IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 2, 2022, accepted May 9, 2022, date of publication May 17, 2022, date of current version June 1, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3175829

A Secure and Privacy Preserved Parking Recommender System Using Elliptic Curve Cryptography and Local Differential Privacy

AWAIS ABDUL KHALIQ[1], ADEEL ANJUM[2], ABDUL BASIT AJMAL[1], JULIAN L. WEBBER[3], (Senior Member, IEEE), ABOLFAZL MEHBODNIYA[3], (Senior Member, IEEE), AND SHAWAL KHAN[1]

[1]Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
[2]Department of Information Technology, Quaid-i-Azam University, Islamabad 45320, Pakistan
[3]Department of Electronics and Communication Engineering, Kuwait College of Science and Technology (KCST), Doha 35003, Kuwait

Corresponding authors: Shawal Khan (shawalsbbu@gmail.com) and Abdul Basit Ajmal (abdulbasitajmal7@gmail.com)

ABSTRACT The privacy preservation has received considerable attention from organizations as the growing population is apprehensive regarding personal data being preserved. Smart Parking is a parking strategy that combines technology and human innovation in an effort to use as few resources as possible (such as time and space) to achieve faster and easier parking spots of vehicles. Smart parking systems utilize third-party parking recommender systems to offer customized parking space recommendations to its users based on their past parking experience. However, indiscriminately sharing a user's data with a third party recommendation system may expose their personal information. As their activity and node mobility can be deduced from previous paring experience. There are several privacy and security issues in existing systems, such as identity and location disclosure, availability and authenticity issues. Another problem with existing solutions is that most distributed systems need a third party to anonymize user data for privacy preservation. Therefore, this article fills the described research gaps by introducing parking recomender systems using Local Differential Privacy (LDP) and Elliptic Curve Cryptography (ECC). Based on ECC we proposed the mutual authentication mechanism using Hash-based message authentication code (HMAC) to provide anonymity and integrity during communication. Moreover, given the risks to security and privacy posed by untrustworthy third parties. We used LDP which uses the Laplace distribution technique to add noise randomly and eliminates any necessity for a third party for data perturbation. In addition to LDP, we utilized the IOTA distributed ledger technology (DLT) to provide a new level of security that ensures immutability, scalability, and quantum secrecy and decentralized the system. Our experiments demonstrate that, in addition to preserving the driver's privacy and security, our proposed model has low storage overheads, computation, and communication costs.

INDEX TERMS Elliptic curve cryptography (ECC), local differential privacy (LDP), IOTA ledger, parking recommendation system.

I. INTRODUCTION

Since the recent evolution of the Internet of Things (IoT) devices, the intelligent transportation system (ITS) in the Smart city provides smart services to its users. One example of this transition is Smart Parking System (SPS). SPS facilitate both its owners and the users. Many companies have already invested, and many applications have already been proposed in this vital research area [1]–[6]. While sharing parking lot information may benefit users, it also poses security and privacy risks such as authentication, single point of failure, location, and identity disclosure [2]–[7]. As with any other company with users/driver's data in raw form, including sensitive information, security must always come first. The Privacy Act Policy has been published in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 in order to protect vehicle and user information collected by parking services [8].

The associate editor coordinating the review of this manuscript and approving it for publication was Yu-Chi Chen.

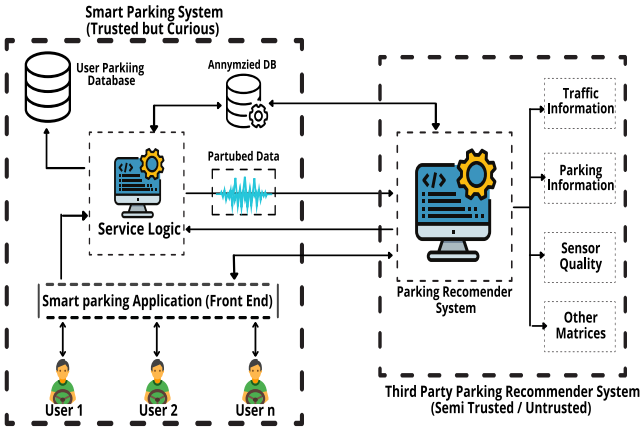

FIGURE 1. Smart parking system using third-party parking recommender system.

In the smart parking scenario, two different types of implementations are often discussed [9], [10]. In the first kind, it is the responsibility of the smart parking application to receive user's requests then recommend the vacant parking lot for the user by itself, this strategy is commonly utilized.

For the second kind, the smart parking application gathers user requests. It sends these to a third-party recommender system, which suggests parking lots based on various factors such as traffic situations, proximity, parking quality, and user experience. Because of the lack of access to a variety of services, a smart parking application will have great difficulty assessing the many factors that go into making parking suggestions for users. Consequently, it is recommended that use the services of third-party recommender systems that are dedicated to achieving these services [11].

The second kind of implementation (recommendations from a third party) mentioned above is the focus of this research. Both implementations acknowledge that the smart parking app is reliable for gathering client requests and establishing a parking database. The second kind of solution, on the other hand, includes a third-party parking recommender system as shown in Figure 1. Since we don't know much about the third-party parking recommender system, we can't say if it's trustworthy; it might be trusted, semi-trusted, or untrustworthy.

The parking database stores the UID (User's Id) and location information (acquired from the customer's query), parking space (collected from the recommendation systems), recent timestamp (the timestamp of the user's request), and user rating (feedback of client after the parking). The purpose of keeping this data in the parking database is to offer users customized parking recommendations based on their previous parking experiences. The parking service provider is trustworthy but curious and can also infer into the user's database to know its mobility patterns.

In the literature, many approaches to address the security and privacy concerns associated with smart parking have been suggested [12]–[14]. Various anonymization techniques also have been developed in the literature, including generalization, suppression, anatomization, pseudonymization, and data masking to protect user's privacy [15], [16]. These data anonymization techniques protect user privacy by removing or modifying identifiers that are used to identify a particular individual in the data. These methods have a high computational and communication cost. In anonymization, reidentification is possible through deanonymization, apart from its high complexity [17], [18]. Due to the low computation overhead in distributed networks, the most appropriate way out to the privacy issues posed by pseudonymization is differential privacy. Noise is added onto raw data via perturbation in differential privacy [19].

In all areas of large data gathering, ϵ-differential privacy is extensively used. The United States Census Bureau, for instance, employs differential privacy for demographic data [20]. Though, there is minimal control over third-party service providers throughout the data collecting phase, which results in regular privacy breaches, such as those that occur on social media platforms such as Facebook [21] and Snapchat [22]. Although such regular privacy disclosures have piqued the public's interest, finding a trustworthy third-party aggregator has proven to be very challenging. The use of conventional differential privacy is limited to a certain degree because of this issue. As a result, where there is no trustworthy third-party service provider, it is essential to examine how to guarantee that private information is not exposed. Some parking service providers have adopted differential privacy [23].

However, these systems have a significant flaw: they need a third party for data perturbation and rely on a centralized system, which is vulnerable to the single point of failure (SPOF) attacks and faces issues like availability. Local differential privacy (LDP) is based on differential privacy protection and was developed due to a significant study into differential privacy [24]. LDP is a strategy that involves perturbing data locally rather than sending it to an untrusted third party (service provider) for aggregation.

In literature, Many authors also proposed blockchain-based solutions to tackle the issues like availability, transparency, and privacy in smart city scenarios such as wireless sensor networks [25], intelligent transportation systems [26], smart grids [27], and eHealth systems [28] but the problem faced by the blockchain network is "Scalability Trilemma" [29] which is defined as the blockchain cannot utilize the property of being "secure," "decentralized" and "scalable" at the same time. It only can utilize two of the three properties. Blockchain systems are also unsuitable for heterogeneous networks such as IoT because of their design issues like high processing time, high fees, and lack of scalability [30]. However, assume the driver discloses the reserved parking lot location to the blockchain. In that case, a system still faces location privacy issues as blockchain cannot tackle it [44].

Furthermore, blockchain validators might not even enable cars to search for parking lots outside their zone [49]. Quantum computers also challenge today's security protocols [36].

It is necessary to develop a model that can maintain data integrity even after a reliable quantum computer has been developed.

The challenges faced by blockchain technology are overcome by IOTA technology. IOTA is a feeless and scalable Distributed Ledger Technology (DLT) that is designed to facilitate frictionless data and value exchange. It is specially designed for microtransactions and Machine to Machine (M2M) economy and is best suitable for IoT devices. IOTA uses a directed acyclic graph (DAG), different from DLT technology used in blockchain, known as Tangle [32].

To conclude, a model for preserving privacy must be presented which assures data protection without the necessity of a third party, maintains confidentiality and integrity even when data remains in the service providers parking database, offers quantum resistance, and distributes computational work across the many entities in the system while retaining strong privacy guarantees.

In this article, motivated by the research gaps in existing literature, we proposed Local differential privacy and ECC based scheme enabled with IOTA DLT to address the privacy and security issues mentioned above. The following are the major contributions we made to this article:

- We proposed the anonymous authentication mechanism for authentication and registration using HMAC to provide anonymity and integrity during the communication. It is resistant against Man-in-Middle (MiM), disclosure, and impersonation attacks, protect communication between users and Key Distribution Center (KDC).
- LDP utilises the Laplace mechanism to change query responses, which removes the need for a third party to do data perturbation. This is because untrustworthy third parties cause a significant threat to both the security and privacy of the user.
- In addition to LDP anonymization techniques, we have presented a model that utilizes the IOTA DLT to provide a new level of security that ensures immutability, scalability, and quantum secrecy throughout the database and protects against a single point of failure issue.
- The trade-off between both privacy and utility is assessed by experimental data drawn through actual parking metrics, allowing users to get parking space suggestions while preserving their privacy. Our experiments demonstrate that, in addition to preserving the driver's privacy and security, our proposed model has low storage overheads, computation, and communication costs.

Following is the structure of this article, section II discusses the preliminaries and required background information, whereas Section III describes related work. The system model, as well as design goals for the system, are explained in section IV. Section V is a detailed explanation of our proposed system. Section VI covers the results of the performance evaluation as well as the security and privacy analysis. Section VII concludes with a conclusion and recommendations for future research.

II. RELATED WORK

Recently, there has been a lot of interest in SPS. Various businesses have set up SPS in various locations across the globe to make it easier to locate available parking spaces for users [1]. For example, ParkMobile [2] and ParkWhiz [4] manages more than 30,000 to 80000 parking lots in more than 200-400 different locations, respectively, throughout the United States. Furthermore, SFpark [5] provides its user's parking reservation services via an online parking system and operates in more than twenty cities of the United States. Many research projects have been undertaken to mitigate the privacy concerns within these systems as they lack privacy protection of its users, including [12]–[14].

The Lu *et al.* [12] suggested a public parking system for large carparks that maintains the anonymity of its users. Roadside units (RSUs) are put in the parking structure in order to collect information from sensors set at parking spots. To be more precise, when a car reaches the parking space, it checks with the help of RSUs to determine if a parking capacity is available. The RSUs will then direct the car to the closest available parking space. The system is primarily concerned with protecting driver's privacy by masking their true identities while communicating with RSUs. To protect user privacy, they have used pseudonymity to obscure the identity of the User. An attacker may still uniquely identify the users via linkage and disclosure attacks. Thus, preserving the explicit identity is insufficient.

