Privacy-preserving User-centric Authentication Protocol for IoT-Enabled Vehicular Charging System Using Decentralized Identity

Rohini Poolat Parameswarath, Prosanta Gope, and Biplab Sikdar

***Abstract*—There has been a shift towards the use of Electric Vehicles (EV) in recent years. Though EVs offer many advantages, there are concerns on the cyber security of its components and the privacy of its users. When users charge their EVs at a charging station, they need to reveal their personal details. An attacker can compromise the users' privacy by identifying and tracking where users charge their EVs. Hence, there is a need to protect EVs from cyber-attacks and preserve its users' privacy. In this paper, we address the problem of privacy preservation of users while charging their EVs in a 5G-enabled vehicular charging system. We propose a user-centric authentication protocol for EV charging based on Decentralized Identifier (DID) and blockchain. We use Verifiable Credential (VC) together with DID which provides Zero-Knowledge Proof (ZKP) about the user. Users have complete control over their identities resulting in user-centric authentication. At the same time, a third party can verify the user's legitimacy before providing services. Hence, our protocol makes the charging service available in a secure way, preserving the privacy of the user.**

***Index Terms*—Electric vehicle charging, IoT, Privacy, User-centric authentication, DID.**

I. Introduction

Electric Vehicles (EVs) are gaining popularity due to various reasons. Cutting energy cost and reducing environmental damage are some of them. Traditional vehicles contribute significantly to air pollution [1]. On the other hand, EVs do not produce much air pollution as they run on electricity instead of gasoline. Governments across the globe are providing generous tax incentives to switch to EVs. For example, according to Land Transport Authority Singapore, the EV population increased by 39% in the first seven months of 2021. One of the reasons for this EV adoption is tax incentives given by the government. However, there are some challenges in EV adoption such as the current limitations of battery technology, the need for an efficient charging infrastructure that involves enhancements in the current distribution network, and the lack of standards and interoperability of different charging systems [2].

EV charging systems broadly consist of Utility Service Providers (USP) and Charging Stations (CS) [3]. The USP is in charge of generating and supplying electricity to CSs. Different protocols such as ISO 15118 and Open Charge Point Protocol (OCPP) are used in EV charging systems for communication. As the number of EVs grows, there is a greater need for a network infrastructure that provides high reliability for vehicles and charging stations to communicate. 5G is an excellent candidate for this application [4].

Though EVs offer many advantages, there are concerns about cyber security of its components and the privacy of the users. All parties communicate through an insecure channel, the Internet. When a user uses or charges his/her EV from a CS, there are security and privacy concerns for the user. Finding a charging station and processing payments also pose a privacy risk to the user. Using this data, an adversary can track a user's location details, daily activities, and habits. Without secure communication, an adversary may do a Man-In-The-Middle attack and may eavesdrop, edit, or delete the messages exchanged among different parties.

A technique employed to achieve privacy of the users in EV charging is by using pseudo-IDs instead of their real identities. Instead of depending on a central issuing authority on pseudo-ID, if users create and manage their IDs, they have full control and ownership of it. Decentralized Identifier (DID) is designed for this purpose. The World Wide Web Consortium (W3C) DID working group [5] developed a standard for DID that enables a verifiable, decentralized digital identity. In centralized systems, all the information is stored on a central server and hence, there is a risk of information misuse. DID eliminates that risk and gives users a level of control and privacy protection than that exists in current centralized systems. Blockchains are digital ledgers implemented in a distributed manner and they can operate without the need for a central authority. Hence, blockchain is an appropriate tool to enable data exchange in the DID paradigm [6]. In this paper, the proposed protocol is built on the concepts of Verifiable Credential (VC) and DID which provides Zero-Knowledge Proof (ZKP) about the user. By employing VC and ZKP, anyone can verify that the Holder of a VC is a valid user but will not be able to learn anything more about the Holder of the VC.

A. Related Work

Electric Vehicle Charging: Many researchers have studied EV charging scenarios and proposed protocols for EV charging. There have been studies on algorithms to schedule EV

Rohini Poolat Parameswarath and Biplab Sikdar are with the Department of Electrical and Computer Engineering, College of Design and Engineering, National University of Singapore, Singapore. (Email: rohini.p@nus.edu.sg, bsikdar@nus.edu.sg)
Prosanta Gope is with the Department of Computer Science, University of Sheffield, United Kingdom. (E-mail: p.gope@sheffield.ac.uk)

charging and security assessment of the EV charging infrastructure. The authors of [3] proposed privacy-preserving authentication and key establishment scheme using lightweight cryptographic methods for vehicle-to-grid communication. EV charging protocols where users use pseudonyms instead of their real identities are presented in [7] and [8]. These solutions help to achieve privacy and unlinkability. However, the methods proposed in [7] and [8] need additional hardware.

