking area.
- F-cach node Fc_i. It is responsible for enhancing a navigation system between to vehicles through acting as an auctioneer node.

IV. THE PROPOSED SPN SYSTEM

1) System Setup

The A-server bootstraps the whole service and setups the parking navigation system parameters according to the following process

- Cryptography system parameter. The A-server chooses a security parameter $\Bbbk$, which ensures the security level of the system and determines the prime order p_o of the bilinear groups. It then determines an additive cyclic group G_1 of points with two generator g_1, g_2 and a bilinear map $\hat{e}$ such that $\hat{e}(G_1 \times G_1) \rightarrow G_2$, where G_2 is a multiplicative cyclic group. In addition, it determines a group $Z^n_{p_o}$ of number. Finally, the Authority-server publish the system parameter as $S_p = \{p_o, G_1, G_2, \hat{e}, g_1, g_2, Z^n_{p_o}\}$.
- Geographic regions parameter. The A-server initializes the service geographic regions for a city by pre-defining the points of parking's geographic regions of the city, as shown in Fig.2. For example, generating a set of keywords $\mathcal{W} = \{w_1, ..., w_n\}$ as a predefined for parking areas. Each $w_i \in \mathcal{W}$ is as a searchable key that describe a particular parking area for the both seller and buyer Aut-Vs.

2) Registration

According to the system public parameter S_p, the system entities are in charge to generate their public-private key pair as the following:

- Aut-V registration. Each seller Aut-V_i and buyer Aut-V_j is required to generate their public and private key pairs (pk_i, sk_i). A seller Aut-V_i picks a random $x_{s_i} \in Z^n_{p_o}$ as private key and then computes $X_{s_i} = x_i g_1$ as the public key.Also, each buyer Aut-V_j picks a random $x_{b_j} \in Z^n_{p_o}$ as private key and computes its public key as $X_{b_j} = x_{b_j} g_1$.
- F-cach node registration. Each F-cach node F_{c_i} is required to generate a public-private key pair $(pk_{F_i}, sk_i^{F_i})$ by picking a random $x_{F_i} \in Z^n_{p_o}$ as a private key and computes $X_{F_i} = x_{F_i} g_1$ as the public key. It then sends (pk_{F_i}) to the A-server. Once receive it, the A-server will issue and signs a certificate σ_{F_i} for F_{c_i}, which includes series number, pk_{F_i}, signature algorithm, etc. The certificate is allowed the Aut-Vs to check the validity of F-cach node during auction process.

3) Offering parking spot

When a seller Aut-V_i is willing to sell its parking spot data dat_i before its leaving, it will then generate a spatial parking message $SP_i = (t_i w_i)$, which t_i is a time (when parking spot will be free) and w_i is the keyword of geographic parking area (keyword of parking location). The keyword of parking geocast area $w_i \in \mathcal{W}$ is denoted as a parking searchable key from which it can help a buyer Aut-V_j to find its interested parking space.

However, sending $SP_i = (t_i w_i)$ as a plain text will definitely lead for revealing seller Aut-V_i's location and time of leaving. To prevent the exposure of $SP_i = (t_i w_i)$, seller Aut-V_i will generate a series of encrypted points of interest. It picks a random values $k_i, \gamma_i, \alpha_i, y_i \in Z^n_{p_o}$ as temperate secret keys and compute the following:

- $K_i^1 = k_i g_1$.

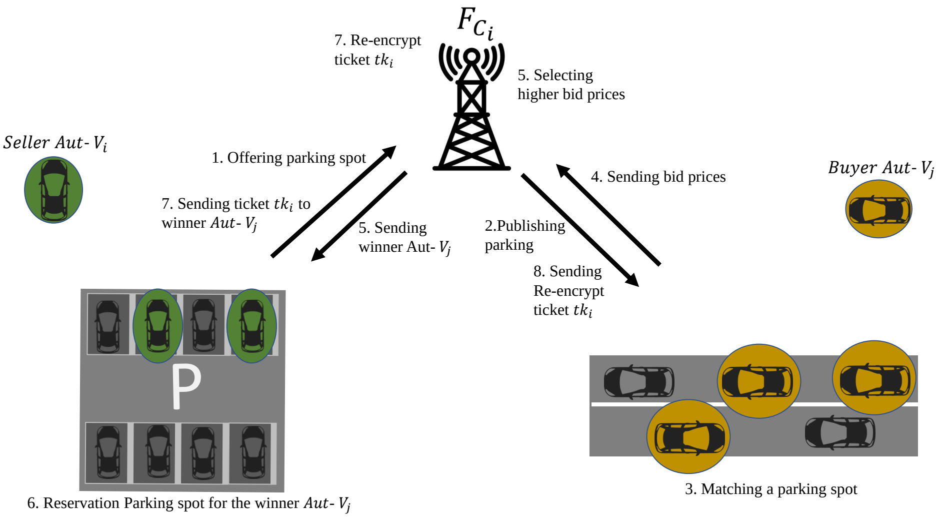
F_{C_i}
7. Re-encrypt ticket tk_i
5. Selecting higher bid prices
Seller $Aut\text{-}V_i$
1. Offering parking spot
7. Sending ticket tk_i to winner $Aut\text{-}V_j$
5. Sending winner Aut- V_j
2.Publishing parking
4. Sending bid prices
Buyer $Aut\text{-}V_j$
8. Sending Re-encrypt ticket tk_i
P
3. Matching a parking spot
6. Reservation Parking spot for the winner $Aut\text{-}V_j$