The authors, Ni *et al.* [13] proposed a scheme to provide information to drivers, via a cloud server, on where to park, protecting their privacy. According to the method a driver will submit encrypted request to the closest RSU, which contains the driver's current position, destination, and current and arrival timings. Whenever a vehicle reaches an RSU, it delivers an encoded query towards the cloud server, that either decodes it and provides open parking area feedback to the user. Finally, the driver contacts the parking lot using an RSU. However, this method requires that the cloud server knows the driver's current location identities.

A method developed by the Huang *et al.* [12] enables autonomous vehicle (AV) drivers to locate the closest parking lot in real time while maintaining their privacy in their location. The approach hides the identity of the user by the use of pseudonyms that are only used once and cannot be linked together. Also included is a location obfuscation technique, which ensures that the exact location of the AV is generalised over a wider radius, which protects the driver's location privacy. Double-reservation attack occur when a dishonest person obtains numerous parking places without actually parking in them, causing the parking owner financial loss. In order to avoid these threats, the user should double-check that he/she has parked in order to acquire a new pseudonym that may be used for a future reservation request.

The authors of [14] suggest a parking management system that uses group signatures to safeguard the privacy (identities) of its users. Cloaking methods are also employed as an extra security measure to guarantee that a specific user's

location is not disclosed. In this model, parking space is distributed over a large geographic area, known as the cell, and service providers are given parking lot choices, which are then passed on to drivers, who submit requests for parking options from a particular location within the parking lot. The service provider employs a HashMap method. According to the scheme, all available parking spaces are kept in a hash tree to ensure effective and rapid matching between driver inquiries and parking owner's offers. Furthermore, vehicles pay parking costs using anonymous digital coupons generated by a third-party server and distributed by a centralized server.

A blockchain-based parking system is proposed by the authors in [34] and [47], which considers public parking with a high number of accessible parking spaces while not taking driver's privacy into consideration.

A public-key encryption method known as ECC, developed by the authors in [1], is used to protect the smart parking's privacy. This scheme is platform-independent and appropriate for resource-constraint devices. To ensure privacy, the authors utilized zero-knowledge proofs, which prevent the sharing of sensitive information. The authors of [1] and [12] examine the run-time and storage overhead to evaluate performance, but they did not consider the privacy and utility trade off of the system they proposed. The smart parking systems [2], [12], and [14] are all administered by a centralized server, making them vulnerable to SPoF as well as the issues related to limited transparency and accountability. The smart system outlined in [7] does not safeguard drivers' precise location privacy. However, it also discloses detailed geo-location data, which may be useless if the coarse location region just has a few parking lots. The location obfuscation scheme used in [12] and [14] reduce the precision with which nearby parking lots are picked.

W.A.Amiri *et al.* [42], [43] proposed a smart parking system using blockchain in which the author used cloaking technique to generalize the cars locations into cloaking area to preserve the privacy of the drivers. Some parking service providers have adopted differential privacy such that Y. Saleem *et al.* [23]. However, these systems have a major drawback that they need a third party for data perturbation and rely on a centralized parking management system or server, are prone to SPOF attacks, and face issues like availability. In [46] Tingting Fu *et al.* proposed vehicle assignment in the Parking sharing system by using homomorphic cryptography but it has significant issue of single point of failure.

The above-mentioned privacy-protection schemes first focus on the User's actual location or even navigation details and preserve privacy by only using encryption, cryptography, or pseudonymity techniques that are susceptible to privacy leakage via linking and disclosure attacks. While focusing on privacy preservation via LDP, we also used ECC to offer anonymous authentication with the IOTA DLT to guarantee security and reliability.

III. PRELIMINARIES

This section provides background information on IOTA and the other cryptographic primitives used in our system.

A. ELIPTIVE CURVE CRYPTOGRAPHY

Cryptography Using Eliptive Curves (ECC) is indeed a sort of public cryptography employing elliptic curves and hence requires fewer keys than non-elliptic curve encryption such as RSA. Among public-key cryptosystems, it may be suitable for constrained settings. In various areas, the (ECC) protocol is very useful in securing communication among multiple entities. The interaction between many players in a system involving several actors and interacting with them for specific goals must be safe and efficient. Participants in the data-sharing system may benefit from ECC's secure mutual authentication provided by the system. Various ECC protocols, such as the EC-Diffi-Helman (ECDH) key exchange protocol, are used to establish secure sessions between the involved parties. It is necessary to first agree on domain parameters that would subsequently be used in protocol design. Because points a and b are located on the curve's coordinates eq (1), the points on the curve must fulfill the corresponding elliptic curve eq (2).

$$4a^3 + 27b^2 \neq 0 \tag{1}$$

$$ECp(a, b) : y^2 = x^3 + ax + bmodP = 0 \tag{2}$$

B. LOCAL DIFFERENTIAL PRIVACY

LDP may be used to a number of data collection settings, including frequency estimation, heavy hitter detection, and frequent item mining. Google [37], Apple [38], as well as other companies in a variety of industries, have chosen LDP techniques to collect clients' default browser webpages and search engine priorities, which can then be used to identify harmful or malicious interception of personal preferences [38] and thus to find the most commonly used emojis or phrases. LDP adds noise to sensitive data locally before transmission rather than sending it to a third party (typically a service provider). Each User uses a randomized algorithm for data value u to get u' for a database D. A third party cannot infer the input from the pair of values u and u' for any potential output value u *. Instead of getting raw data u from each user, the service provider now receives perturbed data u'. As a result, LDP offers privacy assurances, still, the third parties that collect the data may conduct and disclose statistical calculations (mean value, frequency distribution, and so on) for data publishing [36].

Definition 1 (ϵ-Local Differential Privacy): A randomized algorithm L ensures local ϵ-differential privacy, such that for two dissimilar data input elements $u, u' \in D$ in addition to any potential output u^*, we have

$$Pr[L(u) = u^*] \leq e^{\epsilon} Pr[L(u') = u^*] \tag{3}$$

Using this concept of ϵ-LDP shown in eq (3), it can be shown that LDP works with the outputs of the L algorithm

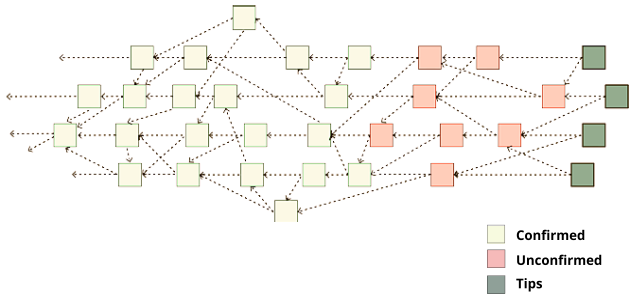

FIGURE 2. IOTA ledger.

when two data inputs, u, and u', are provided. Even after viewing the result u^*, the adversary is unable to tell whether the input to this output was the value u or the value u'.

The privacy and utility trad-off is defined by factor ϵ. The term ϵ (privacy budget) is used in both the differential privacy and the LDP. e^{ϵ} shows that a smaller value of ϵ, indicates more privacy at the expense of utility, while $\epsilon = \infty$ indicates no privacy at the cost of maximum data utility.

In case $\epsilon = 0$:

$$e^{\epsilon} = e^{0} = 1$$

As a result, $\epsilon = 0$ offers perfect privacy.

C. IOTA

Distributed Ledger Technologies (DLT) without relying on a central authority can provide scalability, privacy, and an important facilitator for IoT. The Internet of Things Application (IOTA) [36] uses its own DLT, known as Tangle. Its primary focus is on microtransaction infrastructure for the IoT universe with no transaction fee, high performance, and instant transfer in a lightweight manner [36]. IOTA structure is different from Blockchain and tangle is a directed acyclic graph (DAG) that stores various kinds of information in the form of transactions connected by edges, rather than sequential blocks. An instance of such a graph is illustrated in Figure. 2. In IOTA, every new transaction has to verify two previous transactions to compute a small amount of proof of work (computational work). Verification process In Tangle is different from Blockchain as it has no miners, but members operating on it are, and a verified transaction is transmitted to the entire network. IOTA is more decentralized than Blockchain because all members receive the same rewards and incentives, and there is no hierarchy of responsibilities in Tangle. When using a weighted random walk, cumulative weight is utilized to calculate the number of approvals, and hence higher the cumulative weight, the more approvers there are. Furthermore, in the network, all members use the Markov Chain Monte Carlo (MCMC) protocol to choose which path to take. The network becomes stable, more scalable, and quicker with time, and the path becomes secure over time because as long as more members add more Proof of Work (PoW) from added transactions, most members follow the same path.

IV. NETWORK/THREAT MODELS AND DESIGN GOALS

The network model, threat framework, and project goals of this system are described as follows.

A. NETWORK/SYSTEM MODEL

Our network architecture, as shown in Figure 3, is comprised of four entities: a key distribution centre (KDC), a smart parking system (SPS), also known as a parking service provider, a recommendation system, and users/drivers.

- **Key Distribution Center (KDC):** The KDC initializes the whole system, including the registration of drivers and parking providers, creating public parameters for cryptography, and distributing keys. The KDC serves only as a system initializer but does not handle parking facilities. Thus its function does not clash with the system's decentralization. In practice, the KDC might be the government authority (Ministry of Transport, Metropolitan Corporation, or Capital Development authority)
- **Users:** Users are drivers which uses smartphone application, registered with KDC, perturbed its data (location, timestamp, parking ID, Rating) before communicating with SPS and retrieve parking recommendations from the parking service provider.
- **Smart Parking System (SPS):** The parking service provider, commonly known as SPS, is responsible for managing parking services such as recommendations, aggregates users perturbed data share it with the third-party recommendation system to get the personalized parking recommendations and maintain User's historical data on IOTA DLT. SPS is trusted but curious, which may or may not infer the sensitive information of the user/driver.
- **Parking Recommender System:** It is a semi-trusted or untrusted third-party recommendation systems system which makes suggestions based on a range of parameters (such as parking and traffic statistics, as well as sensor quality).

