A STUDY ON DID AND CP-ABE-BASED SELF-SOVEREIGN IDENTITY OF SMART VEHICLES

Taehoon Kim and Im-Yeong Lee

Department of Software Convergence, Soonchunhyang Univ., Asan-si 31538, Republic of Korea.

ABSTRACT

In existing smart vehicles, vehicle owners must secure self-sovereignty for authentication. To this end, Holders in DIDn(Decentralized Identifier) do not rely on traditional IdM (Identity Management), but control their identity data and authenticate their credentials with Verifiers. However, for the Verifier to authenticate the Holder, there is a situation where additional data other than the VP is required, and this is because the DID based on data access control is transmitted in a general encryption scheme, causing detailed access control problems and inefficiency problems. Study on CP-ABE (Ciphertext Policy Attribute-BasedEncryption)-based data access control schemes in the DID is being actively conducted to solve this problem. However, existing schemes on DID-based CP-ABE generate various security threats. This paper proposes a study on DID and CP-ABE-based self-sovereign identity of smart vehicles.

KEYWORDS

Smart Vehicle, Decentralized Identifier, Self-Sovereign Identity, Ciphertext Policy Attribute-Based Encryption

1. INTRODUCTION

As IT (Internet Technology) develops, data has become important, affecting smart vehicles. As a vehicle is connected to the Internet, a vast amount of data is generated. If personal information is included among the generated data, it must be managed carefully and importantly.

To this end, the DID (Decentralized Identifier) system, which allows users to manage their identity information, has begun attracting attention. DID is a new paradigm in which Holders can self-control their unique identifiers and data without relying on a single central system or third-party authority to manage their credentials [1, 2]. In other words, unlike existing identification schemes, DID is not controlled by a central system and is a scheme that allows individuals to have complete control over their information. Furthermore, the characteristic of DID is that the Holder (user), the subject of data sovereignty, secures their data sovereignty [1].

Recently, a standard for DID has been established by the W3C (World Wide Web Consortium), and based on this, and DID is being studied and used in various fields. However, when authenticating in a DID environment, there are cases where the Verifier requests additional data other than credentials from the Holder. For example, a vehicle owner (Holder) wants to authenticate a service provider (Verifier) for data communication and service. At this time, the vehicle owner must provide credentials containing personal identification data and share

David C. Wyld et al. (Eds): NLPML, AIAP, SIGL, CRIS, COSIT, DMA -2023
pp. 147-158, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.130812

historical data related to the vehicle with the Verifier. However, access control for previous data related to vehicles stored in the VDR is not provided for service providers, so authority verification is not performed [3-4]. Therefore, service providers can indiscriminately access previous vehicle-related data. To solve these problems, existing DID must provide confidentiality and access control for the vehicle-related historical data stored in the VDR.

For confidentiality and data access control, study on user data access control schemes such as ABE (Attribute-Based Encryption), PRE (Proxy Re-Encryption), and ZKP (Zero-Knowledge Proof) is continuously being conducted. Among these studies, schemes using CP-ABE (Ciphertext Policy Attribute-Based Encryption) in the DID environment are being studied. However, this has the following problems.

First, it does not prove to the VDR that the Verifier has authorized access to Holder's vehicle-related identity data.

Second, data misuse and abuse occur due to unauthorized Verifiers' illegal access.

Third, in the existing CP-ABE, the output length of the ciphertext increases as the number of attributes of the attribute set, which is the input value of the access structure, increases. As a result, in the case of the CP-ABE-based data access control scheme in the DID environment, overhead for the storage capacity of the VDR occurs. In addition, there are various security threats, and they are presented as targets to be resolved before applying secure DID.

This paper analyzed CP-ABE access control scheme in the existing DID environment to solve the abovementioned problems. This proposed scheme provides the following contributions.

- **Verification of approval of access rights to Holder's data**: The Verifier provides an access token to the VDR to prove that the Holder has approved access to their data. Therefore, the VDR verifies that the Holder has approved the Verifier.
- **Deny data access using Verifier revocation**: VDR verifies Holder approval and Verifier withdrawal based on Holder credentials and user list. Therefore, the Verifier who has withdrawn cannot access Holder's data.
- **Minimize storage capacity for limited resources**: The Holder can output ciphertext of a certain size so that it is not affected by the number of attributes during encryption. This reduces the storage capacity overhead of the VDR.