Decentralized Identifiers: DID is a type of identifier that enables verifiable, decentralized digital identity which is built on the self-sovereign identity paradigm. A DID is a simple text that consists of three parts: a) the DID Uniform Resource Identifier (URI), b) the DID method identifier, and c) the DID method-specific identifier. A DID resolves to a DID document stored on a public ledger which contains information such as when it was created and the public key to authenticate the DID subject. This process is called DID resolution. A DID resolver is a software and/or hardware component that performs the DID resolution function to resolve a DID to the corresponding DID document. Four operations ('Read', 'Create', 'Update', and 'Deactivate') can be performed on a DID. The DID resolution functions resolve a DID into a DID document by executing the 'Read' operation [5].

Verifiable Credential: VCs are credentials issued by a trusted **Issuer** that can be cryptographically verified [9]. At least one proof mechanism such as digital signature must be expressed for a credential to be a verifiable credential. A **Verifier** can verify the VC cryptographically. VC acts as a means by which facts about the **Holder** of the VC can be proved. The authors of [10] discussed how the privacy of IoT devices can be improved considerably by using DID and VC. The authors of [11] developed a phone app for covid vaccination certification using the concept of DID and VC which ensures that users' privacy is protected.

Asymmetric Cryptography: We consider the asymmetric cryptographic technique Elliptic Curve Digital Signature Algorithm (ECDSA) for signing and verifying the VC. An asymmetric cryptographic technique enables signing data and verifying signature using a pair of keys (a public key and a private key). The owner of the private key does not share it with anyone else. The public key is available to others. ECDSA requires a substantially shorter key than another popular algorithm, Rivest–Shamir–Adleman (RSA), to offer the same level of security. We consider a key length of 256 bits in the proposed protocol.

Zero-Knowledge Proof: ZKP is a method a prover uses to prove to a verifier that a statement is true without revealing it. We use ZKP to enhance the privacy of the credentials. ZKP consists of 'prove' and 'verify' algorithms. The prover uses the 'prove' algorithm to prove a statement and the verifier uses the 'verify' algorithm to verify the proof [12]. ZKPs satisfy the following three properties:

Completeness: An honest prover can convince an honest verifier that a statement is true.

Zero-Knowledge: The ZKP reveals that the statement is true without revealing anything else.

Soundness: A prover cannot prove a false statement.

Blockchain: Blockchain is a shared, immutable ledger that enables decentralized peer-to-peer data storage. It is designed in such a way that, once data is committed to it, data is immutable [13]. Blockchains help participants to do transactions anonymously. Hence, blockchain is an ideal candidate for applications where preserving privacy is important. Blockchain is the main component of the decentralized public key infrastructure that can be trusted and acts as the DID registry. DID is written to blockchain so that it is available publicly, but no sensitive data is stored on the ledger. The authors of [13] proposed a protocol on blockchain that helps EVs to select charging stations based on parameters such as pricing and location.

Key Recovery: In DID mechanism, blockchains store only DIDs and public keys. The storage of the private key is the user's responsibility. The event of a key loss is inevitable at some point in time. We incorporate a solution for key recovery based on One-Time Pad (OTP), a secure encryption algorithm [14]. The OTP is a long string of random characters. It must be at least as long as the private key. To encrypt the private key, each character from the private key is XORed with the corresponding character from the OTP. This recovery key can be stored on blockchain. The private key could be lost in events such as the mobile device gets damaged or when the private key gets deleted accidentally. In such circumstances, the private key can be retrieved from the recovery key. Since the adversary does not know the OTP, the only option for the adversary to get the private key is by executing a brute force attack. The brute force is practically impossible if the encrypted key is at least 128 bits long [14]. We use a private key of 256 bits. Hence, it is practically impossible for the adversary to decrypt the encrypted private key.

B. The Operation of DID and VC

The operation of DID and VC in the EV charging scenario is illustrated in Figure 1 [5] and [6]. The main blocks and the operations in Figure 1 are briefly explained below.

DID Subject: A DID subject (user) creates his/her DID and controls it.

DID Resolution: The DID resolves to a DID document. A system component called DID resolver takes the DID as input and returns the corresponding DID document as output. The DID document is stored on decentralized platforms like blockchain and contains information such as the DID subject's public key.

Issuer: A trusted Issuer (USP) signs credentials and issues the VC to the DID subject.

Verifier: The Verifier (CS) verifies the VC of the DID subject before providing services. To interact with the Verifier, the DID subject discloses his/her DID and presents the VC. Then, the Verifier uses the USP's public key to validate the VC. Thus, a trust framework is formed among the involved entities: the DID subject, the Issuer, and the Verifier where trust is established through claims that can be cryptographically verified [5].