B. ADVERSARY MODEL & SECURITY THREATS

It is safe to trust the KDC since it is owned and managed by the government, which is concerned about the security and privacy of the users and owners of the smart parking system. So in our scenario, KDC is assumed to be trusted. However, external attackers may try to get system access in order to receive parking recommendations without registration. Additionally, attackers may eavesdrop upon conversations in the system in order to know sensitive information about drivers, or they could perform impersonation or forgery attacks against drivers to obtain information about them. Users may also try to misuse the system while remaining anonymous and try to pollute the reputation rating by evaluating events that did not happen. The primary adversary in our system as shown in Figure 4 is a third-party recommendation system which is not trusted because we know very little

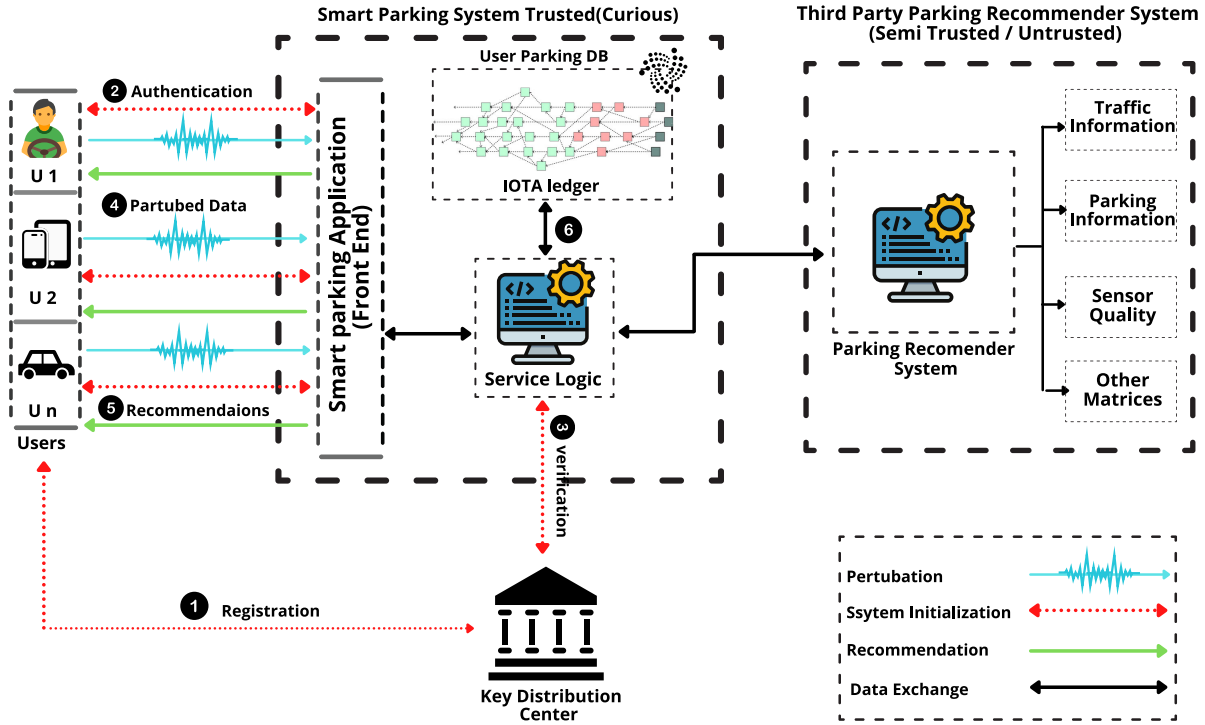

FIGURE 3. Proposed system model.

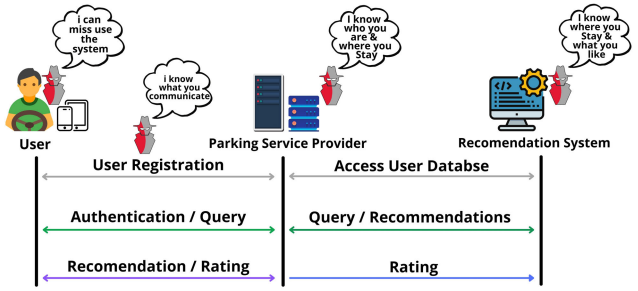

FIGURE 4. Adversary model.

about it, and it may or may not infer the user's sensitive information or monitor its life habits and movement patterns. The system is susceptible to a disclosure attack because of the historical parking database that it has in a centralized server. Thus, the parking system must protect its users' privacy by preventing an adversary from identifying them through their unique parking id or reputation score.The smart parking system is trusted but curious in our scenario, and an internal user may also be interested in the User's sensitive information. We also assume that the attacker has access to a stable quantum computer that can be utilized to break both symmetric and asymmetric encryption protocols effectively. Shor's algorithm, when employed in combination with a stable quantum computer, has the potential to break conventional cryptosystems. The system must preserve privacy and protect users' real identities and sensitive information.

C. DESIGN GOALS

- **Decentralization:** To prevent performance degradation and a Distributed denial of service (DDoS) attacks, the system should be decentralized and not governed by a central authority.
- **Preserving drivers privacy.** To preserve users' privacy, we have set the following objectives for our system.
  Driver anonymity. The actual identities of the drivers should be secured from other entities such as SPS, parking recommendation system, as well as external threats, nobody should be able to deduce the driver's true identification from the information he transmits.
  User/Driver untraceability. Even if the driver's true identity is being preserved by masking it, it is feasible to deduce the driver's identity by following the driver's movements, reputation score or timestamp of the parking. Therefore, our proposed scheme should be capable of accomplishing the following objectives.
  1) A smart parking application, a parking recommendation system, and external adversaries cannot access the drivers' previously visited places or parking information (e.g., preferred parking destination, rating score).
  2) Any system entity should not link the messages of available parking inquiries and at different times.
- **Anonymous Authentication:** Only authorized users can anonymously use the parking services (i.e., get recommendations and provide ratings) without disclosing their real identities.

- **Accountability:** The central authority (KDC) should verify the registered User and parking service providers. In the case of a disagreement, KDC ought to be authorized to invalidate the drivers' true identity.
- **Man-In-Middle Attack:** Message Authentication Code (HMAC) is an authentication code that protects the identity of the devices being authenticated. It is impervious to Man-in-the-Middle (MiM) cyber-attacks and can encrypt connections involving KDC and Users throughout the registration process.
- **Disclosure Attack:** The keys for the sessions between the entities should not be used for the next sessions because and the KDC should generate the fresh keys after each verification of the user so that the user can not be uniquely recognized with any of its derivatives. No entity can disclose users personal information in the system and during the message exchange.
- **Impersonation Attack:**The adversary should not be able to perform an impersonation attack to pretend as a legitimate user to avail the system services illegally. The anonymous credentials can not be used more than once in the authentication process so that the adversary can not use the credentials to impersonate himself.
- **Background Knowledge Attack:** The personal information such as user ID and user mobility patterns such as parking location should not be linked together on the basis of historical database or background knowledge to uniquely identify the user in the system.
- **Quantum resistance:** The system should be resistance against the quantum computing attacks and the attacker should not compromise the system even after the enough resources such as quantum computer.

V. PROPOSED SYSTEM

In this section we present our ECC based anonymous authentication protocol for smart parking recommender system with privacy preservation through LDP and IOTA DLT.

A. OVERVIEW

In our proposed system,as shown in Figure 3 the entities involved are KDC, users/drivers,SPS, and third-party recommender system. The users have installed the SPS app on their smartphones and have sufficient resources to perform less computationally expensive tasks such as simple LDP computation, but not enough to maintain the IOTA ledger. A SPOF might compromise the SPS also pose security threats to all the user's historic data if attacked or compromised. So data should not be maintained in its raw form in parking database. The IOTA ledger is utilized to avoid attacks such as a SPOF and also provide quantum secrecy and decentralized the system. Our system consists of registration and authentication phases, data perturbation through LDP, and IOTA DLT maintenance phases. In the first step of the *Initialization* and *RegistrationPhase* as presented in Figure 5, the user will request the KDC for anonymous credentials $FID\upsilon_i$ with his real $ID\upsilon_i$ and KDC will initialize the system, which is responsible for distribution of keys among users. The primary notations and their description is given in table 1. Once the user gets the anonymous keys $FID\upsilon_i$ the user will request for the parking services to the SPS with anonymous credentials $FID\upsilon_i$. In the Authentication Phase, after successfully authenticated, the user will be able to use the parking services such as nearest parking recommendations. During the data perturbation phase, each user/driver perturbs their sensitive data individually in a local setting before submitting it to the service provider for aggregation. Then after aggregation, the statistical record or results are shared with the third-party recommendation system via IOTA DLT for recommendations. The SPS will maintain IOTA DLT; after the User successfully rating the recommended parking lot, the User historical data is stored in the database and shared to the IOTA ledger.

TABLE 1. Notations.

Notation	Description
EC_p	Eliptive Curve
SPS	Smart Parking System
α	Primitive Element
υ_i	User
KDC	Key Distribution Center
FID_{υ_i}	Anonymous Credentials
Q(a,b)	A generator of Elliptic Curve
SK_{KDC}	The private key of KDC
PK_{KDC}	The public key of KDC
H(.)	Hash Function
$Z*_p$	Multiplicative Cyclic group
ID_{υ_i}	Driver Real ID
SK_{υ_i}	User private key
T	Timestamp
$\|\|$	Concatenation
M'_{υ_i}	User encrypted message with Users' SK_{υ_i}
M'_{KDC}	KDC encrypted message with $HMAC$
D_i	Number of attribute
E	Encryption
D	Dataset
$HMAC$	Hased based message authentication protocol
μ	Original Dataset
μ'	Perturbed data
ϵ	Privvacy Budget (epsilon)
L	Randomize algorithm

B. AUTHENTICATION AND REGISTRATION PHASE

In this phase, an Elliptic Curve ECp is considered that produces a set of elliptic curve points ECp with the point $Q(a, b)$ upon that curve, which is a primitive element α. The order of curve $\#E - 1$ over the prime field is $P - 1$ which defines the total number of points on the curve. The point Q is a generator of EC such that $n.Q = \Theta$, *where* Θ is the point of infinity or zero, which defines the order of the ECp. As both points a and b lie on the co-ordinates of the curve, the condition in eq 1 is satisfied for the given non-singular Elliptic curve in 4:

$$ECp\,(a, b) : y^2 = x^3 + ax + b \,mod\, P \neq 0 \qquad (4)$$

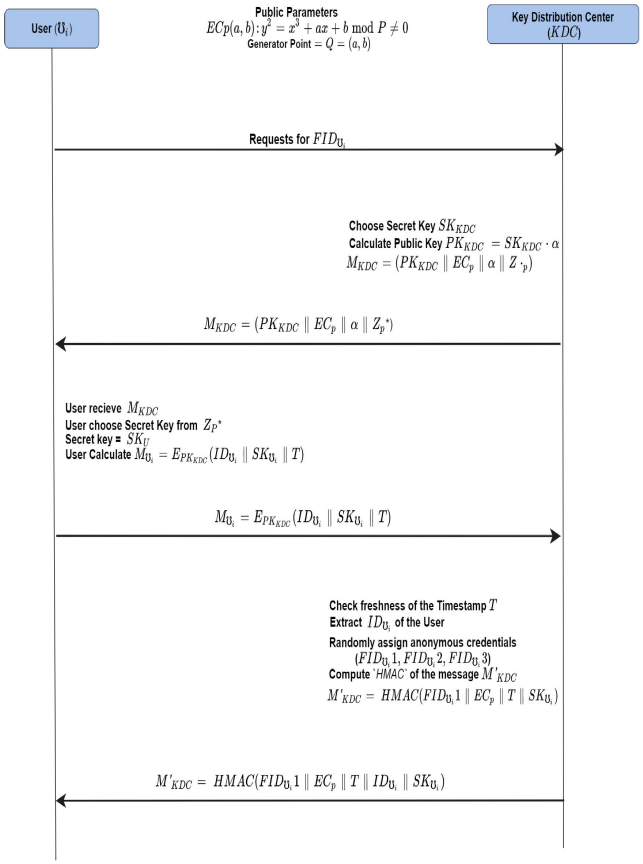

FIGURE 5. Registration process.