FIGURE 1. The proposed SPN system

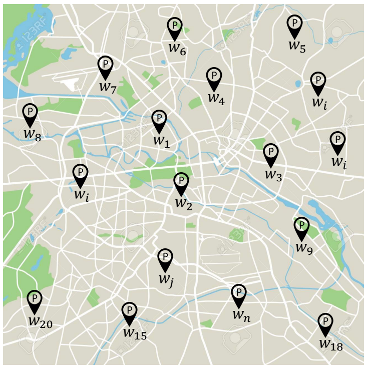

FIGURE 2. Pre-defining the points of parking's geographic regions of the city

- $K_i^2 = \gamma_i g_1$
- $K_i^3 = \hat{e}(g_1, g_1)^{\gamma_i(k_i+w_i)+t_i y_i}$.
- $K_i^4 = [\sum_{j=1}^{n} a_j t_i^{j-1}]\gamma_i K_i^1$.
- $K_i^5 = [\sum_{j=1}^{n} a_j w_i^{j-1}]y_i g_1$.
- $K_i^6 = (K_i^2, K_i^3, K_i^4, K_i^5)$.

The seller Aut-V_i will then send (K_i^6) to the F-cach node F_{c_i}. Once receiving (K_i^6) from Aut-V_i, F_{c_i} will directly post K_i^6 to the public via the navigation parking application or website.

4) Matching a parking spot

A buyer Aut-V_j that is seeking for a parking spot in a certain area and time, it can receives a notification of the posted K_i^6 from F_{c_i}'s parking application or website. Therefore, the buyer Aut-V_j will first check if the K_i^6 is fit in its desired area w_j and time t_j by performing the following:

- $\lambda_j^1 = t_j K_i^4$
- $\lambda_j^2 = w_j K_i^5$

Then, buyer Aut-V_j verifies the following equation:

$$\lambda_j = \frac{K_i^3}{\hat{e}([\lambda_j^1 + w_j K_i^2] + t_j \lambda_j^2, g_1)} = 1$$

If the above equation is true, the buyer Aut-V_j will start sending its price pr_j strategy to the F_{c_i} for inserting pr_j into the auction game and compete with other buyer vehicles on the posted parking spot.

Lemma 1: Matching a parking spot phase is complete if the $t_j = t_i$ and $w_j = w_j$

Proof. $\lambda_j = 1$, since:

$$\begin{aligned}
\lambda_j &= \frac{K_i^3}{\hat{e}([\lambda_j^1 + w_jK_i^2] + t_j\lambda_j^2, g_1)} \\
&= \frac{\hat{e}(g_1, g_1)^{\gamma_i(k_i+w_i)+t_iy_i}}{\hat{e}([\lambda_j^1 + w_jK_i^2] + t_j\lambda_j^2, g_1)} \\
&= \frac{\hat{e}(g_1, g_1)^{\gamma_i(k_i+w_i)+t_iy_i}}{\hat{e}([t_jK_i^4 + w_jK_i^2] + t_jw_jK_i^5, g_1)} \\
&= \frac{\hat{e}(g_1, g_1)^{\gamma_i(k_i+w_i)+t_iy_i}}{\hat{e}([t_j[\sum_{j=1}^n a_jt_i^{j-1}]\gamma_iK_i^1 + w_jK_i^2] + t_jw_jK_i^5, g_1)} \\
&= \frac{\hat{e}(g_1, g_1)^{\gamma_i(k_i+w_i)+t_iy_i}}{\hat{e}([\gamma_iK_i^1 + w_jK_i^2] + t_jw_jK_i^5, g_1)} \\
&= \frac{\hat{e}(g_1, g_1)^{\gamma_i(k_i+w_i)+t_iy_i}}{\hat{e}([\gamma_iK_i^1 + w_jK_i^2] + t_jw_j[\sum_{j=1}^n a_jw_i^{j-1}]y_ig_1, g_1)} \\
&= \frac{\hat{e}(g_1, g_1)^{\gamma_i(k_i+w_i)+t_iy_i}}{\hat{e}([\gamma_iK_i^1 + w_jK_i^2] + t_jy_ig_1, g_1)} \\
&= \frac{\hat{e}(g_1, g_1)^{\gamma_i(k_i+w_i)+t_iy_i}}{\hat{e}([\gamma_ik_ig_1 + w_j\gamma_ig_1] + t_jy_ig_1, g_1)} \\
&= \frac{\hat{e}(g_1, g_1)^{\gamma_i(k_i+w_i)+t_iy_i}}{\hat{e}([\gamma_i(k_i + w_j)g_1] + t_jy_ig_1, g_1)} \\
&= \frac{\hat{e}(g_1, g_1)^{\gamma_i(k_i+w_i)+t_iy_i}}{\hat{e}(\gamma_i(k_i + w_j) + t_jy_ig_1, g_1)} \\
&= \frac{\hat{e}(g_1, g_1)^{\gamma_i(k_i+w_i)+t_iy_i}}{\hat{e}(g_1, g_1)^{\gamma_i(k_i+w_j)+t_jy_i}} = 1
\end{aligned}$$