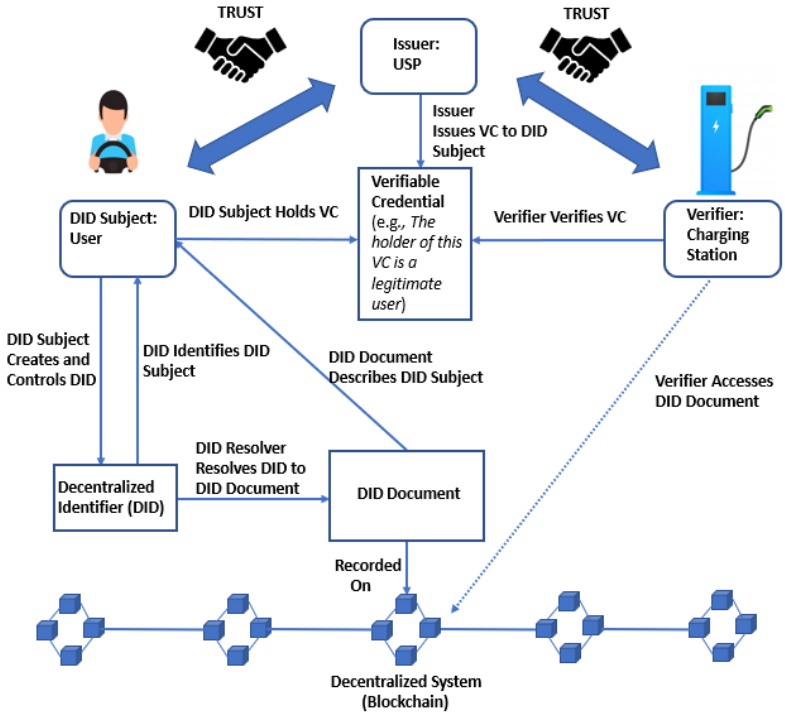

Fig. 1. DID and Verifiable Credential.

C. Motivation

Though several authentication protocols have been proposed in the literature for EV charging, none of them enables user-centric authentication where users have the power to create and control their identities. In the existing works, the users' identities are created and managed by central servers. Information leakage is more likely when all the information is stored on centralized systems. Centralized storage of information also has the risk of being a single point of failure. To address these issues, a user-centric authentication protocol for EV charging based on DID and VC is proposed in this paper. The users create and control their IDs without depending on a central server. They do not reveal their real identities while charging their EVs. At the same time, charging stations can confirm the users' legitimacy by verifying their VCs. The proposed protocol also considers possible loss of user's private key. To address this problem, the proposed protocol incorporates a solution for key recovery.

D. Our Contributions

The main contributions of this work are:

1. A new DID and blockchain-based privacy-preserving user-centric authentication protocol for EV charging: We use the concepts of DID, VC, ZKP, and blockchain together to preserve the privacy of users while charging electric vehicles. The users create their IDs and have full control over it. They use VCs signed by the USP to show their legitimacy.

2. Authenticated Key Agreement: The participants establish a session key through an authenticated key agreement scheme.

3. Key Recovery: The proposed protocol incorporates a solution to recover the private key if it is lost.

The rest of the paper is organized as follows. In Section II, we discuss the system and the adversary model. In Section III, we present the proposed scheme. Performance evaluation of the proposed protocol is presented in Section IV. Finally, we conclude the paper in Section V.

II. System Model

A. System Model

The system model for EV charging is depicted in Figure 2. There are three entities in the model: USP, CS, and users.

USP: A USP consists of power generation and distribution centre, as well as data centre. There are several ways to generate power, including hydroelectric power plants, solar farms, and wind farms. The distribution centre distributes the generated electricity to the CSs at different locations. The USP maintains user information in its data centre. The data centre helps to store and process registered users' information. We assume that USP is a trusted party with sufficient resources to maintain user information in its data centre securely.

CS: CSs are spread out at various locations. The charging rate may change depending on where the CS is located. For example, the charging rate in a city centre may be higher than that in a suburban location to account for the higher operating charges in the city centre.