1) SYSTEM INITIALIZATION AND REGISTRATION PHASE

The User υ_i first directly sends a request to KDC for anonymous credentials $FID\upsilon_i$. The KDC selects the Elliptic Curve EC_p of prime order with a primitive element or generator $Q(a, b)$ of the curve. The KDC chooses a random number or secret key SK_{KDC} as shown in eq (5) and computes the public key PK_{KDC} which is a shared secret between the User and KDC.

$$PK_{KDC} = SK_{KDC} * \alpha M_{KDC} = PK_{KDC} \parallel EC_p \parallel Z*_p \quad (5)$$

Then KDC sends M_{KDC} to User υ_i, now υ_i compute its secret key let say SK_{υ_i} from $Z*_p$ then υ_i send M_{υ_i} encrypted with KDC public key PK_{KDC} which includes his real ID_{υ_i}, secret key SK_{υ_i} as well as Timestamp T and directs it toward the KDC as shown in eq (6). The KDC computes the hash of the ID_{υ_i} here we assume that hash function H(.) is the same on both sides.

$$M_{\upsilon_i} = E_{PK_{KDC}}(ID_{\upsilon_i} \parallel SK_{\upsilon_i} \parallel T) \quad (6)$$

Upon receiving the parameters as illustrated in Figure 5, the KDC first decrypt M_{υ_i} using its secret key SK_{KDC} and check the freshness of timestamp T, and extract the ID_{υ_i}. After extracting ID_{υ_i} the KDC randomly assigns anonymous credentials let say $FID_{\upsilon_i}^{[1]}$, $FID_{\upsilon_i}^{[2]}$, $FID_{\upsilon_i}^{[3]}$, to the υ_i, and KDC sends the calculated $FID_{\upsilon_i}1$, T, and SK_{υ_i} with calculate an $HMAC$ of the message M'_{KDC} to the User which is shown in

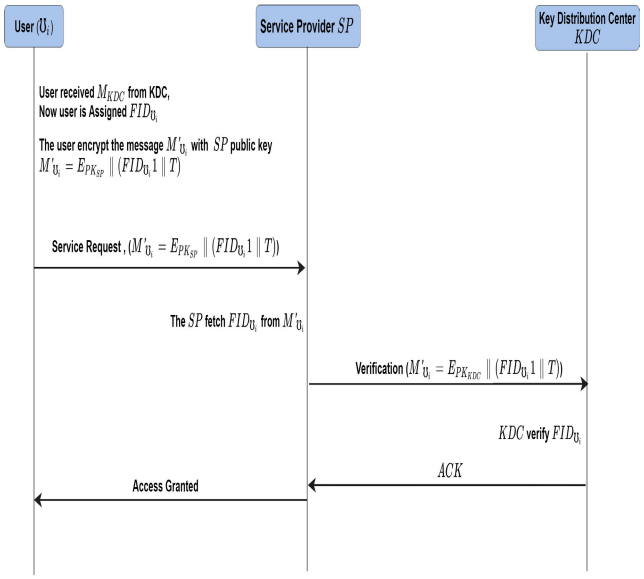

FIGURE 6. Authentication process.

eq (7). The KDC stores $\{ID_{\upsilon_i}, FID_{\upsilon_i}, T\}$ in a tracker list and then reverts back, this database is being used to determine the signer whenever KDC verifies a signature.

$$M'_{KDC} = HMAC(FID_{\upsilon_i}^{[1]} \parallel EC_p \parallel ID_{\upsilon_i} \parallel T \parallel SK_{\upsilon}) \quad (7)$$

The user receives M'_{KDC} from KDC, now User has FID_{υ_i}

2) AUTHENTICATION PHASE

As shown in the Figure 6, the User sends M'_{υ_i} to SPS for authentication.

$$M'_{\upsilon_i} = E_{PKSP}(FID_{\upsilon_i}^{[1]} \parallel T) \quad (8)$$

The SP fetch $FID_{\upsilon_i}^{[1]}$ and verifies it from KDC as represented in eq (8) after verification the access for the parking service is granted to the User. Note that the anonymous credentials $FID_{\upsilon_i}^{[1]}$, are only used once for authentication/reservation to avoid a linking attack. After each verification of $FID_{\upsilon_i}^{[1]}$, from KDC, the User will get new $FID_{\upsilon_i}^{[2]}$,and then $FID_{\upsilon_i}^{[3]}$, upto $FID_{\upsilon_i}^{[n]}$, and this process goes on as presented in eq (9).

$$M'_{KDC} = HMAC(FID_{\upsilon_i}^{[n]} \parallel EC_p \parallel T \parallel SK_{\upsilon_i} \quad (9)$$

In case of any dispute, the SP will share the corresponding FID_{υ_i} of the υ_i to KDC, and KDC will revoke the M_{υ_i} and extract the actual ID_{υ_i} and match User FID_{υ_i} from the tracing list, the list gives plenty, such as negative points on his driving license to the υ_i according to predefined rules.

C. LOCAL DIFFERENTIAL PRIVACY

In our proposed scheme, each user υ_i, when connected with a Service Provider SP, in a specific timestamp T, has some data value u. u consists of K number of attributes, A_i, which include (*Timestamp*, *Location*, *Rating*, *Parkingspace*), etc as shown in eq (10).

$$K_i = A_i, A_{(i+1)}, A_{(i+2)}, \ldots A_m \quad (10)$$

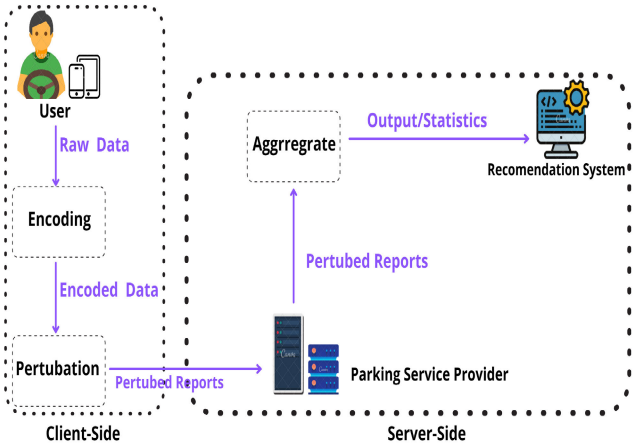

FIGURE 7. Client and server-side LDP process diagram.

When the user establishes a connection with SP at each timestamp T_i. It produces some data μ_i, which is stored in the SP database. This data μ_i has to be submitted to SP and then perturbed before being transmitted to the third-party aggregator. Under different distributions, we used the same methodology as that proposed in [39] by employing the count sketch [40] and Laplace mechanism [36] to reduce space-time complexity and computational overhead while obtaining high data utility. The protocol includes two parts: the client-side, the local perturbator, and the other are server-side, which is the aggregator. The process of encoding and perturbation is done on the client-side, and the server performs the aggregation process on the server-side as shown in Figure 7.

1) CLIENT-SIDE ALGORITHM

The client-side performs the perturbation, and each tuple is encoded to avoid data leakage by a randomly selected hash function. Each piece of encoded value produces a perturbed report by applying the Laplace mechanism, which fulfils the concept of ϵ-local differential privacy. Algorithm 1 illustrates the particular steps on the client side.

In Algorithm 1, the H is the number of hash functions, the privacy budget is ϵ, and m is the hash length of the mapping value; these parameters must pass before deploying the algorithm. The local sensitivity of adding Laplace noise in the one-hot encoding vector v is at most 2 [41], meaning that any two different bits of data will have at most two variations in vector v. Algorithm one sends the perturbed report $u_i j, x'$ that has randomly chosen index j of hash function and noise x' (hashed map position) and by setting an all-zero vector of size m in line 1. It, then in lines 2-4 it selecting the hash function H and hash mapping on the vector v by randomly selecting v and H, where $v_{hj}(u)$ denotes choosing the function j to hash value u. Furthermore, it adds the Laplace noise in lines 5-7, the mapping vector has a length of m, which is already known. If the value of x' is higher than or equal to m, the noise mapping position x' will equal $x' - m$; otherwise, the noise mapping position x' will equal $x' + m$ if the value of $x' <= 0$. In line 8, the algorithm sends a perturb data report υ_i.

Algorithm 1 Client-Side Laplace Count Mean Sketch Algorithm

Input: $u \in D, \epsilon, m, H$ (R)
Output: Perturb Data u'_i

1: Start
2: Vector Initialization $v \leftarrow \{0\}^m$.
3: Randomly select sample j from $[k]$
4: Set $v_{hj(u)} \leftarrow 1$
5: Represent position of mapping bit x
6: Laplacian noise addition $x' = x + Lap\left(\frac{\Delta s}{\epsilon}\right)$
7: Round x'
8: **if** $(x < 0)$ **then**
9: $\quad x' = m + 1$
10: **else if** $(x \geq m)$ **then**
11: $\quad x' = x' - m$
12: **end if**
13: **return** $u'_i \{j, x'\}$
14: End

Each user will send its perturb data report υ_i to the smart parking service provider SP for data aggregation with $O(1)$ time and $O(k + m)$ space complexity.

2) SERVER-SIDE ALGORITHM

Once the server receives the perturbed reports υ_i from the client, it performs aggregation and produces statistics for the recommendation system. The aggregator creates a mapping matrix and keeps track of each value mapping location, accumulating information under various hash functions. The server gets the estimated frequency value by using count mean sketch matrices. Algorithm 2 illustrates the particular steps on the server-side.

Algorithm 2 Server-Side Laplace Count Mean Sketch Algorithm

Input: report $R_i = \left\{j^{(1)}, x^{(1)}\right\}, \ldots \left\{j^{(n)}, x^{(n)}\right\}$
Output: Calculates the frequency of data values $\int(u)$

1: Start
2: Initialization of Sketch $S = \{0\}^{(k*m)}$
3: **for** i `in Range` $(0, n)$ **do**
4: $\quad S\left[j^{(i)}\right]\left[x^{(i)}\right] = 1$
5: **end for**
6: **for** u `in` $(0, |D|)$ **do**
7: $\quad$ **for** j `in` $(0, k)$ **do**
8: $\quad\quad \int(u) = \frac{\sum_j^i S[J]|H_j(u)|. \int_{-\infty}^{\infty} \frac{\Delta s e^{\frac{-|y|s}{\Delta s}} dy}{2e}}{\int_{-1.5}^{1.5} \frac{\Delta s e^{\frac{-|y|s}{\Delta s}} dy}{2e}}$
9: $\quad$ **end for**
10: **end for**
11: **return** $\int(u)$
12: END

In Algorithm 2 the parameters H, ϵ and m must pass before deploying the algorithm. On the server-side, algorithm two

first creates an all-zero matrix of length $k * m$, which is then used to compute the result. Additionally, the system builds a running index for each separate report location. In the first step at line 1, the algorithm initializes all $k * m$ size of zero matrices, and then in line 2, it adds 1 to the index position of all collected n reports. In line 3 of the algorithm, each data matrix value is recorded at the appropriate location of each hash function, and also each attribute value frequency is calculated using the count sketch.

In the server-side algorithm, the time complexity is $O(n+|D|*k)$, whereas the space complexity is $O(n+|D|*k)$.