To this end, this Section analyzes the background, and existing related schemes. Next, Section 3 presents the requirements for this proposed scheme, and Section 4 proposes entities and protocols for this proposed scheme. Next, Section 5 compares and analyzes the requirements presented in Section 3 with existing related studies. Finally, Section 6 concludes with the conclusion of this proposed scheme.

2. RELATED WORK

In this section, we analyze DID, CP-ABE, and existing schemes, which are used in this paper, and discuss existing schemes.

2.1. Decentralized Identifier

By the principle of SSI (Self-Sovereign Identity), DID allows users to control and manage their personal information by disclosing minimum personal information and claims [5, 6].

Furthermore, DID uses a distributed system such as blockchain to provide decentralization. In addition, a DID authentication scheme based on data access control can be configured as a blockchain-based on/off-chain [7]. And the system scenario of DID is shown in Figure 1.

2.1.1. System Entities

A brief description of DID entities.

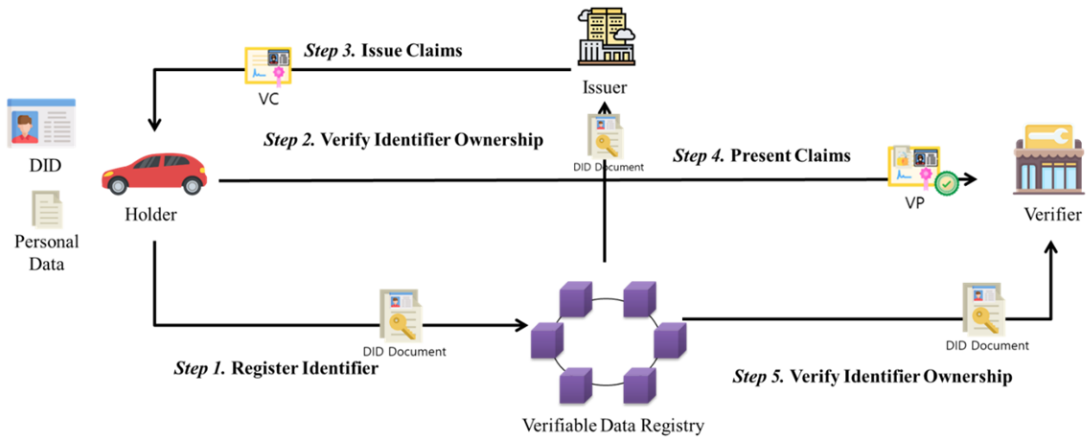

Figure 1. Scenario of DID

- **Holder**: As the subject of data sovereignty, create DID, DDO (DID Document), and VP (Verifiable Presentation) and manage data based on data access control.
- **Issuer**: As a trusted credential Issuer, it creates the Holder's VC (Verifiable Credential).
- **Verifier**: As a VP Verifier, it performs qualification verification for the Holder's VP and decrypts the ciphertext based on the Holder's authentication and data access control.
- **VDR**: As a verifiable data repository, manages DID and DID documents, Holder's ciphertext.

2.2. Ciphertext Policy Attribute-Based Encryption

CP-ABE [8] operates as shown in Figure 2 and has the following advantages. First, it enables fine-grained access control for encrypted data. Second, if the attribute secret key of the Verifier and the access structure of the ciphertexts stored in the cloud match, several ciphertexts can be decrypted. Through this, CP-ABE can reduce the overhead of communication and storage capacity [9]. Finally, as study on CP-ABE-based data access control in the DID environment progresses, multiple Verifiers solve the problems of sharing secret keys and generating ciphertext for the same data.