Users: There are several users, each with a mobile device (MD) connected to the Internet. They use biometrics and a password for two-factor authentication on the MD. Using mobile devices, users communicate with USP and CS through

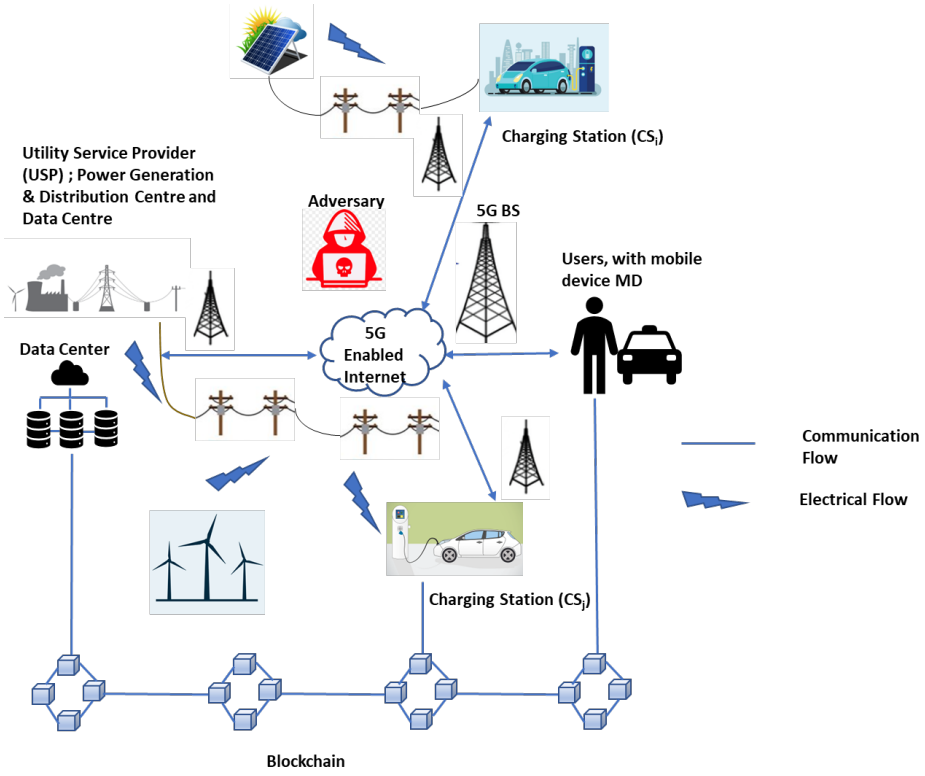

Fig. 2. System model.

the Internet. Each user is required to register once with the USP. After that, the users can charge their EVs at any CS.

The communication between different entities is through the 5G-enabled Internet. We assume that there is reliable network connectivity to carry out the communication. 5G's high reliability, high speed, and low communication latency are all desirable features for an EV charging system to deliver the best user experience. Usage of 5G-enabled Internet enables the system to scale up without disruption to the level of service quality.

B. Adversary Model

In EV charging, there are privacy and security concerns for the users. All parties communicate through an insecure channel, the Internet. An adversary may do a man-in-the-middle attack and may eavesdrop, edit, or delete the messages. While finding a charging station to charge the vehicle and processing payments, the user's details are revealed that poses a privacy risk. Similarly, the user's location details, daily activities, interests, and habits can be tracked. The adversary can impersonate a legitimate user and try to obtain services. On the other hand, a dishonest user can provide wrong location of the charging station to pay lower charges than what should be paid. A dishonest charging station also may impersonate another and demand higher charges from a user. Hence, location checking of the user and the charging station by the trusted party, the USP, and an authenticated key agreement scheme where all the parties agree on a session key are also required.

III. Proposed Protocol

There are three participants in the proposed protocol: Issuer, User, and Verifier. Each entity has a DID and a private/public key pair. Here, USP is the Issuer and charging station is the Verifier. The proposed protocol consists of setup and authentication phases. After authentication, a session key is established among the participants for secure communication. The high-level view of the setup and authentication phases is shown in Figure 3. A flow diagram for the steps involved in the setup and authentication phases is illustrated in Figure 4.

A. Assumptions

The following assumptions are made in the paper:

1. The USP is considered a trusted party. The users and the CSs trust that the USP will not misuse their information. It is also assumed that the USP keeps the sensitive information of the users securely.
2. There is a secure channel for the user to communicate with the USP during the initial setup phase.
3. The USP and the CS do not collude with a malicious intent.

B. Setup Phase

The setup phase consists of the following steps:

Step 1: The USP is a trusted party with a DID DID_{USP}. The charging station, CS_j (the Verifier) has a DID DID_{CSj}. The USP and the CS store their public keys in their DID documents on the blockchain.