For protecting pr_j from being disclose, buyer Aut-V_j will generate ciphertext as

$$\rho_j = [(pr_jw_j)g_2]^{\pi_i}$$

Where π_i is the influence factor of the estimate time difference of the Aut-V_j to reach the parking spot. A lower π_i makes the time difference more important. The buyer Aut-V_j will then send ρ_j to the F_{c_i} node.

5) Winner buyer Aut-V_j

The F_{c_i} node is acting as auctioneer that is in charge to sell the parking spot to the buyer Aut-V_j with higher price ρ_j. Therefore, assume that the F_{C_i} node receives a number of $(\rho_j)_{j=1}^n$, it will then start performing an auction process by descendingly sorting $(\rho_j)_{j=1}^n$ as follows:

$$\rho_1 > \rho_2 > \ldots > \rho_n$$

The F_{c_i} node will select the buyer Aut-V_j with a higher price ρ_j and delete the others. The F_{c_i} node will then request from the winner Aut-V_j to make its payment according to its submitted price ρ_j and send a copy of payment receipt pr_j as a encrypted message under seller Aut-V_i's public key. Thus, the winner Aut-V_j

picks a random values $e_i \in Z_{p_o}^n$ as a temperate secret key and compute the following:

- $p_i^1 = e_ix_{b_j}X_{s_i}$
- $p_i^2 = x_{b_j}e_ig_1 \oplus pr_j \oplus \sigma_{F_i}g_1$

It then foreword the received price (p_i^1, p_i^2) to the seller Aut-V_i.

6) Parking Reservation

Once seller Aut-V_i receives (p_i^1, p_i^2), it will decrypt it using its private key, such as,

$$\begin{aligned}
pr_j^{'} &= x_{s_i}^{-1}p_i^1 \oplus \sigma_{F_i}g_1 \oplus p_i^2 \\
&= x_{s_i}^{-1}e_ix_{b_j}X_{s_i} \oplus \sigma_{F_i}g_1 \oplus p_i^2 \\
&= e_ix_{b_j}g_1 \oplus \sigma_{F_i}g_1 \oplus p_i^2 \\
&= e_ix_{b_j}g_1 \oplus \sigma_{F_i}g_1 \oplus x_{b_j}e_ig_1 \oplus pr_j \oplus \sigma_{F_i}g_1 \\
&= pr_j
\end{aligned}$$

Thus, if the pr_j is valid, seller Aut-V_i will reserve the pinking spot by buying a parking ticket tk_i from the parking center and then generate a token as a ticket parking for the winner buyer Aut-V_j. It will pick a random values $r_i, \in Z_{p_o}^n$ as the temperate secret key and perform the following:

- $E_i^1 = r_ix_{s_i}X_{b_j}$.
- $E_i^2 = x_{s_i}r_iX_{F_i} \oplus tk_i \oplus \sigma_{F_i}g_1$

The seller Aut-V_i sends (E_i^1, E_i^2) to the winner buer Aut-V_j via F_{C_i} node. Note that, the seller Aut-V_i's revenue v_i after reserving the parking spot should be satisfying the following condition:

$$v_i = pr_i - tkg_i > 0$$

7) Receiving Parking data

The F_{C_i} will re-encrypt the secret key as $\overline{E_i^1} = x_{F_i}E_i^1$ and sends $(E_i^2, \overline{E_i^1})$ to winner buyer Aut-V_j. Therefore, the buyer Aut-V_j obtains the parking ticket data detail by decrypting E_i^2 using its private key x_{b_j}, such as:

$$\begin{aligned}
tk_i^{'} &= E_i^2 \oplus x_{b_j}^{-1}\overline{E_i^1} \oplus \sigma_{F_i}g_1 \\
&= x_{s_i}r_iX_{F_i} \oplus tk_i \oplus \sigma_{F_i}g_1 \oplus x_{b_j}^{-1}\overline{E_i^1} \oplus \sigma_{F_i}g_1 \\
&= x_{s_i}r_iX_{F_i} \oplus tk_i \oplus x_{b_j}^{-1}\overline{E_i^1} \\
&= x_{s_i}r_iX_{F_i} \oplus tk_i \oplus x_{b_j}^{-1}x_{F_i}r_ix_{s_i}X_{b_j} \\
&= x_{s_i}r_ix_{F_i}g_1 \oplus tk_i \oplus x_{b_j}^{-1}x_{F_i}r_ix_{s_i}x_{b_j}g_1 \\
&= x_{s_i}r_ix_{F_i}g_1 \oplus tk_i \oplus x_{F_i}r_ix_{s_i}g_1 \\
&= tk_i
\end{aligned}$$

Once buyer Aut-V_j arrived to the parking location, it will show the ticket tk_i to the parking center in order to be allowed to park in its reservation spot.