D. IOTA DLT

In IOTA, every new transaction has to verify two previous transactions to compute a small amount of proof of work (computational work). Verification process In Tangle is different from Blockchain as it has no miners, but members operating on it are, and a verified transaction is transmitted to the entire network. IOTA is more decentralized than Blockchain because all members receive the same rewards and incentives, and there is no hierarchy of responsibilities in Tangle. When using a weighted random walk, cumulative weight is utilized to calculate the number of approvals, and hence higher the cumulative weight, the more approvers there are. Furthermore, in the network, all members use the Markov Chain Monte Carlo (MCMC) method to choose which path to take. The network becomes stable, more scalable, and quicker with time, and the path becomes secure over time because as long as more members add more PoW from added transactions, most members follow the same path.Our proposed IOTA network model is demonstrated in Figure 8.

When n number of users connect with an SP at a given timestamp T, the data collected at one particular timestamp are stored at the SP. When entering a new timestamp $ti+1$, the perturbed data di collected from n number of Users stored at an SP are concatenated together, resulting in D'. As demonstrated in Figure 8, file producers must keep their seed files in IOTA. The following describes the procedure:

- Create a seed file for the requested file by using the Client application.
- Assemble the seed file and time stamp into the MAM message and proceed to the transaction start phase.
- Using the prepareTransfers function, group transactions together into bundles.
- Call getTransactionsToApprove to get an IRI, execute a tip select to validate two tips, and provide the TX hashes of both two transactions.
- Using the attachToTangle method, send the transaction and its TX hash to the PoW node for workload proof. The transaction is then saved and propagated by IRI, using the storeTransactions and broadcastTransactions functions respectively.

VI. EVALUATIONS

A. SECURITY AND PRIVACY ANALYSIS

Theorem 1: The proposed algorithm LCS satisfies the definition of ϵ-local differential privacy.

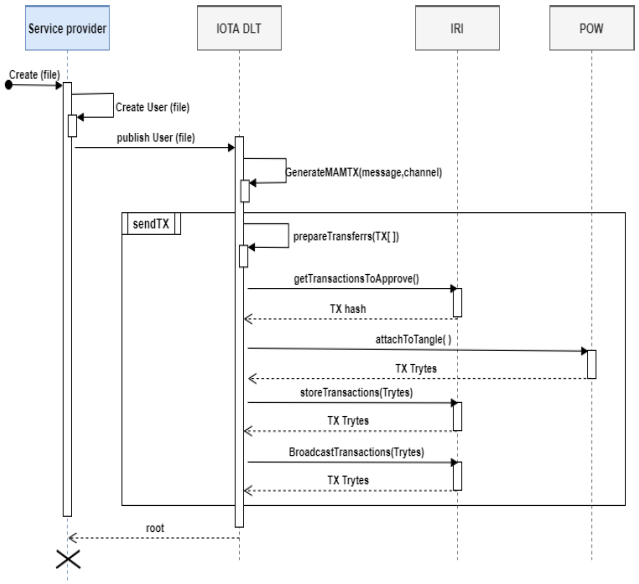

FIGURE 8. Transaction publishing process.

Proof: Given any set of input values u and u' and any possible outcome u^*, $p_{(u)}$ is named as the probability density function of $A(u)$, and $p_{(u')}$ is the probability density function of $A(u')$; compare the probability of these two.

$$\frac{Pr[A(u)=u']}{Pr[A(u')=u^*]} = \frac{Pr[u+v]}{Pr[u'+v]} = \frac{p_u(v)}{p_v(v)} = e^{\epsilon}$$
$$= \left(\frac{\left|\int(u)-\int(u')\right|}{\Delta s}\right) < e^{\epsilon}$$

Because sensitivity is $\Delta s = 2$, the highest difference between $\left|\int(u)-\int(u')\right| = 2$; That is the value range of $\left|\int(u)-\int(u')\right|$ $[0, 2]$ and local differential privacy definition is satisfied because $\left(\frac{\left|\int(u)-\int(u')\right|}{\Delta s}\right) \leq 1$.

1) FORMAL SECURITY ANALYSIS

This section simulates our proposed system utilizing the most generally recognized and used Automated Validation of Internet Security Protocols and Applications (AVISPA) tool to demonstrate that our scheme is safe against replay and man-in-the-middle attacks.We perform a security evaluation analysis of our proposed security protocol by simulating it using AVISPA tool in SPAN version 1.6 installed in VirtualBox 6.0 with 2 GB RAM to verify our authentication protocol based on a decentralized environment.

The tool is integrated with python language and works for claims defined for security protocol. AVISPA is a high-level language for defining protocols & associated security features in a scalable and descriptive manner. A number of state-of-the-art automated algorithms are implemented through a range of back-ends which are integrated into the system [35]. Each participant role has a basic role, and composition roles describe instances of basic roles.

The security protocols must be developed in HLPSL (High Level Protocols Specification Language), which is a role-oriented language. The Dolev–Yao model is used to

represent an intruder(i) and protocol run can go on without the intruder(i) knowing about it. Several sessions, principles, and fundamental roles are specified in HLPSL. HLPSL is translated to the intermediate format (IF) using the HLPSL2IF translator, and then the output format (OF) is produced using one of four back ends that are OFMC,SAMTC,CL-AtSe and TA4SP.

For analysis of our proposed protocol, we consider HLPSL language, In HLPSL we have defined three fundamental roles for the key distribution centre KDC and the smart parking system SP in reference to the registration and authentication phases. In addition to these roles, our implementation also requires the specification of session, goal, and environment roles in HLPSL. Our analysis demonstrate that our proposed ECC based anonymous authentication protocol is secure against the man in the middle, disclosure and impersonation attacks.

We have integrated three primary roles in our protocol: U, P, and KDC for User, Service Provider and KDC respectively. The KDC in HLPSL is responsible for the registration and authentication phases of our system. HLPSL has additional roles that need to be established in order for our scheme to work properly: session, goal, and environment roles. KDC is critical in the formation of HLPSL, as seen in Figure 10. KDC receives the start signal during the registration phase and changes its state from 0 to 1, which is stored in the variable State. KDC then securely transmits the registration request (Kup, U_{id}, N_p) to the U through the $SND()$ channel.

The channel type declaration (dy) indicates that the channel is intended for use with the Dolev–Yao threat model, which assumes that an intruder(i) has the capability of intercepting, analyzing, or altering communications transmitted over an unprotected public network channel. Using the $RCV()$ channel, U is then able to safely receive the message (U, P, F_{id}, SK_{up}) from KDC. The played by A declaration in this role indicates that the agent stated in variable A performs in the role. Declaration secret (Kup, U_{id}, N_p, $Auth1$, Sk_{KDC}) implies that the information U_{id} and Sk_{KDC} are only known to KDC.

In Figure 9, we have integrated the roles of the KDC and SP throughout the registration and authentication stages in a similar manner.

Our analysis demonstrate that our proposed ECC based anonymous authentication protocol is secure against the man in the middle, disclosure and impersonation attacks as shown in the Figure 11.

2) INFORMAL SECURITY ANALYSIS

This section evaluated our security protocol informally against various types of adversarial attacks and checked the security feature. This analysis is based on the knowledge of the analyst and author. Comparison of security feature with existing approaches is given in Table 2.

- **Resistant Against DDoS Attack** We use IOTA DLT to robust our system against a single point of failure (SPoF). The service provider will append the historical parking records of the user to the IOTA ledger, which is entirely decentralized and scale-able.
  In this proposed framework, we have used IOTA DLT platform instead of centralized platform (e.g, Cloud Network). Due to the decentralized nature of platform it reduces the probability of attack. As there is no involvement of any third party for registration and authentication of participants which largely decrease the attack surface area. By using IOTA DLT, participants (SPs, KDC) are distributed among different BAs that minimize the attack probability on the system. In addition, $Users$ do not need to get registered with the SP whenever they want to send the data request (RoD). That eliminate the changing secret (PK_{KDC}, SK_{KDC}) for each session and prevent system desynchronization.
- **Preserving drivers' privacy** We preserve the privacy of the user/driver in all phases of our system to achieve anonymity and untractability. The user's real identity is only used once in the registration phase, and only KDC can know its real ID_{v_i}. Still, no other entity can trace the derivatives of the user identity in the transmitted message of the user.

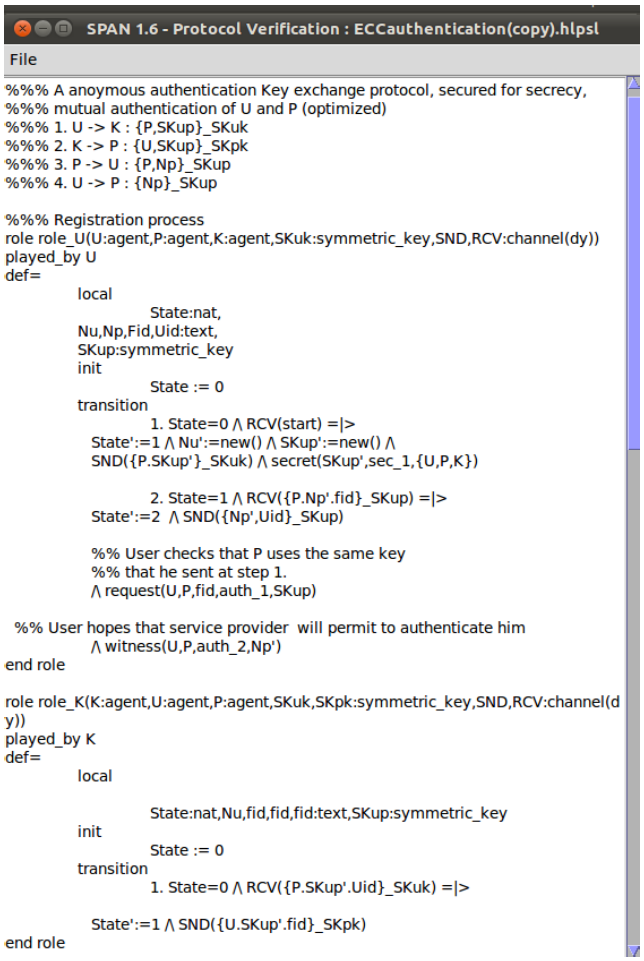

FIGURE 9. Role specification for user, and KDC in HLPSL.

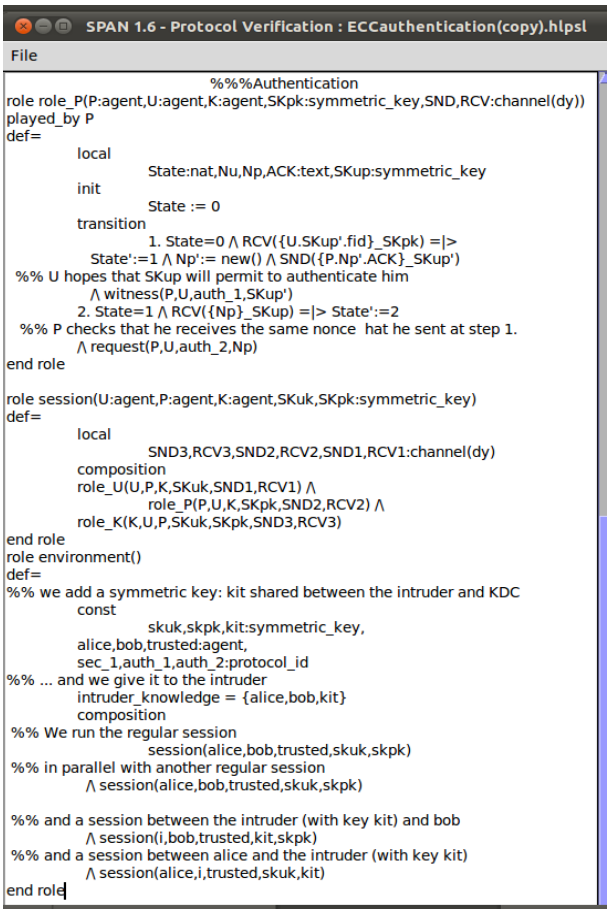

FIGURE 10. Role specification for provider,session, environment and goal in HLPSL.