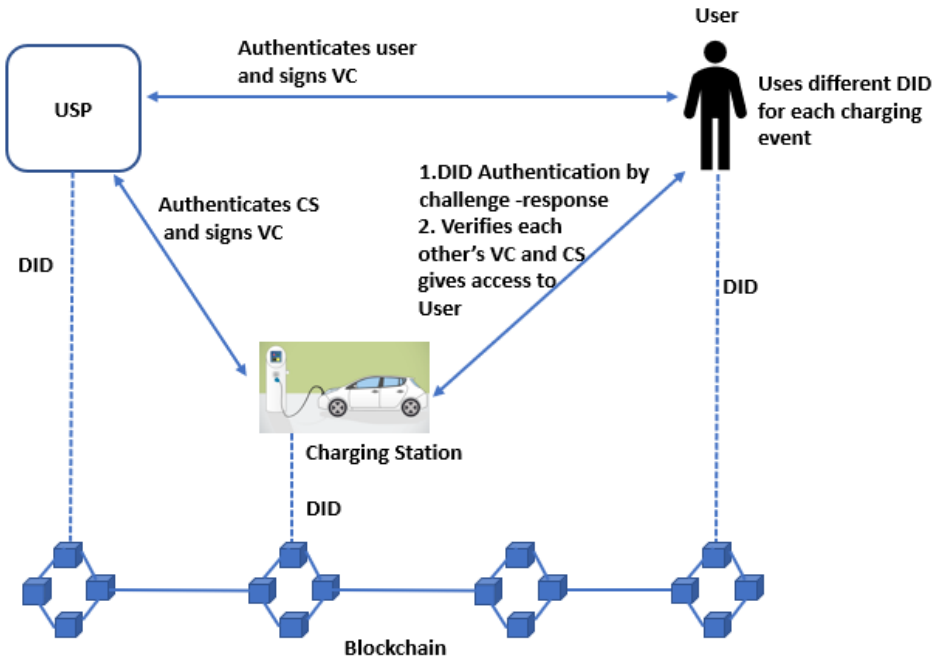

Fig. 3. A diagram showing setup and authentication phases.

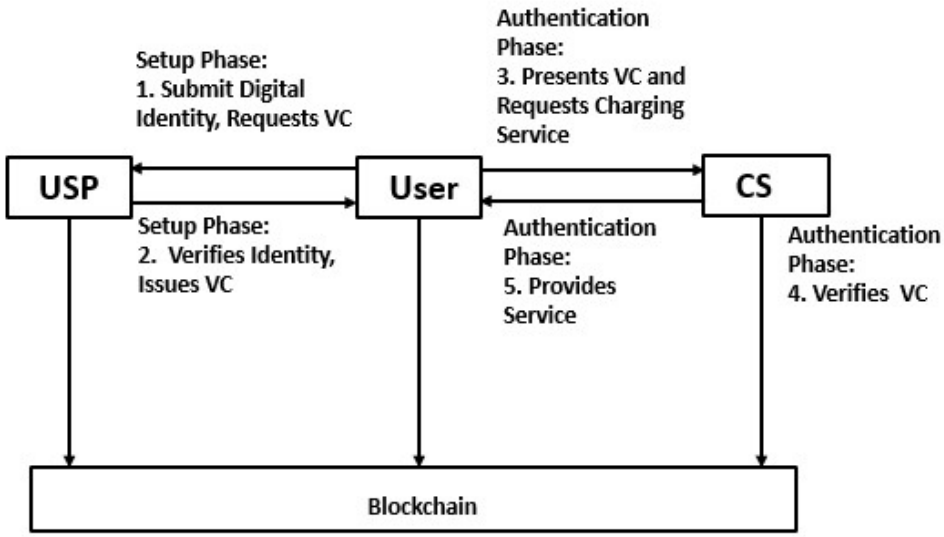

Fig. 4. A flow diagram for the steps involved in the setup and authentication phases.

Step 2: $User_i$ has a DID DID_{useri} and a pair of private and public keys. $User_i$ stores his/her private key in the digital wallet on the mobile device MD_i and the public key in the DID document for DID_{useri} on the blockchain.

Step 3: $User_i$ sends a registration request, a copy of his/her digital identity (ZKP of verifiable credential provided by a trusted government agency), DID_{useri}, and a pseudo-ID $PDID_{useri}$ to the USP.

Step 4: The USP needs to verify the legitimacy of the user. The USP verifies the user's digital identity by checking the government agency's signature on the VC. Then, the USP issues a credential for the user and signs the credential with the USP's private key as a VC. After that, the USP generates a key K_i and stores DID_{useri}, $PDID_{useri}$, and K_i. The USP sends K_i, the credential, and the signature to the user.

Step 5: $User_i$ inputs his/her biometrics and password into his/her mobile device. Its hash is stored on the mobile device for future authentication. $User_i$ stores the credential, the signature, and K_i in the digital wallet on the mobile device.

Step 6: Similarly, the CS also registers with the USP and

receives a credential, a signature, and a key K_j from the USP.

Step 7: This step will help with the key recovery in the future if the private key is lost. A One-Time Pad of the same length as the private key is generated. The user generates a recovery key from the private key by performing XOR operation with the OTP, and stores this OTP encrypted recovery key on the blockchain.