V. SECURITY ANALYSIS

In this section, we will present the security analysis of the proposed cryptography EHMK scheme in order to illustrate the ability of the EHMK scheme in solving security and privacy Problems as descried in Subsection III-F.

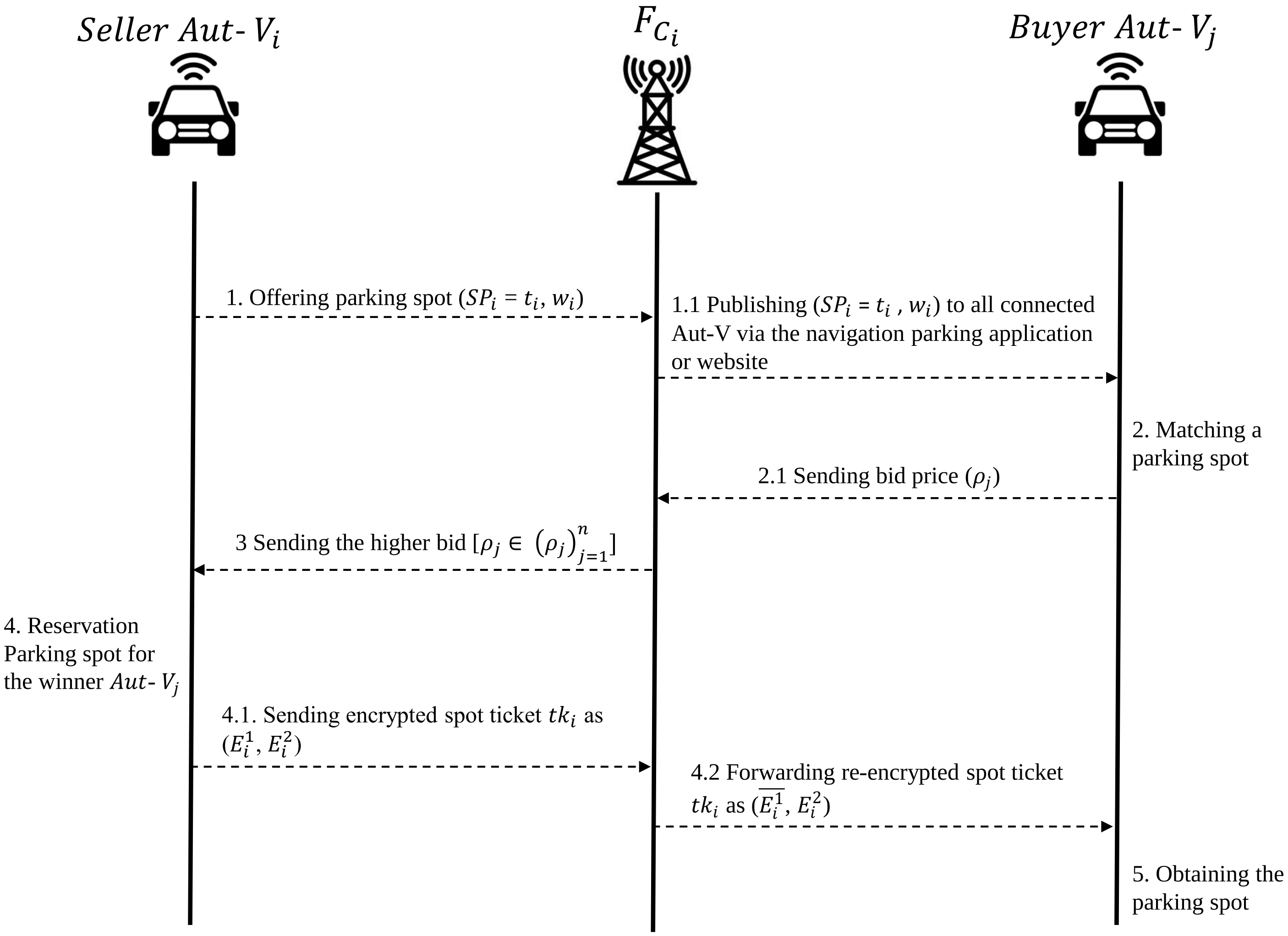
Seller Aut- V_i
F_{C_i}
Buyer Aut- V_j
1. Offering parking spot ($SP_i = t_i, w_i$)
1.1 Publishing ($SP_i = t_i$, w_i) to all connected Aut-V via the navigation parking application or website
2. Matching a parking spot
2.1 Sending bid price (ρ_j)
3 Sending the higher bid [$\rho_j \in (\rho_j)_{j=1}^{n}$]
4. Reservation Parking spot for the winner Aut- V_j
4.1. Sending encrypted spot ticket tk_i as (E_i^1, E_i^2)
4.2 Forwarding re-encrypted spot ticket tk_i as ($\overline{E_i^1}, E_i^2$)
5. Obtaining the parking spot

FIGURE 3. The proposed SPN system

1. Confidentiality and integrity: The proposed EHMK scheme achieves confidentiality and integrity from two perspective as descried below.