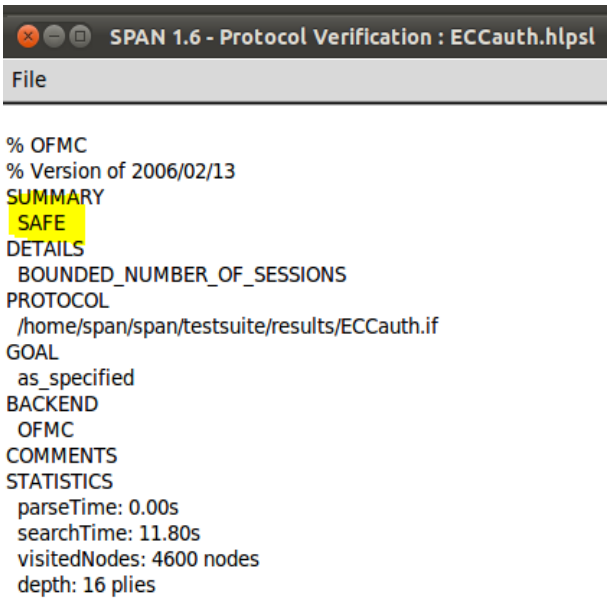

FIGURE 11. Anonymous authentication protocol analysis using OFMC backend.

- **Anonymity** The KDC randomly assign anonymous credentials $FID_{\upsilon_i}^{[1]}, FID_{\upsilon_i}^{[2]}, FID_{\upsilon_i}^{[3]}$, to the user when the user registered first time with the KDC. Except for the system initialization phase, the user's real ID_{υ_i} can not be revealed at any stage because anonymous credentials are used to verify the user in the authentication phase and neither the *SP* nor third party recommender system can uniquely identify the user in the system.
- **Prevention of Untracablity attack** The user in our system is untraceable because of anonymous credentials $(FID_{\upsilon_i}^{[1]}, FID_{\upsilon_i}^{[2]}, FID_{\upsilon_i}^{[3]})$, such as $M'_{KDC} = HMAC(FID_{\upsilon_i}1 \parallel EC_p \parallel T \parallel SK_\upsilon)$. The adversary can not link the user as the message will be expired due to the involvement of the timestamp in each message.
- **Prevention of Secret Disclosure attack** We use *HMAC*,public and private keys $(SK_{\upsilon_i}, PK_{\upsilon_i}, SK_{KDC}$ $PK_{KDC}, SK_{SP}, PK_{SP})$ to encrypt and decrypt the message between the entities involved in our system. In any case, if the adversary is able to compromise the message, it still can not disclose the user's real identity. Moreover, the keys for this session can not be used for the next sessions because the KDC will generate the fresh keys $FID_{\upsilon_i}^{[1]}, FID_{\upsilon_i}^{[2]}, FID_{\upsilon_i}^{[3]}$, after every verification of the user.
- **Prevention of Impersonation Attack** The adversary can not perform an impersonation attack due to the fact that the *HMAC* is used between the KDC and user using a shared secret between them, and the adversary can not decrypt the *HMAC* without the knowledge of secret keys $(SK_{KDC}, SK_{\upsilon_i})$. In the worst case, if the adversary is able to compromise the message between the user and *KDC* or *SP*, it can not impersonate because the *KDC* does the verification, and the anonymous credentials can not be used more than once in the authentication process.
- **Resistant Against Man in the Middle Attack** The communication between the entities is encrypted with the *HMAC* such as $M'_{KDC} = HMAC(FID_{\upsilon_i}1 \parallel EC_p \parallel T \parallel SK_\upsilon)$, the adversary is unable to decrypt M'_{KDC} or any other message without the prior knowledge of the secret keys.
- **Prevention of Background Knowledge Attack** We use local differential privacy to thwart background knowledge attacks so that the attacker can not link the user to any record as data is perturbed before sending to the third party, and the attacker can not differentiate a data value u or u' belong to a particular user or not.
- **Accountability** In case of any dispute, the SP will share the corresponding FID_{υ_i} of the υ_i to *KDC*, and *KDC* will revoke the M_{υ_i} and extract the actual ID_{υ_i} and match user FID_{υ_i} from the tracing, the list gives plenty, such as negative points on his driving license to the υ_i according to predefined rules.
- **Quantum Resistance** IOTA use winternitz OTS which is secure against the quantum computing attack. WOTS algorithm is thought to be the most efficient post-quantum signatures for key generation and signature compression. IOTA has prepared for the quantum era by using a quantum robust WOTS scheme. Variants of WOTS include WOTS+ and WOTS-T.

TABLE 2. Comparison of security feature with existing approaches.

Schemes	[23]	[45]	[48]	[50]	[14]	Proposed Scheme
Decentralized	x	✓	✓	✓	✓	✓
Anonymous Authentication	x	✓	x	x	x	✓
Impersonating Attack	x	x	x	x	x	✓
Secret Disclosure	✓	x	✓	x	x	✓
Man in the Middle	x	x	✓	✓	✓	✓
Background Knowledge attack	✓	✓	x	x	x	✓
Accountability	x	✓	x	x	x	✓
Quantum Resistance	x	x	x	x	x	✓

TABLE 3. Parking dataset of Santander city December 2017.

Attribute	Height	Distinct Values
Number of records	15296	5
Longitude	506	29
Latitude	506	29
Parking spot	275	15
Timestamp	6232	7

B. PERFORMANCE EVALUATION

We utilised a real-world Santander, Spain, parking data set that included the timestamp of the time of reservation of parking spaces in December 2017. After that, actual spots inside Santander are utilised to produce a synthetic parking data set by adding random 8 of 29 user positions and scores to every entry inside the actual space occupancy record set in order to examine the privacy protection methods known as local differential privacy. Thus, while the data set is artificial, it is derived out of a actual data set on parking capacity and actual places, and thus accurately represents a real dataset. Detailed information of dataset is given in the Table 3. The data collection contains 15,296 records, each of which contains 506 separate actual places representing user's present position (georeferenced), 275 parking spaces, 6232 timestamps, and ratings from 1-5 for the month of December 2017.

1) EXPERIMENTAL SETTING

The performance of our proposed scheme is analyzed by setting up Python 3.7.12 with NumPy v1.16.6 and Pandas v0.24.2 libraries on a Windows 10 pro version 20H2 with an Intel Core i5 2.7 GHz processor with a 8 GB DDR3 RAM environment. We have used IOTA Reference Implementation (IRI) and Nodejs to implement the protocol and determine its feasibility and functionality. Client and authentication servers are setups to register the participants for each transaction whenever the participants are registered and authenticated with the authenticator server on parking dataset of 15296 records of Santander city.

2) PERFORMANCE METRICS

We use Mean Absolute Error (MAE) and Root mean square error (RMSE) [33] to evaluate our proposed local differential privacy accuracy.

a: MEAN ABSOLUTE ERROR (MAE)

The average number of errors in MAE is calculated as the absolute difference between the actual and noisy responses of the average query results. The high value of MAE guarantees stronger privacy. Still, at the cost of utility, because the difference between the actual and noisy responses of the average query results is high, inversely, in the case of low MAE, the utility is enhanced. Still, the privacy will be low because the difference between the actual and noisy responses of the average query results is low.

$$MAE = \frac{1}{N}\sum_{N}^{i=2}(u_{ai} - u'_{ni}) \tag{11}$$

Where u_{ai} and u'_{ni} are actual and noisy query responses of the query i, and N is the total number of queries.

b: ROOT MEAN SQUARE ERROR (RMSE)

The root mean square error (RMSE) is a quadratic evaluation function that also calculates the average number of errors. It's the square root of the average squared deviations between the real and noisy query results. It quantifies both privacy and utility. As with MAE, a high RMSE indicates a large difference between the true and noisy query results, which increases privacy but decreases utility. While a low root mean square error means that the difference between true and noisy query responses is small, this improves utility but compromises privacy.

$$RMSE = \sqrt{\frac{\sum_{i=1}^{N} = (u_{ai} - u'_{ni})}{N}}. \tag{12}$$

We measure the privacy and utility trade-off of local differential privacy by using MAE and RMSE between the privacy budget (ϵ) 0.1 to 1.0 and also analyze each sensitivity Δf(1-5) of the records between.

3) PERFORMANCE ANALYSIS

We recorded readings in order to assess the time complexity of registration and authentication. For a single operation in milliseconds, a separate time threshold is used. It takes somewhat longer for the drivers to register for the first time than it does for authentication. An access token is made when the driver registers. This token is used by the driver to prove their identity. We repeated this procedure many times to get an average time for registration and authentication.

The cost of computing is expressed in GAS. It deducts 90737 GAS from the overall limit of 113421 GAS for every transaction.

Figure 12 demonstrates that registration time is rather long when compared to authentication time. We observed many

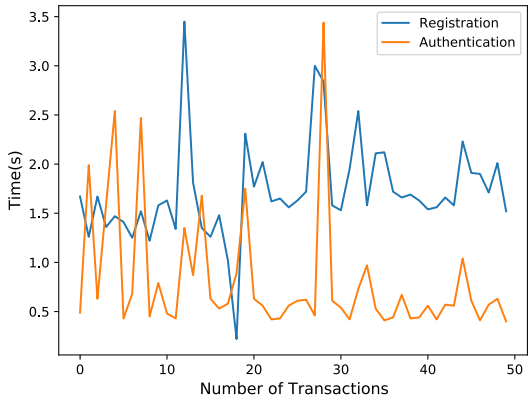

FIGURE 12. Time complexity of registration and authentication process.

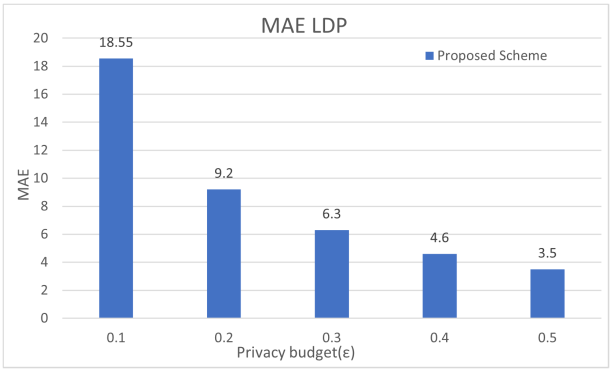

FIGURE 13. MAE LDP on different privacy budget.