C. Authentication Phase

To use the services offered by CS_j, $User_i$ must go through the authentication process. $User_i$ also should authenticate CS_j to ensure that it is not a malicious party.

Step 1: $User_i$ inputs his/her biometrics and password into his/her mobile device. Then, $User_i$ and CS_j disclose their DIDs to each other. Both parties resolve the DID to the corresponding DID document on the blockchain. Both the user and the CS obtain each other's public key from the DID document and encrypt a challenge with the public key obtained from the DID document. Then, they send the encrypted challenge to each other. The recipient decrypts the encrypted challenge using its private key and replies with the response. Each party verifies the validity of the other party's DID by comparing the response received with the challenge sent.

Step 2: $User_i$ creates a ZKP of the credential using the ZKP prove algorithm to show that he/she holds a valid credential. Then, $User_i$ XORs the location details with K_i. $User_i$ composes a message with the generated ZKP, the signature obtained from the USP, and the encoded location details. Then, $User_i$ encrypts the message with the public key of CS_j and sends it to CS_j. Thus, only the intended recipient, CS_j, with the private key can decrypt the message. This encryption prevents eavesdropping by an adversary. Upon receiving the message, CS_j decrypts it with its private key. Then, CS_j preforms signature verification on the received signature by using the public key of the USP. CS_j also verifies the user's ZKP using the ZKP verify algorithm. From the ZKP, CS_j is not able to learn anything other than the fact that the user holds a valid credential. Similarly, the user also verifies the CS's VC. After that, CS_j XORs its location details with K_j and sends it to the USP together with the encoded location details from $User_i$.

Step 3: The USP decodes the message and compares the location details received from $User_i$ and CS_j and ensures that they are the same. After that, the USP generates a new VC, encodes it with K_i, and sends it to the user. This new VC can be used for authentication during the next charging event. Changing the VC of the user for each charging event ensures that the user can't be tracked. Then, the USP generates a session key, encodes it, and sends it to CS_j and $User_i$.

Step 4: CS_j and $User_i$ store the session key received from the USP. Thus, a session key is established between the user and the CS.

Step 5: If the user loses the private key, the recovery key stored on the blockchain can be retrieved. Then, by performing XOR operation with the One-Time Pad, the private key can be recovered.

Scenario 1: If a person wants to charge his vehicle multiple times a day, he/she must go through the authentication process before charging each time as the charging station does not keep any information about the user.

Scenario 2: The proposed protocol supports a shared vehicle scheme as well. In a shared vehicle scheme, each user must register separately with the USP and use their own DIDs and VCs to request for EV charging.

IV. Performance Evaluation

We first evaluate the proposed scheme based on security properties achieved. Then, we present the computation cost of the proposed scheme.

A. Security Properties

The proposed protocol achieves the following security properties:

Privacy of the User: The user's identity is not revealed while charging the EV. The user provides a proof that he/she is a valid user without revealing his/her real identity by making use of the DID and the VC. Hence, our scheme makes it difficult for an adversary to track a user's presence in a location, daily habits, and trajectory.

Unlinkability: By using DID instead of real identity, the proposed scheme breaks the link between the user's real identity, location, and the time of charging. The DID and VC used during each authentication event is different. Hence, an adversary can't link two authentication events of the same user.

Mutual Authentication: In the proposed scheme, both user and CS authenticate each other by verifying each other's DID and VC.

Non-Repudiation: VC mechanism works on asymmetric cryptography. The user and the CS verify the signature on VC by using the USP's public key. This ensures non-repudiation since the private key used to sign the VC is only known to the USP. The USP that signed the credential cannot deny having signed it.

Accountability: Both the user and the charging station verify each other's VC. The VCs are signed by the trusted party, the USP. The USP has verified legitimacy of the user and the CS, thus providing accountability.

Session Key Agreement: At the end of the authentication process, a session key is established between the CS and the user. Hence, the proposed method ensures session key agreement.

Protection Against Impersonation Attacks: An adversary can't provide the same biometrics and password as a legitimate user. Hence, the adversary can't use the mobile device where the user's private key is stored. Another protection is provided by comparing the location information of the user and the CS. This prevents a user from providing a forged location id to pay lower amount for charging and prevents the CS from giving a forged location to charge the users more than the actual amount.

Protection Against Replay Attacks: In a replay attack, the adversary captures messages and replays it later to get

authenticated. During authentication, the parameters used are changed in each session. Hence, the adversary can't execute a replay attack.