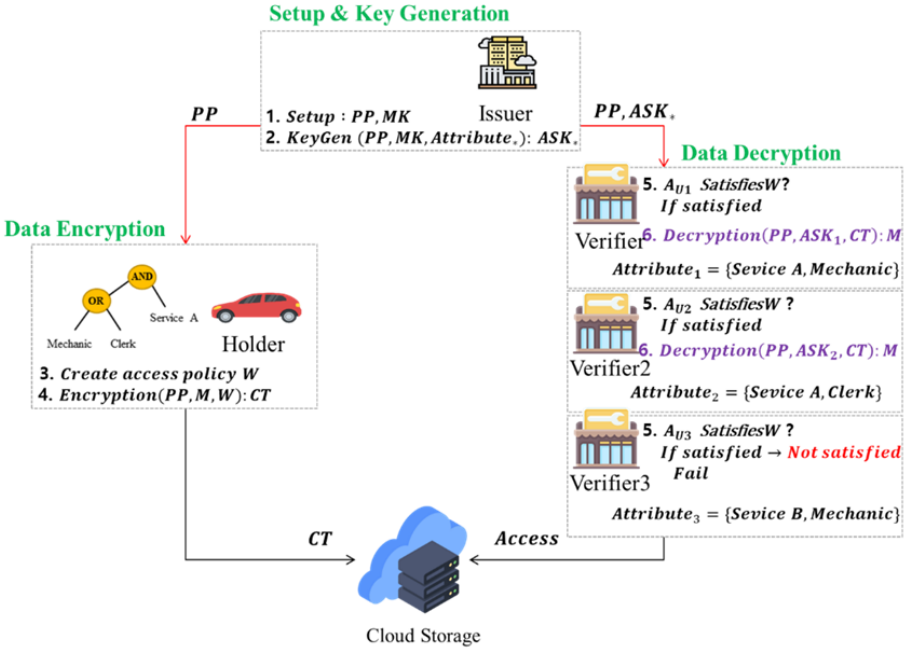

Figure 2. Scenario of CP-ABE

2.3. Related Work

Data access control schemes using CP-ABE in the existing DID environment are analyzed.Schanzenbach et al. [10] proposed an architecture that allows Holders to discover digital IDs by securely sharing ID attributes with Verifiers without a centralized Identity Provider (IdP). Schanzenbach et al. In this scheme, Holders can manage their attributes in the Name System and optionally grant access to Verifiers.

The Soltani et al. [11] scheme minimizes data so that the Verifier provides a service to the Holder. In addition, the scheme uses data capsules to protect Holder's personal information. It transfers personal data between the Holder and Verifier 1:1. However, Holders must send an encrypted text to Verifiers whenever they request data access, resulting in an inefficient problem. Furthermore, since the Verifier is not revoked, there is a problem that the unsubscribed Verifier can access the ciphertext. As the number of attributes increases, the scheme includes attribute-related information in the ciphertext. Therefore, the output length of the ciphertext increases. Moreover, suppose the Verifier wants to access Holder data stored in the VDR.

Xiao et al. [12] proposed encryption and partial decryption by modifying the Blockchain-based Self-Sovereign Identity Management (BbSSIM) scheme and the CP-ABE of Threshold. The Xiao et al. scheme records information about Verifiers from which the Issuer has withdrawn in the Attribute Revocation List to protect the user's personal information for key generation and data access. Furthermore, the Issuer records and transmits the Attribute Revocation List to the VDR. Moreover, since the file list is used to request the cipher text to the VDR, the ciphertext search function is provided.

3. REQUIREMENTS

This section describes the requirements for this proposed scheme. The system of this proposed scheme must satisfy the following requirements.

- **Verification of approval of access rights to Holder's data**: In DID, data access control should transfer the ownership of verification data to the holder, ensuring self-sovereignty. To ensure this, the verifier must be able to verify with the VDR that the holder has been granted access to the holder's data. Thus, the holder must prove it by including cryptographic data that only the holder of the verification data can create in the VP.
- **Deny data access using Verifier revocation**: This is a problem that occurs when using CP-ABE in a DID environment. The Holder outputs the ciphertext using the access structure created based on the Holder's data to be encrypted and the attributes that can decrypt the ciphertext. However, as the number of attributes increases in the process of generating the access structure, the output length of the ciphertext increases. To solve this problem, when Holder encrypts its information, it must be able to output the ciphertext of a specific length without being affected by the number of selected attributes.
- **Minimize storage capacity for limited resources**: In the existing DID environment, in the CP-ABE-based data access control scheme, if the VDR does not search for the ciphertext requested by the verifier, it cannot find the ciphertext requested by the verifier cannot transmit it. To solve this, the VDR must be able to find the correct ciphertext and send it to the verifier.