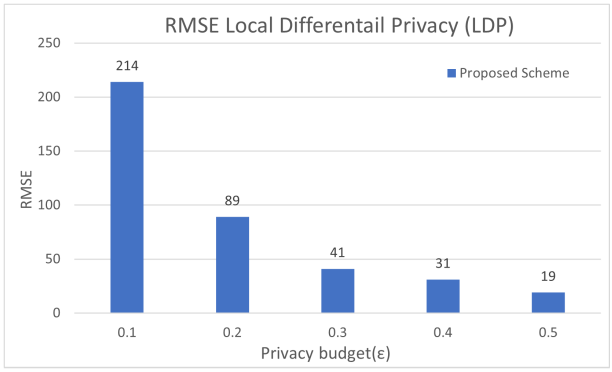

FIGURE 14. RMSE LDP on different privacy budget.

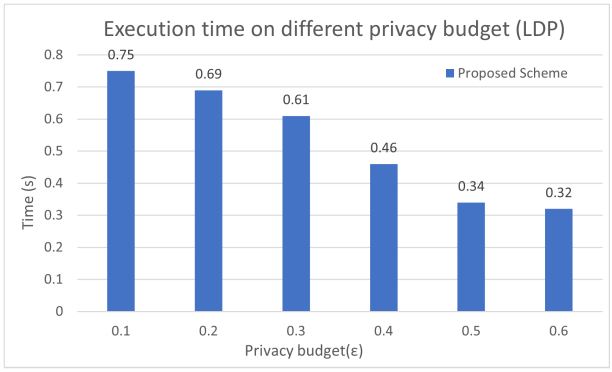

FIGURE 15. Execution time LDP on different privacy budget.

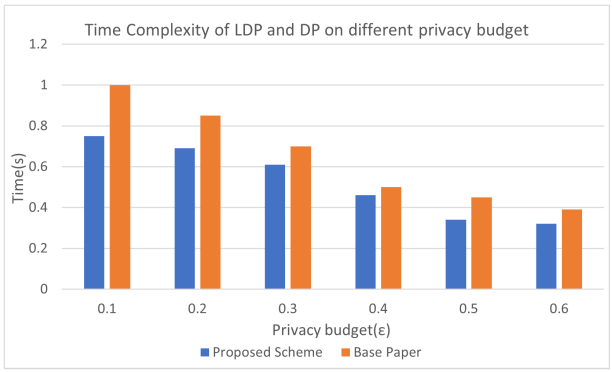

FIGURE 16. Time Complexity of LDP and DP on different privacy budget.

transactions in order to set up the average time complexity. The registration time complexity is 1.71s, while the authentication time complexity is 0.81s, which is much lower than the registration time.

We use MAE and RMSE for evaluating local differential privacy in terms of accuracy and privacy for privacy budgets ranging from ϵ 0.1 to 1.0. The mean absolute error (MAE) for privacy budgets ranges from ϵ 0.1 to 1.0 for sensitivity Δ f = 1. (i.e., the addition or removal of a user affects one record in the parking data set). In this case, it is shown that the MAE is very high, with values of 18.55 since 0.1 ensures the maximum privacy at the expense of the lowest utility, as seen in Figure 13. However, as the privacy budget ϵ increases, the MAE continues to decrease dramatically, and at 1.0, MAE is near zero, indicating that maximum utility.

Similarly, we meaure root mean suqare error (RMSE) for privacy budgets ranges from ϵ 0.1 to 1.0 for sensitivity Δ f = 1. In this case, it is shown that the RMSE is very high, with values of 210 since 0.1 ensures the maximum privacy at the expense of the lowest utility, as seen in Figure 14. However, as the privacy budget ϵ increases, the RMSE continues to decrease dramatically, and at 1.0, RMSE is less than 10, indicating that maximum utility.

Figure 15 illustrates execution time on different privacy budget ϵ 0.1 to 0.6. At 0.1, local differential privacy took 0.75 seconds as at lower the privacy budget ϵ, more noise needs to be added. On the other hand, at ϵ 0.6 it takes less time 0.32 seconds because at ϵ 0.6, the utility is high with the increase no of ϵ.

C. COMPARISON OF RESULTS

Execution time on different privacy budget ϵ 0.1 to 0.6 for our proposed scheme and base paper (differential privacy) is illustrated in Figure 16. At 0.1, our proposed scheme took 0.75 seconds but differential privacy technique used in [23] took 1 seconds, as at lower the privacy budget ϵ, more noise needs to be added. On the other hand, at ϵ 0.6 both differential privacy and local differential privacy takes less time 0.32 and 0.38 seconds respectively because at ϵ 0.6, the utility is high with the increase no of ϵ. The differential privacy technique used in [23] takes more computation as the addition of noise is done at single location while on other hand in our proposed

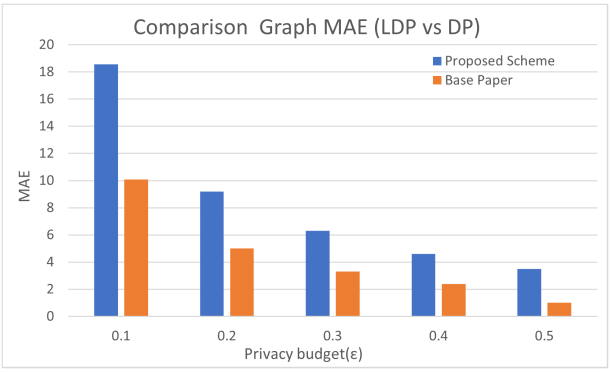

FIGURE 17. LDP vs DP MAE comparison on different privacy budget.

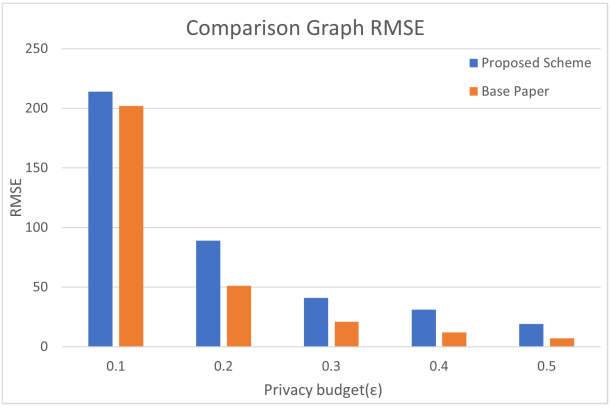

FIGURE 18. LDP vs DP RMSE comparison on different privacy budget.

scheme noise is added locally and overall computation is divided among other entities rather than a centralized location.

The MAE is high 18.2 and 10 at privacy budget ϵ 0.1 for both in local differential privacy and differential privacy respectively. But our prooosed local differential privacy achieves more privacy at privacy budget of 0.1 as compared to base paper [23] differential privacy as shown in Figure 17. At privacy budget of 0.5 the MAE for differential privacy is close to zero which means differential privacy gives more utility as compared to proposed local differential privacy.

The RMSE is high 210 and 202 at privacy budget ϵ 0.1 for both in local differential privacy and differential privacy respectively. But our proposed local differential privacy achieves more privacy at privacy budget of 0.1 as compared to differential privacy as shown in Figure 18. At privacy budget of 0.5 the RMSE for differential privacy is close to zero which means differential privacy gives more utility as compared to local differential privacy.

our proposed scheme not only provide stronger privacy but also grantees security and divide computation among different entities. The privacy utility trade off shows that our scheme provide more privacy on lower privacy budgets.

1) COMPUTATION OVERHEAD

The computational cost of our proposed protocol for authentication level includes the key generation and hashing. The complexity in the computation of ECC is cubic if the prime numbers of bit length are used. The modular multiplication is considered to solve the ECC bit length. For this purpose, the double-and-add algorithm is used to entertain the bit length. Using ECC, we have the advantage of more security with fewer parameters $2^3 = 8$ compared to other public-key RSA and Discrete Logarithm encryption schemes. These two schemes provide the same protection as ECC but with larger computations. ECC needs 2 bits of increase in parameter length compared to RSA and DL, which 20-30 bit increase in bit-length to achieve the same security level. The attacker's efforts to break the security also increase in the case of ECC.

The key generation of parties involves secret number which needs point multiplication over the Curve. The length of the message depends on the encryption scheme, which is used to encrypt the message. In our scheme, the data provider, consumer, and authenticator communication are hashed and asymmetrically encrypted including the timestamp. By generating shared secret include some computation which has scalar multiplication properties and the hashing. It can be seen that during the registration and authentication phases, a very less amount of analysis is needed because they do not consider the bit length much larger as compared to in other public-key schemes. We assume that the total number of bytes used for Hash, HMAC are 16, timestamp STs and for the identity of entities consumes 4 bytes of data. The generation of a key for communication is only done at once, authentication. That is why it does not create extra computational overhead for the rest of the communication.

VII. CONCLUSION AND FUTURE WORK

This paper proposes a secure and privacy-preserved parking recommender scheme based on IOTA DLT, local differential privacy, and elliptic curve cryptography. Privacy of parking data is a major concern in data sharing systems as various parking service providers are sharing the historical data with third-party recommender systems for better user experience and personalized parking recommendations that may lead to unauthorized access to individual's data and the user can be uniquely identified by using background knowledge attack by the attacker. We have developed the anonymous security protocol for authentication and registration using ECC and *HMAC* that authenticates the user to prevent unauthorized access to data and provide anonymity and integrity during the communication. Our proposed protocol is efficient against secret disclosure, traceability, and Unlinkability attacks compared to existing schemes such as ECCbAP. However, the time for authentication of our proposed system is slightly high because *HMAC* is used to provide anonymity and integrity during sharing of data, which is acceptable in data privacy. It is also resistant against (MiM) attacks to protect communication between users and KDC. LDP utilizes the Laplace mechanism to change query responses, which removes the need for a third party to do data perturbation. This is because untrustworthy third parties cause a significant threat to the user's security and privacy. In addition to LDP

anonymization techniques, we have presented a model that utilizes the IOTA ledger to provide a new level of security that ensures immutability, scalability, and quantum secrecy throughout the database and protects against a single point of failure issue. The trade-off between privacy and utility is assessed by experimental data drawn through actual parking metrics, allowing users to get parking space suggestions while preserving their privacy. Our experiments demonstrate that, in addition to protecting the driver's privacy and security, our proposed model has low storage overheads, computation, and communication costs.

In future, we will add the anonymous payment scheme by using IOTA tokens and anonymous reputation management along with the proposed scheme and evaluate our scheme with real data set of the user parking.

REFERENCES

[1] I. Aydin, M. Karakose, and E. Karakose, "A navigation and reservation based smart parking platform using genetic optimization for smart cities," in *Proc. 5th Int. Istanbul Smart Grid Cities Congr. Fair (ICSG)*, Apr. 2017, pp. 120–124.

[2] *Parkme*. Accessed: Dec. 1, 2021. [Online]. Available: https://www.parkme.com/

[3] *Parkmobile*. Accessed: Aug. 5, 2021. [Online]. Available: https://www.parkmobile.io/

[4] *Parkwhiz*. Accessed: Aug. 10, 2021. [Online]. Available: https://www.parkwhiz.com/

[5] *Fybrsfpark*. Accessed: Jul. 5, 2021. [Online]. Available: https://www.fybr.com/

[6] *Spothero*. Accessed: Jun. 7, 2021. [Online]. Available: https://spothero.com/

[7] M. G. Divya and M. M. Kavitha, "Secure privacy preserving identification model for mobile sensing system," in *Proc. Global IoT Summit*, 2018.

[8] L. Mitrou, "Data protection, artificial intelligence and cognitive services?" *Artif. Intell. Cogn. Services*, 2018.