Protection Against Eavesdropping and Man-In-The-Middle Attacks: To perform eavesdropping and man-in-the-middle attacks, the adversary needs to eavesdrop on the messages and modify them. During authentication, both user and CS encrypt the messages with the public key of the recipient. Thus, only the legitimate recipient with the private key can decrypt the message. Thus, the proposed protocol provides protection against eavesdropping and Man-In-The-Middle attacks.

B. Security Analysis

In this section, we compare the proposed protocol with two other schemes [3] and [15] for EV charging based on the security properties achieved. The major characteristic that sets the proposed scheme apart from others is user-centric authentication. The proposed scheme also provides non-repudiation that is not provided by the other schemes. The proposed scheme prevents the user and the CS from providing a forged location while [15] does not provide that feature.

C. Computation Cost

The setup phase is carried out only once since the user is required to register with the USP only once. Hence, the performance of the proposed method depends mainly on the performance during authentication. In this section, we evaluate the performance of the proposed protocol based on the computation cost incurred during authentication.

TABLE I
COMPUTATION COST DURING AUTHENTICATION

Operation	User's Device	CS	USP
$Encryption$	2	2	0
$Decryption$	2	2	0
$Signature\ Generation$	0	0	1
$Signature\ Verification$	1	1	0
Computation Time (ms)	28.93	28.93	29.17

To perform the simulations, we employed a personal computer with Intel (R) Core (TM) i5-11320H @3.20 GHz and 8 GB of RAM memory. The main operations involved in authentication are encryption, decryption, signature generation, and verification. The time taken by other operations such as XOR is negligible. With an implementation in Python, ECDSA signature generation, verification, encryption, and decryption take 29.17 ms, 20.11 ms, 2.18 ms, and 2.23 ms, respectively. The number of operations performed and the total approximate execution time taken by each entity during authentication is given in Table I. The user and the CS perform encryption and decryption operations while executing the challenge-response procedure in Step 1 of the authentication phase. Then, the user and the CS perform encryption and decryption once again in Step 2 of the authentication phase. Hence, the user's device and the CS each takes $2 \times 2.18 + 2 \times 2.23 + 20.11 = 28.93$ ms and the USP takes 29.17 ms to complete one round of authentication.

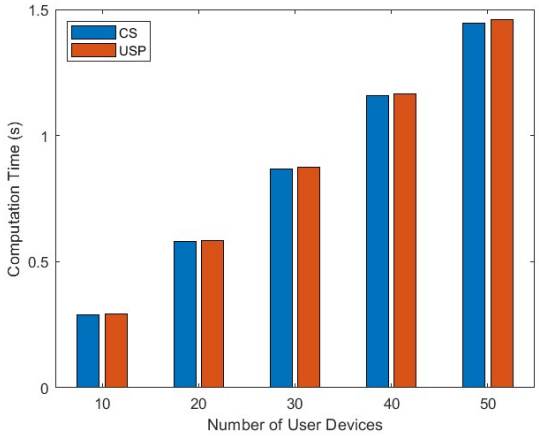

Fig. 5. Effect of number of users on computation time.

We now examine how the computation time changes as the number of users increases. When the number of users increases, the CS and the USP must authenticate each user and the computation time increases accordingly. For example, when there are 10 users, the CS takes 0.2893 s and the USP takes 0.2917 s to authenticate all of them. The computation time taken by the CS and the USP during authentication is plotted against the number of users in Figure 5. The increase in computation time with an increase in the number of users is reasonable since the USP and the CS are not resource-constrained. Hence, the proposed protocol is scalable.

V. CONCLUSION

In this paper, we proposed a user-centric authentication protocol for electric vehicle charging based on DID, VC, and ZKP which can be built on blockchain. The proposed protocol enables users to create and manage their IDs and charge their EVs in a privacy-preserving manner. The proposed scheme also incorporates a method to recover the private key of the user if it is lost. It helps to achieve several security properties. Our evaluation has shown that the computational cost is reasonable and the proposed protocol is scalable. One limitation of using DID and VC for authentication is that the proposed mechanism can only be implemented if all stakeholders accept a DID framework. This process can be expensive and time-intensive.

REFERENCES

[1] C. Chan and K. Chau, "An overview of power electronics in electric vehicles," *IEEE Transactions on Industrial Electronics*, vol. 44, no. 1, pp. 3–13, 1997.

[2] G. Haddadian, M. Khodayar, and M. Shahidehpour, "Accelerating the global adoption of electric vehicles: barriers and drivers," *The Electricity Journal*, vol. 28, no. 10, pp. 53–68, 2015.

[3] P. Gope and B. Sikdar, "An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6607–6618, 2019.

[4] "How can 5G operators enable an electric future," Online, https://www.automotiveworld.com/articles/how-can-5g-operators-enable-an-electric-future/, [Accessed: Aug 2022].