- Protecting seller Aut-V data. Before the seller Aut-V_i sending its parking spot data to the F-cach node, it will first protect it. In compliance with Definition 2, the seller Aut-V_i encrypts it spatial parking message SP_i under the *CDH* assumption, which prevents the following a malicious behavior.
    - A malicious F-cach node F_{C_i} will not be able to disclose or even modify the parking data SP_i. Since the sellerencrypts its SP_i under random secure $k_i, \gamma_i, \alpha_i, y_i \in Z_{p_o}^n$ to calculate $(K_{i1}, K_{i2}, K_{i3}, K_{i4}, K_{i5})$.
    - A malicious buyer Aut-V_j will be able to check if the seller parking's data is matching with its requirement by verifying $(K_{i2}K_{i3})$ without disclosing seller Aut-V_i's privacy. Thus, the malicious buyer Aut-V_j will have not chance to disclose or even modify the parking data SP_i.
- Protecting buyer Aut-V_j data. The buyer Aut-V_j sends it price as a ciphertext ρ_j under Definition 2. Thus, a malicious F-cach node F_{C_i} will from disclosing or modifying the real buyer Aut-V_j price pr_j without known the w_j searchable keyword.

2. Secure sorting Computation. Since the proposed EHMK is designed based on a homomorphic concept the a F-cach node F_{C_i} that is acting as an auctioneer will be able to sort bidder vehicles descendly according to their claimed prices without disclosing their real prices.

3. Authentication. The authentication phase is achieved, when the F-cach node authenticated itself by using its digital signature σ_{F_i} on the message that is generated on the p_i^2 copy of payment receipt to be sent to the seller Aut-V_i. The receiver authenticates the source message by using the F-cach node's digital signature σ_{F_i} to obtain the parking token from decrypting $(E_i^2, \overline{E_i^1})$.

VI. PERFORMANCE EVALUATION

This section assesses the proposed SPN performance with the fog catch system. We will first demonstrate the evaluation environment parameter settings. Next, a computational cost and communication overhead analysis will be conducted to evaluate the security and privacy features of the proposed EHMK protocol. In addition, the proposed sp-auction mechanism will be evaluated based on vehicle' participation satisfaction.

A. SPN PARAMETER SETTINGS

The cryptography parameters of the proposed EHMK scheme are implemented a type A pairing with the system security parameter $\Bbbk = 128$ on the elliptic curve $y^2 = x^3 + x$ over the field F_p with prime $p = 3mod\ 4$. The primitives of the cryptography are implemented utilizing JPBC library[1] as well as Java on a PC that has a Microsoft Windows 10 with Intel Core i7-8700 CPU @4.6GHz, 32.00 GBRAM and 1TB of memory.

B. COMPUTATIONAL AND COMMUNICATION OVERHEAD

Any cryptography protocol's performance efficiency must be presented with limiting the assessment of computation and transmission overhead. Therefore, the focus of this part will be on assessing the computation and communication overhead efficiency performances of the suggested EHMK scheme.

1) Computation time Cost

The computational time cost is demonstrated by measuring the time consumption of performing the cryptography operations, which can be measured by counting the number of computing scalar multiplication and bilinear pairing in each system phases. Thus, lets MG and PB are used to defined the time consumption of computing scalar multiplication g_1, g_2 and bilinear pairing $\hat{e}$, respectively. The computation time cost of the proposed EHMK cryptography scheme will be evaluated based on following algorithms:

- Algorithm 1. Offering parking spot. This algorithm takes 4 multiplication operations $4(MG)$ and one bilinear pairing PB for generating a ciphertext K_i^6 for encrypting parking data $SP_i(t_i, Wi)$.
- Algorithm 2. Searching for a parking spot. This algorithm takes 2 number multiplication operations $2(MG)$ and 2 bilinear pairing $2(PB)$ for verifying if the offering parking spot is matching with its searching requirements. Thus, if the verification result is satisfied, the buyer Aut-V_j will continue this algorithm by generation one multiplication operation MG to generate a ciphertext of its offering price ρ_j.
- Algorithm 3. Winner buyer Aut-v. This algorithm takes three multiplication operation $3(MG_1)$ to send a copy of payment receipt pr_j for the winner buyer Aut-V_j to the seller Aut-V_i.
- Algorithm 4. Parking Reservation. This algorithm takes two process as follows:
  - Re-encryption process. In this process, the F_{C_i} requires to compute a multiplication operation MG for generating a re-encrypting the $E_i^1 \rightarrow \overline{E_i^1}$.
  - Decrypting process. In this process, the buyer Aut-V_j takes two multiplication operations $2(MG)$ for decryptying tk_i.