[9] *Worldwide Interoperability for Semantic IoT (WISE-IoT)*. Accessed: Dec. 1, 2019. [Online]. Available: http://wise-iot.eu/en/home/

[10] P. Sotres, C. Torre, L. Sanchez, S. Jeong, and J. Kim, "Smart city services over a global interoperable Internet-of-Things system: The smart parking case," in *Proc. Global IoT Summit*, 2018, pp. 1–6.

[11] B. Shao, X. Li, and G. Bian, "A survey of research hotspots and frontier trends of recommendation systems from the perspective of knowledge graph," *Expert Syst. Appl.*, vol. 165, Mar. 2021, Art. no. 113764.

[12] 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.

[13] 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.

[14] L. Zhu, M. Li, Z. Zhang, and Z. Qin, "ASAP: An anonymous smart-parking and payment scheme in vehicular networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 7, pp. 133496–133508, Sep. 2018.

[15] M. Arif, G. Wang, and V. E. Balas, "Secure VANETs: Trusted communication scheme between vehicles and infrastructure based on fog computing," *Stud. Inform. Control*, vol. 27, no. 2, pp. 235–246, 2018.

[16] T. Diab, M. Gilg, F. Drouhin, and P. Lorenz, "Anonymizing communication in VANets by applying I2P mechanisms," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[17] T. Wang, Z. Zheng, M. H. Rehmani, S. Yao, and Z. Huo, "Privacy preservation in big data from the communication perspective—A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 753–778, Aug. 2019.

[18] S. Gambs, M. Olivier, and M. N. del Prado Cortez, "De-anonymization attack on geolocated data," *J. Comput. Syst. Sci.*, vol. 80, no. 8, pp. 1597–1614, 2017.

[19] T. Stefanovic and S. Ghilezan, "Differential privacy and applications," in *Logic and Applications LAP*. 2021, p. 52.

[20] Accessed: Dec. 1, 2021. [Online]. Available: https://ecommons.cornell.edu/handle/1813/60392/

[21] *Facebook's Privacy Problems: A Roundup*. Accessed: Oct. 10, 2021. [Online]. Available: https://www.theguardian.com/technology/2018/dec/14/facebook-privacy-problems-roundup

[22] *'The Snappening' Is Real: 90,000 Private Photos and 9,000 Hacked Snapchat Videos Leak*. Accessed: Dec. 1, 2021. [Online]. Available: https://www.thedailybeast.com/

[23] Y. Saleem, M. H. Rehmani, N. Crespi, and R. Minerva, "Parking recommender system privacy preservation through anonymization and differential privacy," *Eng. Rep.*, vol. 3, no. 2, Feb. 2021, Art. no. e12297.

[24] G. Cormode, S. Jha, T. Kulkarni, N. Li, D. Srivastava, and T. Wang, "Privacy at scale: Local differential privacy in practice," in *Proc. Int. Conf. Manage. Data*, May 2018, pp. 1655–1658.

[25] T.-H. Kim, R. Goyat, M. K. Rai, G. Kumar, W. J. Buchanan, R. Saha, and R. Thomas, "A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks," *IEEE Access*, vol. 7, pp. 184133–184144, 2019.

[26] M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud, and M. Abdallah, "Blockchain-based firmware update scheme tailored for autonomous vehicles," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Marrakesh, Morocco, Apr. 2019, pp. 1–7.

[27] J. Wang, L. Wu, K.-K.-R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1984–1992, Mar. 2020.

[28] E. Chukwu and L. Garg, "A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations," *IEEE Access*, vol. 8, pp. 21196–21214, 2020.

[29] E. Fatnassi and H. Kaabi, "A multi-agent system model for the personal rapid transit system," in *Proc. Int. Conf. Comput. Inf. Syst. Ind. Manage. (IFIP)*. Cham, Switzerland: Springer, Jun. 2017, pp. 492–501.

[30] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)*, Feb. 2017, pp. 32–37.

[31] A. Faccia, *Quantum Finance. Opportunities and Threats*. 2020.

[32] E. Vieira, P. C. Bartolomeu, S. M. Hosseini, and J. Ferreira, "IOTApass: Enabling public transport payments with IOTA," in *Proc. IEEE 6th World Forum Internet Things (WF-IoT)*, Jun. 2020, pp. 1–6.

[33] N. Wang, X. Xiao, Y. Yang, J. Zhao, S. C. Hui, H. Shin, J. Shin, and G. Yu, "Collecting and analyzing multidimensional data with local differential privacy," in *Proc. IEEE 35th Int. Conf. Data Eng. (ICDE)*, Apr. 2019, pp. 638–649.

[34] *Parkgene*. Accessed: Mar. 5, 2021. [Online]. Available: https://parkgene.io/

[35] *AVISPA Automated Validation of Internet Security Protocols and Applications*. Accessed: Sep. 2021. [Online]. Available: http://www.avispaproject.org/

[36] N. Wu, C. Peng, and K. Niu, "A privacy-preserving game model for local differential privacy by using information-theoretic approach," *IEEE Access*, vol. 8, pp. 216741–216751, 2020.

[37] M. E. Gursoy, A. Tamersoy, and S. Truex, "Secure and utility-aware data collection with condensed local differential privacy," 2019, *arXiv:1905.06361*.

[38] *Distributor*. Accessed: Mar. 5, 2021. [Online]. Available: https://www.disruptordaily.com/

[39] X. Fang, Q. Zeng, and G. Yang, "Local differential privacy for human-centered computing," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, p. 65, Dec. 2020.

[40] X. Jin, X. Li, H. Zhang, R. Soulé, J. Lee, N. Foster, C. Kim, and I. Stoica, "NetCache: Balancing key-value stores with fast in-network caching," in *Proc. 26th Symp. Operating Syst. Princ.*, Oct. 2017, pp. 121–136.

[41] J. Zhang, G. Cormode, and C. M. Procopiuc, "Private data release via Bayesian networks," *ACM Trans. Database Syst.*, vol. 42, no. 4, pp. 1–41, 2017.

[42] W. A. Amiri, M. Baza, K. Banawan, M. Mahmoud, W. Alasmary, and K. Akkaya, "Alasmary and K. Akkaya, "Towards secure smart parking system using blockchain technology," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–2.

[43] W. A. Amiri, M. Baza, K. Banawan, M. Mahmoud, W. Alasmary, and K. Akkaya, "Privacy-preserving smart parking system using blockchain and private information retrieval," in *Proc. Int. Conf. Smart Appl., Commun. Netw. (SmartNets)*, Dec. 2019, pp. 1–6.

[44] S. Singh, D. Satish, and S. R. Lakshmi, "Ring signature and improved multi-transaction mode consortium blockchain-based private information retrieval for privacy-preserving smart parking system," *Int. J. Commun. Syst.*, vol. 34, no. 14, Sep. 2021, Art. no. e4911.
[45] M. M. Badr, W. A. Amiri, M. M. Fouda, M. M. E. A. Mahmoud, A. J. Aljohani, and W. Alasmary, "Smart parking system with privacy preservation and reputation management using blockchain," *IEEE Access*, vol. 8, pp. 150823–150843, 2020.
[46] T. Fu, P. Liu, K. Liu, and P. Li, "Privacy-preserving vehicle assignment in the parking space sharing system," *Wireless Commun. Mobile Comput.*, vol. 2020, Oct. 2020, Art. no. 8862652.
[47] Z. Li, M. Alazab, S. Garg, and M. S. Hossain, "PriParkRec: Privacy-preserving decentralized parking recommendation service," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4037–4050, May 2021.
[48] P. Dzurenda, C. A. Tafalla, S. Ricci, and L. Malina, "Privacy-preserving online parking based on smart contracts," in *Proc. 16th Int. Conf. Availability, Rel. Secur.*, Aug. 2021, pp. 1–10.
[49] C. Zhang, L. Zhu, C. Xu, C. Zhang, K. Sharif, H. Wu, and H. Westermann, "BSFP: Blockchain-enabled smart parking with fairness, reliability and privacy protection," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6578–6591, Jun. 2020.
[50] A. K. Tyagi, S. Kumari, T. F. Fernandez, and C. Aravindan, "Privacy preserved, trusted smart parking allotment for future vehicles of tomorrow," in *Proc. Int. Conf. Comput. Sci. Appl.* Cham, Switzerland: Springer, Jul. 2020, pp. 783–796.

AWAIS ABDUL KHALIQ received the B.S. degree in information technology (BSIT) from the University of Azad Jammu and Kashmir, Muzaffarabad, Pakistan, in 2014. He is currently pursuing the M.S. degree in information security with COMSATS University Islamabad, Pakistan. His research interests include data privacy in the smart city, differential privacy, and blockchain.

ADEEL ANJUM received the Ph.D. degree in computer sciences from the University of Nantes, Nantes, France. He is currently an Associate Professor with the Department of Information Technology, Quaid-i-Azam University, Islamabad, Pakistan, and a Research Assistant Professor with the Southern University of Sciences and Technology (SUSTECH), Shenzhen, China. His research interests include access control systems, model-driven architecture, and work flow management systems.

ABDUL BASIT AJMAL received the master's degree in information security from COMSATS University Islamabad, Pakistan, in 2021. Currently, he is working as a Security Researcher with the Research and Development Security Laboratory, COMSATS University Islamabad. His current research interests include privacy preserving, threat hunting, cyber defense, adversary simulation, and risk assessment.

JULIAN L. WEBBER (Senior Member, IEEE) received the M.Eng. and Ph.D. degrees from the University of Bristol, U.K., in 1996 and 2004, respectively. He worked at Texas Instruments Europe, from September 1996 to October 1998. He was a Research Fellow at the University of Bristol, from November 2001 to August 2007, and at Hokkaido University, Japan, from September 2007 to March 2012. He was a Research Scientist at the Wave Engineering Laboratories, ATR Institute International, Japan, from April 2012 to March 2018. He has been an Assistant Professor with Osaka University, since April 2018, and a Guest Research Scientist with ATR. His research interests include signal processing and wireless communication systems design and implementation. He is a member of IEICE.

ABOLFAZL MEHBODNIYA (Senior Member, IEEE) received the Ph.D. degree from INRS-EMT University of Quebec, Montreal, Canada, in 2010. He was a Marie-Curie Senior Research Fellow at University College Dublin, Ireland, and he was an Assistant Professor at Tohoku University, Japan, and a Research Scientist at the Advanced Telecommunication Research (ATR) International, Kyoto, Japan. He is an Associate Professor and the Head of the ECE Department with the Kuwait College of Science and Technology (KCST). His research interests include communications engineering and the IoT and artificial intelligence in wireless networks and real world applications. He was a recipient of numerous awards, including the JSPS Young Faculty Startup Grant, the KDDI Foundation Grant, the Japan Radio Communications Society (RCS) Active Researcher Award, the European Commission Marie Skodowska-Curie Fellowship, and the NSERC Visiting Fellowships in Canadian Government Laboratories. He is a Senior Member of IEICE.

SHAWAL KHAN received the bachelor's degree in computer science from Shaheed Benazir Bhutto University, Upper Dir, Khyber Pakhtunkhwa, Pakistan. He is currently pursuing the master's degree in information security with the COMSATS Institute of Information Technology, Islamabad, Pakistan. His research interests include access control, cryptography, and network security.