4. PROPOSED SCHEME

In this section, we propose a study on DID and CP-ABE-based self-sovereign identity of smart vehicles, satisfying the requirements presented in Section 3. As shown in Figure 3, this proposed scheme consists of setting, issuance, key generation, claim proof, access, and verifier revocation.

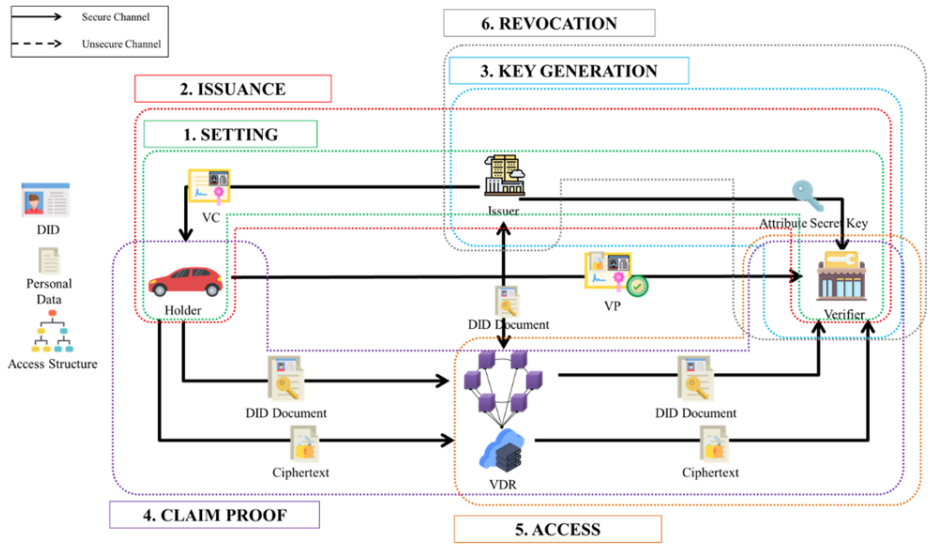

Figure 3. Flow of proposed scheme

4.1. System Entities

The system entity of this proposed scheme is as follows.

- **Holder (Vehicle Owner)**: As the vehicle owner, the Holder, the subject of data sovereignty, verifies personal data from the Issuer, receives the VC, and then receives the authentication service from the Verifier through the VP.
- **Issuer**: The Issuer is a trusted institution that verifies the Holder's personal data and issues VC to the Holder.
- **Verifier (Service Provider)**: The Verifier is a service provider that verifies the Holder's VC and provides services to the Holder.
- **Verifiable Data Registry (VDR)**: VDR is personal data store that stores and manages all entities' personal data and DID-related data when authenticating entities.

4.2. System Parameters

Table 1 shows the system parameters used in the proposed scheme.

Table 1. System parameters.

Symbol	Definition
*	Participant entities mean the Holder, Issuer, and Verifier collectively
p, q	Large prime number
G_1, G_2	Addition group and multiple group
g	Generator of G_1
e	Pairing function
DID_*, DDO_*	Participant's DID and DID document
PP_I, MK_I	Issuer generated public parameters and master key
$H_1()$	Cryptographic hash function, $H_1: \{0,1\}^* \rightarrow Z_p^*$
M_H	Holder's personal data
CT_H	Ciphertext of Holder's personal data
EVC_H	Holder's verifiable data credentials
AVC_V	Verifier's verifiable attribute credentials
$Att_V, \ldots, Att_{V_j}$	Holder chosen Verifier's attributes
$Aset_V$	Verifier's owned attribute set
W_H	An access structure created based on the Holder's chosen attributes
nc_V, rnc_V	Nonce and updated nonce
UL_I	List of users managed by the issuer
VP_H	Holder's verifiable presentation
ASK_V	Attribute-based secret key