As a result, Table 1 shows the calculation overhead and running time expenses for each approach. It is able to determine that the parking place algorithm offering is using a low computation time cost. This encourage seller Aut-V_i to participate without concerned bout their computation and time costs. In contrast, Searching for a parking spot algorithm consumes more computation cost then algorithm 1. Thus, only the serious buyer Aut-V_j will continue to perform this algorithm.

2) Communication cost

The binary length of the ciphertext is measured to illustrate the communication cost. Therefore, each G_1 or G_2 is measured as 160 bits. In addition, each Z_{qo}^n value or $\{0,1\}$ is equal 256 bits.

In addition, let $|G_1|$, $|G_2|$, $|Z|$ and $|M|$ demonstrate the size of elements in G_1, G_2, Z_{qo}^n and $\{0,1\}$, respectively. Therefore, the ciphertext length size of the proposed EHMK cryptography scheme will be evaluated in each communication phase, as follows:

- Phase 1: In the Offering parking spot, the seller Aut-V_i sends the offering parking data $K_i^6 = (K_i^2, K_i^3, K_i^4, K_i^5)$ to the connected F_{C_i}. Thus, the length size of the K_i^2 is $|G_1|$, the length size of the K_i^3 is $|G_2|$, K_i^4 is $(n|G_1|)$ and the length size of the K_i^5 is $(n|G_1|)$.
- Phase 2: In the searching for a parking spot, the buyer Aut-V_j sends its calmed payment value ρ_j to the connected F_{C_i}, which cost $|G_1|$ of communication length size.
- Phase 3: In the winner buyer Aut-V_j, the F_{C_i} selects the winner buyer Aut-V_j and then sends (p_i^1, p_i^2) to the seller Aut-V_i. Thus, the length size of the p_i^1 is $|G_1|$ and the length size of the p_i^2 is $3|G_1|$.
- Phase 4: In the Parking Reservation, , the seller Aut-V_i sends (E_i^1, R_i^2) to the buyer Aut-V_j. The length size of the E_i^1 is $|G_1|$ and the length size of the E_i^2 is $3|G_1|$.

Therefore, Table 2 illustrates the communication cost for each communication phase in the proposed parking navigation network system with their length bit costs. Overall, the time cost of performing proposed scheme is more practical with stable of communication and computation cost during performing auction process.

[1] http://gas.dia.unisa.it/projects/jpbc/

TABLE 1. Computational cost

	Offering parking	Searching for parking	Winner	Parking Reservation	Receiving parking
Operations	$4MG + BP$	$3MG + PB$	$3MG$	$5MG$	$3MG$
Run Time (ms) with $n = 50$					
Max Time	352 ms	268 ms	45.7 ms	149.7 ms	44.5 ms
Min Time	298 ms	223 ms	37 ms	109 ms	34.90 ms
Avarage Time	348 ms	238 ms	41.9 ms	125.7 ms	38.7 ms

TABLE 2. Communication overhead

	Phase 1	Phase 2	Phase 3	Phase 4
Operations	$(2n+1)\|G_1\| + \|G_2\|$	$\|G_1\|$	$4\|G_2\|$	$4\|G_2\|$
Length size	$2n(160) + 320$ *bits*	160 *bits*	640 *bits*	640 *bits*

C. PERFORMANCE OF SPN SYSTEM

In this experiment, the F-cach node F_{C_i} is acting as auctioneer temporary server, which is in charge of selecting a buyer Aut-V_j for reserving a particular parking spot by considering the level location privacy of both seller and buyer Aut-V_j and the time of performing the auction process. We set up time interval A, B, which A is indicated a period time between (7 to 9) AM mooring and B is a period time between (12 to 2) PM after noon. In addition, we set a range time to performing each auction process determined as $(60ms)$. After this time, the announcement parking spot SP_i will be considered as expired spot and will be removing from the F_{C_i}'s caching memory. Thus, the experiment is contacted as the following scenarios:

- scenario 1. At the A time period, it can note that, the number of buyer Aut-Vs are increased compared with seller Aut-Vs. This is because this time most of people are going to their work place. Thus, having a parking spot is a less chance for bidders Aut-Vs. However, this will positively affect the seller Aut-v satisfaction as shown in Fig.**??**. This is because more buyer Aut-Vs will join the auction system, which in contrast, the seller Aut-V_i will obtain a satisfaction payment for reserving its parking spot, especially if the parking spot is close from most of people work place. In addition, the auctioneer F_{C_i} will be shortly find a buyer Aut-V_j with a higher claimed payment, which reducing the time of auction process as well as the time of caching parking spot in its memory.
- scenario 2. At the B time period, it can note that, the number of buyer Aut-Vs are decreased while the number of seller Aut-Vs are increased. This is because this time most of people leaving their work places. Thus, having a parking spot could be very easy. This will negatively affect the seller Aut-v satisfaction as shown in Fig.5. This is because there is a lack of buyer Aut-Vs will join the auction system, which in contrast, the seller Aut-V_i will obtain a less expected payment for reserving its parking spot. Moreover, the auctioneer F_{C_i} may difficultily find a buyer Aut-V_j with a fair claimed payment, which the time of auction process may increased with the time of caching parking spot in its memory.