[5] "Decentralized Identifiers (DIDs)," Online,https://www.w3.org/TR/did-core/, [Accessed: Aug 2022].

[6] "Own your digital identity," Online, https://www.microsoft.com/en-sg/security/business/identity-access-management/decentralized-identity-blockchain, [Accessed: Aug 2022].

[7] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "Roaming electric vehicle charging and billing: An anonymous multi-user protocol," in *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2014, pp. 939–945.

[8] H. Nicanfar, S. Hosseininezhad, P. TalebiFard, and V. C. Leung, "Robust privacy-preserving authentication scheme for communication between electric vehicle as power energy storage and power stations," in *2013 Proceedings IEEE INFOCOM*. IEEE, 2013, pp. 3429–3434.

[9] "Verifiable Credentials Data Model 1.0," Online, https://www.w3.org/TR/vc-data-model/, [Accessed: Aug 2022].

[10] Y. Kortesniemi, D. Lagutin, T. Elo, and N. Fotiou, "Improving the privacy of iot with decentralised identifiers (dids)," *Journal of Computer Networks and Communications*, vol. 2019, 2019.

[11] M. Eisenstadt, M. Ramachandran, N. Chowdhury, A. Third, and J. Domingue, "Covid-19 antibody test/vaccination certification: there's an app for that," *IEEE Open Journal of Engineering in Medicine and Biology*, vol. 1, pp. 148–155, 2020.

[12] J. Groth, "On the size of pairing-based non-interactive arguments," in *Annual international conference on the theory and applications of cryptographic techniques*. Springer, 2016, pp. 305–326.

[13] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Computer Science-Research and Development*, vol. 33, no. 1, pp. 71–79, 2018.

[14] S. M. Smith and V. Gupta, "Decentralized autonomic data (dad) and the three r's of key management," White Paper, May 2018. [Online]. Available: https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/DecentralizedAutonomicData.pdf/

[15] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for v2g using physical unclonable function," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7234–7246, 2020.

Rohini Poolat Parameswarath received the Master of Technology degree in Software Engineering from the National University of Singapore, Singapore in 2009. She is a cyber security researcher at the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. Currently, she is pursuing a PhD with research focusing on protocols for security and privacy in vehicular environments. Prior to joining the National University of Singapore, she was part of the cyber security research team at the Singapore University of Technology and Design, Singapore. Before embarking on her career in cyber security research, she worked as a software engineer in multinational companies. She is passionate about finding solutions to the current challenges in the cybersecurity landscape. Her research interests include cyberattack detection, ways to prevent attacks, data privacy, and cryptographic protocols in domains such as Internet of Things (IoT), cyber-physical systems, and vehicular networks.

Prosanta Gope (Senior Member, IEEE) is currently working as an assistant professor with the Department of Computer Science (Cyber Security), University of Sheffield, U.K. He served as a research fellow with the Department of Computer Science, National University of Singapore. He has authored more than 100 peer-reviewed articles in several reputable international journals and conferences and has four filed patents. Several of his papers have been published in high-impact journals, such as IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Industrial Electronics, and IEEE Transactions on Smart Grid. Primarily driven by tackling challenging real-world security problems, he has expertise in lightweight anonymous authentication, authenticated encryption, access control, security of mobile communications, healthcare, the Internet of Things, Cloud, RFIDs, WSNs, smart-grid, and hardware security of the IoT devices. He has served as the TPC Member/Chair in several reputable international conferences, such as ESORICS, IEEE TrustCom, ARES, etc. He currently serves as an associate editor for IEEE Internet of Things Journal, IEEE Systems Journal, IEEE Sensors Journal, and the Journal of Information Security and Applications (Elsevier).

Biplab Sikdar is an Associate Professor in the Department of Electrical and Computer Engineering at the National University of Singapore, where he also serves as the Interim Head of the Department of Electrical and Computer Engineering. He received the B. Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He was an Assistant Professor from 2001-2007 and Associate Professor from 2007-2013 in the Department of Electrical, Computer, and Systems Engineering at Rensselaer Polytechnic Institute from 2001 to 2013. He is a recipient of the NSF CAREER award, the Tan Chin Tuan fellowship from NTU Singapore, the Japan Society for Promotion of Science fellowship, and the Leiv Eiriksson fellowship from the Research Council of Norway. His research interests include IoT and cyber-physical system security, network security, and network performance evaluation. Dr. Sikdar is a member of Eta Kappa Nu and Tau Beta Pi. He has served as an Associate Editor for the IEEE Transactions on Communications, IEEE Transactions on Mobile Computing, and IEEE Internet of Things Journal and is an IEEE COMSOC and VTS Distinguished Lecturer and ACM Distinguished Speaker.