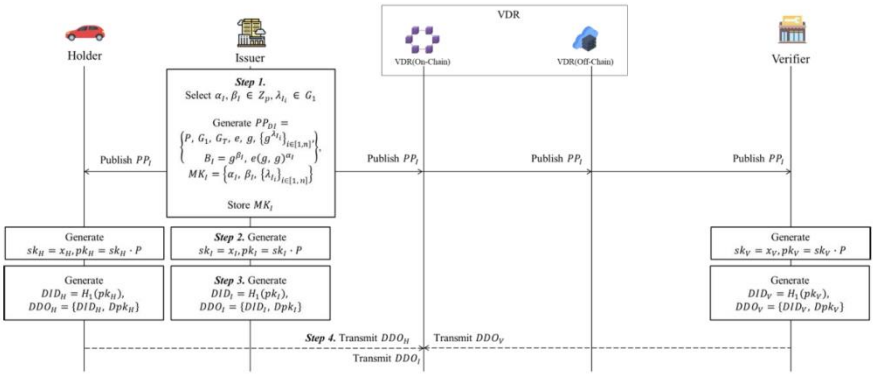

Figure 4. Setting

4.3. Proposed Scheme

4.3.1. Setting

In the setting, the Issuer generates common data necessary for all entities. And the Holder, Issuer, and Verifier register themselves in the VDR's On-Chain.

Step 1: The Issuer selects a random numbers $\alpha_I, \beta_I \in Z_p$, generator $\lambda_{I_i} \in G_1$, creates the public parameter PP_I, and the master key MK_I. Afterwards, Issuer publishes PP_I to all entities and securely stores MK_I.

Step 2: Participants select a prime number x_* on Z_p, use it as a private key sk_*, and generates and publishes each participant's public key pk_*.
Step 3: The participants hash pk_* to generate identifier values DID_* and DDO_*.

Step 4: The participant transmits DDO_* to the VDR's On-Chain.

4.3.2. Issuance

In the issuance, the Holder encrypts their personal data for data access and uploads it to VDR's Off-Chain. Moreover, Moreover, the Issuer issues verifiable data credentials to the Holder

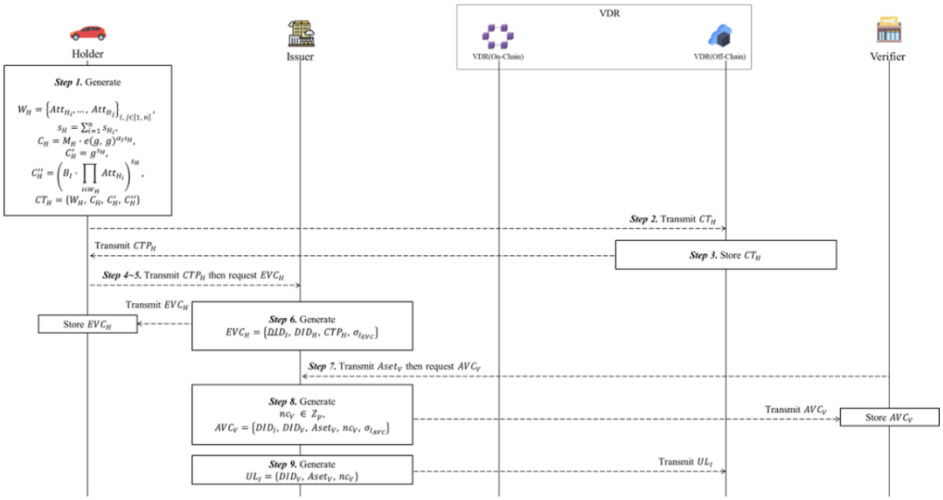

Figure 5. Issuance

associated with the ciphertext stored in the VDR. Finally, a verifiable attribute credential containing the attributes of the verifier is issued to the Verifier.

Step 1: To encrypt his personal data, Holder selects the verifier attribute $\{Att_{H_i}, \ldots, Att_{H_j}\}_{i,\, j\in[1,n]}$ that can decrypt it, creates access structure W_H. Input the holder's personal data M_H , W_H, PP_I to generate the ciphertext CT_H.

Step 2: The Holder transmits CT_H to VDR's Off-Chain.

Step 3: VDR' Off-Chain securely stores CT_H and transmits the stored path CTP_H to the Holder.