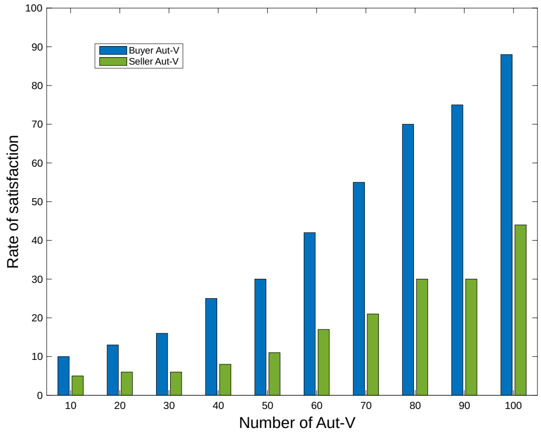

FIGURE 4. Rate of satisfaction between Seller and buyer Aut-Vs

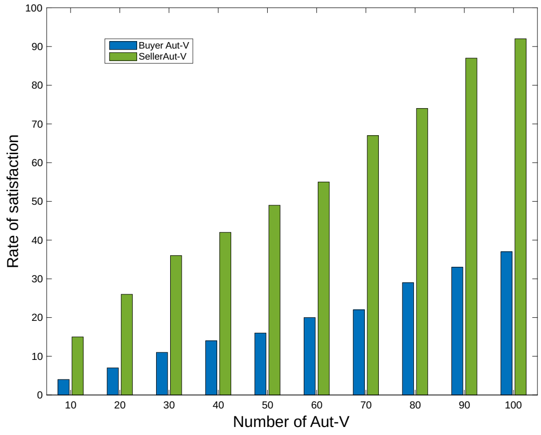

FIGURE 5. Rate of satisfaction between Seller and buyer Aut-Vs

D. COMPARISON

From above scenarios studies, we evaluate the efficiency of the proposed system on a city traffic performance compared with navigation systems based on VANET technology in [21] and cloud application system in [22]. As shown in Fig.6, it can note that the proposed system reduce the searching time of the parking spot by 49% compared with VANET and cloud-based system. The proposed SPN system is efficiently reducing the issue of a city's traffic from helping most of Aut-V owner to find a suitable parking spot before reaching the place. In addition, the Aut-V owner is more satisfied due to save their time from searching for a parking and reducing their gas payment.

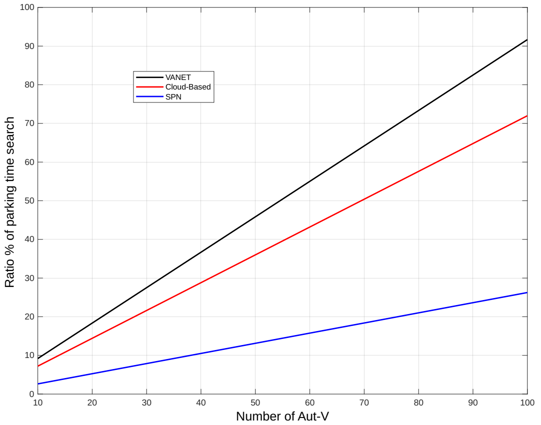

FIGURE 6. Comparison of rate of parking time search

VII. CONCLUSION AND FUTURE WORK

This paper presents a novel security incentive mechanism for improving the parking navigation system for the Aut-Vs paradigm that takes into account sharing data among Aut-Vs at low latency and minimum cost. A fog caching (FC) system has been developed to increase efficiency of data sharing with mobility of high-flexibility. In designing a secure incentive mechanism based on an FC network, we propose a secure parking navigation (SPN) system for the Aut-Vs paradigm. The proposed SPN combines auction methodology with an attribute-based encryption algorithm to design a secure incentive mechanism that guarantees the security and privacy of sharing parking data. Security analysis demonstrates that our work is able to achieve privacy protection in sharing data, and secure search and collusion resistance, while an evaluation on performance illustrates high feasibility and scalability of the SPN system's proposed scheme. Future research should focus on improving security in sharing data such as using blockchain technology taking into account low computation and communication costs.

REFERENCES

[1] M. M. Rahman and J.-C. Thill, "Impacts of connected and autonomous vehicles on urban transportation and environment: A comprehensive review," *Sustainable Cities and Society*, p. 104649, 2023.