Step 4: Upon receiving CTP_H, the Holder transmits CTP_H to the VDR's On-Chain.

Step 5: The Holder sends CTP_H to the Issuer, requesting verifiable data credentials.

Step 6: Upon receiving this, the Issuer generates a verifiable data credential EVC_H and sent to the Holder, who stores it securely.

Step 7: The Verifier sends $Aset_V = \{Att_{V_1}, \dots, Att_{V_n}\}_{i\in[1,n]}$ to the Issuer, requesting verifiable attribute credentials AVC_V.

Step 8: Upon receiving this, the Issuer selects nonce $nc_V \in Z_p$ to generates the verifiable attribute credential AVC_V, and the AVC_V is sent to the Verifier and securely stored.

Step 9: Afterwards, the Issuer generates user list UL_I using Verifier's DID_V, attribute set $Aset_V$, nc_V, and transmits UL_I to VDR's Off-Chain for storage.

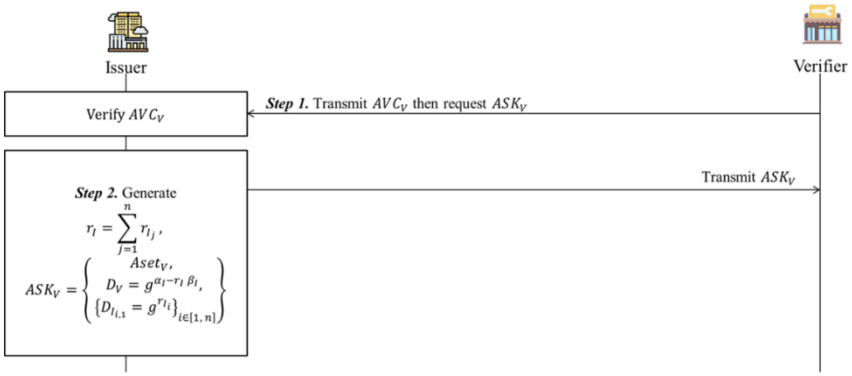

Figure 6. Key generation

4.3.3. Key Generation

In the key generation, the Verifier transmits AVC_V to the Issuer for ciphertext decryption, and the Issuer generates a private key corresponding to the attributes of the verifier and sends it to the Verifier.

Step 1: The Verifier sends its own AVC_V to the issuer and requests the generation of a corresponding attribute secret key.

Step 2: The Issuer sets the Verifier's attributes set $Aset_V$, selects a random number for each attribute $r_{I_j} \in Z_p$, calculates r_I as follows, and uses MK_I, PP_I, $Aset_V$, r_I to generate the Verifier's attribute secret key ASK_V and transmit it to the Verifier.

4.3.4. Claim Proof

In the claim proof, the Holder sends a verifiable data credential to the Verifier to be served, and the Verifier verifies it.

Step 1: The Holder uses $\{EVC_{H_a}, \dots, EVC_{H_b}\}_{a,b\in[1,n]}$ to generate VP_V and then transmits it Verifier.

Step 2: The Verifier verifies $\sigma_{H_{EVCs}}$ included in VP_V and $\sigma_{I_{EVC}}$ included in EVC_H.

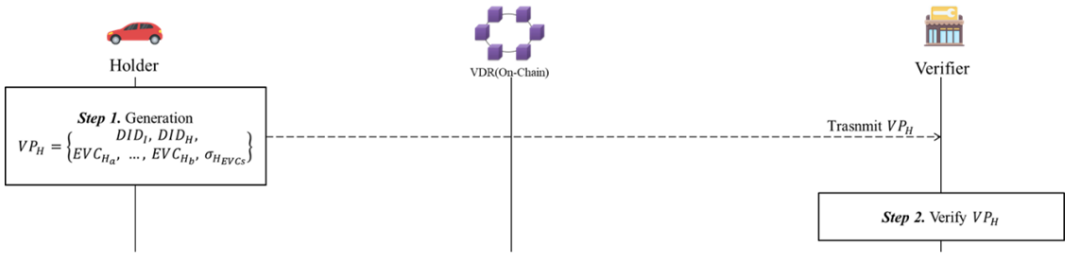

Figure7. Claim proof

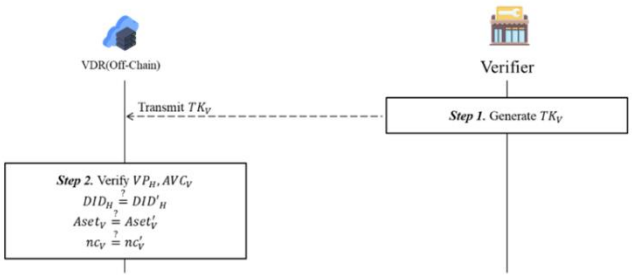

Figure 8. Access

4.3.5. Access

In access, the Verifier creates an access token to access the Holder's data stored Off-Chain in the VDR. Off-chain then verifies the Verifier's right to access the data and the Holder's authorization.

Step 1: The Verifier creates an access token TK_V using AVC_V, VP_H to access the Holder's personal data.

Step 2: The Verifier transmits TK_V to VDR's Off-Chain, and Off-Chain verifies signature values $\sigma_{I_{AVC}}$, $\sigma_{H_{EVCs}}$, $\sigma_{I_{EVC_a}}$, ..., $\sigma_{I_{EVC_b}}$ included in AVC_V, VP_H.

4.3.6. Revocation

In the revocation, revocation is performed to retrieve the previous authority if a registered Verifier wants a revocation.

Step 1: The Verifier sends its own AVC_V to the issuer and requests withdrawal. The requested Issuer extracts $DID'_V, Aset'_V, nc'_V$ from AVC_V and compares them with the values contained in UL_I.

Step 2: If the above values are the same, the issuer selects a random number $rnc_V \in Z_p$, updates the Verifier's nc_V in UL_I to rnc_V, and then withdraws the registered verifier.

Step 3: The Issuer sends the updated UL_I to VDR's Off-Chain, and the Off-Chain stores it.

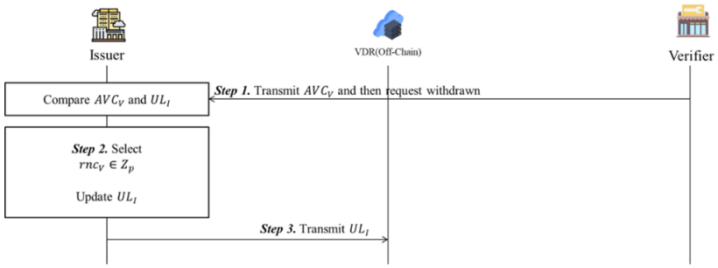

Figure 9. Revocation

5. ANALYSIS OF PROPOSED SCHEME

In this section, we analyze the proposed scheme and existing schemes based on the requirements presented in Section 3.

- **Verification of approval of access rights to Holder's data**: This proposed scheme presents VP_H to the Off-Chain of VDR to prove that the holder authorizes the verifier. Furthermore, the verifier presents AVC_V, including $Aset_V$,nc_V, to the VDR's Off-Chain to prove whether or not he/she has withdrawn. Afterward, the VDR compares DID_V, $Aset_V$, nc_V included in the UL_I received from the issuer with DID'_V, $Aset'_V$, nc'_V included in AVC_V.

- **Deny data access using Verifier revocation**: VDR verifies Holder approval and Verifier withdrawal based on Holder credentials and user list. Therefore, the Verifier who has withdrawn cannot access Holder's data.

$$\boldsymbol{DID_V} \stackrel{?}{=} \boldsymbol{DID'_V}$$
$$\boldsymbol{Aset_V} \stackrel{?}{=} \boldsymbol{Aset'_V}$$
$$nc \stackrel{?}{=} nc'$$

- **Minimize storage capacity for limited resources**: In this proposed scheme, Holder outputs ciphertext with a specific length without being affected by the number of attributes through the following aggregation operation. Moreover, this is not affected by the number of attributes, even in the decryption operation.

Table 2. Analysis of proposed scheme.