[2] C. Ding, C. Li, Z. Xiong, Z. Li, and Q. Liang, "Intelligent identification of moving trajectory of autonomous vehicle based on friction nanogenerator," *IEEE Transactions on Intelligent Transportation Systems*, 2023.

[3] X. Xiao, Z. Peng, Y. Lin, Z. Jin, W. Shao, R. Chen, N. Cheng, and G. Mao, "Parking prediction in smart cities: A survey," *IEEE Transactions on Intelligent Transportation Systems*, 2023.

[4] B. Padmaja, C. V. Moorthy, N. Venkateswarulu, and M. M. Bala, "Exploration of issues, challenges and latest developments in autonomous cars," *Journal of Big Data*, vol. 10, no. 1, p. 61, 2023.

[5] Z. Tian, T. Feng, B. Yao, Y. Hu, and J. Zhang, "Where to park an autonomous vehicle? results of a stated choice experiment," *Transportation Research Part A: Policy and Practice*, vol. 175, p. 103763, 2023.

[6] Y. Jo, J. Ha, and S. Hwang, "Survey of technology in autonomous valet parking system," *International Journal of Automotive Technology*, vol. 24, no. 6, pp. 1577–1587, 2023.

[7] C. Huang, R. Lu, X. Lin, and X. Shen, "Secure automated valet parking: A privacy-preserving reservation scheme for autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11 169–11 180, 2018.

[8] S. Kim, R. Shrestha, S. Kim, and R. Shrestha, "Security and privacy in intelligent autonomous vehicles," *Automotive Cyber Security: Introduction, Challenges, and Standardization*, pp. 35–66, 2020.

[9] J. Cui, F. Ouyang, Z. Ying, L. Wei, and H. Zhong, "Secure and efficient data sharing among vehicles based on consortium blockchain," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 8857–8867, 2021.

[10] J. Xiong, R. Bi, M. Zhao, J. Guo, and Q. Yang, "Edge-assisted privacy-preserving raw data sharing framework for connected autonomous vehicles," *IEEE Wireless Communications*, vol. 27, no. 3, pp. 24–30, 2020.

[11] A. M. A. Alamer, "A secure and privacy blockchain-based data sharing scheme in mobile edge caching system," *Expert Systems with Applications*, vol. 237, p. 121572, 2024.

[12] A. Alamer, "Security and privacy-awareness in a software-defined fog computing network for the internet of things," *Optical Switching and Networking*, vol. 41, p. 100616, 2021.

[13] B. Xia, J. Wu, J. Wang, Y. Fang, H. Shen, and J. Shen, "Sustainable renewal methods of urban public parking spaces under the scenario of shared autonomous vehicles (sav): A review and a proposal," *Sustainability*, vol. 13, no. 7, p. 3629, 2021.

[14] Y. Feng, Y. Huang, B. Li, H. Peng, J. Wang, and W. Zhou, "Connectivity enhancement of e-vanet based on ql-mrsu self-learning energy-saving algorithm," *IEEE Access*, vol. 11, pp. 3810–3825, 2023.

[15] N. I. Sarkar, F. Ahmed, and S. Gul, "Deploying a low-cost wi-fi-based vehicular ad hoc network in a shopping mall parking lot: An empirical study," *Electronics*, vol. 12, no. 22, p. 4672, 2023.

[16] A. Raj and S. D. Shetty, "Smart parking systems technologies, tools, and challenges for implementing in a smart city environment: a survey based on iot & ml perspective," *International Journal of Machine Learning and Cybernetics*, pp. 1–22, 2024.

[17] R. Lu, X. Lin, H. Zhu, and X. Shen, "An intelligent secure and privacy-preserving parking scheme through vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 6, pp. 2772–2785, 2010.

[18] T. W. Chim, S.-M. Yiu, L. C. Hui, and V. O. Li, "Vspn: Vanet-based secure and privacy-preserving navigation," *IEEE transactions on computers*, vol. 63, no. 2, pp. 510–524, 2012.

[19] W. Cho, Y. Park, C. Sur, and K. H. Rhee, "An improved privacy-preserving navigation protocol in $\{$VANET$\}$ s." *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 4, no. 4, pp. 80–92, 2013.

[20] C. Sur, Y. Park, and K. H. Rhee, "An efficient and secure navigation protocol based on vehicular cloud," *International Journal of Computer Mathematics*, vol. 93, no. 2, pp. 325–344, 2016.

[21] G. Li, Q. Sun, L. Boukhatem, J. Wu, and J. Yang, "Intelligent vehicle-to-vehicle charging navigation for mobile electric vehicles via vanet-based communication," *IEEE Access*, vol. 7, pp. 170 888–170 906, 2019.

[22] D. Anand, A. Singh, K. Alsubhi, N. Goyal, A. Abdrabou, A. Vidyarthi, and J. J. Rodrigues, "A smart cloud and iovt-based kernel adaptive filtering framework for parking prediction," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 3, pp. 2737–2745, 2022.