Requirements	[10]	[11]	[12]	Proposed Scheme
Verification of approval of access rights to Holder's data	X	X	X	O (VP Verification)
Deny data access using Verifier revocation	O (Attribute's Version Control)	X	O (Attribute Revocation List)	O (User List)
Minimize storage capacity for limited resources	X (No Compre-ssion)	X (No Compre-ssion)	X (No Compre-ssion)	O (Compression)

O: Provided, X: Not Provided

6. CONCLUSIONS

As data becomes more important, data management is also emerging in smart vehicles. To solve this problem, as research and development of DID are in the limelight, the verifier must access the holder's sensitive data when authenticating the holder in the DID environment. Moreover, existing schemes have proposed data access control during authentication using CP-ABE in a DID environment to provide this. However, approval cannot be proven when the verifier accesses

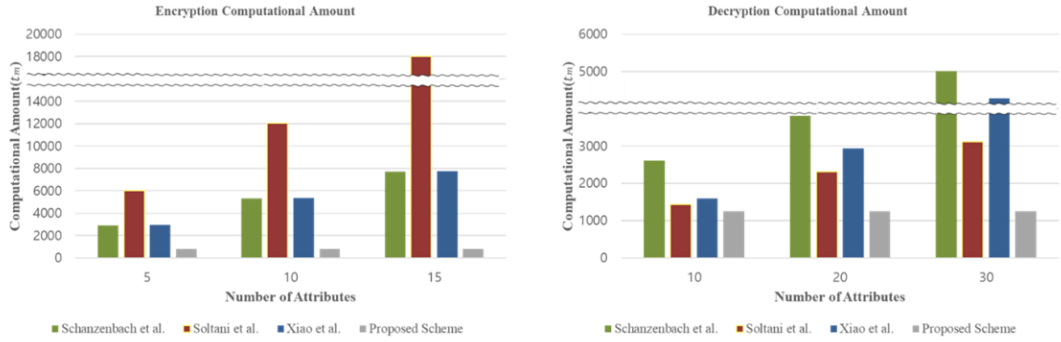

Figure 10. Analysis of proposed scheme

the holder's data. Moreover, when the registered verifier withdraws, verification of whether or not the verifier has withdrawn is not provided. Also, since the number of attributes is proportional to the output length of ciphertext, problems such as overhead occur in the storage capacity of the VDR.

This proposed scheme proposes a CP-ABE-based access control scheme for self-sovereign identity in a DID environment to solve this problem. In this proposed scheme, VDR's Off-Chain can verify whether the verifier is a verifier authorized by the holder and can verify whether it is a verifier that has withdrawn. In other words, when requesting data access, the Off-Chain of VDR verifies withdrawal and determines whether to transmit data. Therefore, this proposed scheme minimizes the exposure of the ciphertext. In addition, it is possible to output a specific length of ciphertext that is not affected by the number of attributes.

This proposed scheme guarantees user self-sovereign identity using data access based on DID and CP-ABE in resource-limited environments using IoT, such as smart vehicles.

ACKNOWLEDGEMENTS

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (RS-2022-00167197, Development of Intelligent 5G/6G Infrastructure Technology for The Smart City) and this word was funded by BK21 FOUR (Fostering Outstanding Universities for Research)(No.:5199990914048) and this work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2022R1A2B5B01002490) and the Soonchunhyang University Research Fund.

REFERENCES

[1] Reed, Drummond, et al., "Decentralized identifiers (dids) v1. 0.", Draft Community Group Report, 2020.

[2] Sporny, Manu, et al. "Verifiable Credentials Data Model v1.1.", Draft Community Group Report, 2021.
[3] Belchior, Rafael, et al. "SSIBAC: self-sovereign identity based access control.", 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE, 2020.
[4] Halpin, Harry. "Nym credentials: privacy-preserving decentralized identity with blockchains.", 2020 Crypto Valley Conference on Blockchain Technology (CVCBT), IEEE, 2020.
[5] Mühle, Alexander, et al. "A survey on essential components of a self-sovereign identity.", Computer Science Review 30, pp. 80-86, 2018.
[6] Antonopoulos, Andreas M. "Mastering Bitcoin: unlocking digital cryptocurrencies. ", O'Reilly Media, Inc., 2014.
[7] Kaneriya, J., & Patel, H., "A comparative survey on blockchain based self sovereign identity system.", In 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), pp. 1150-1155, IEEE, 2020.
[8] Bethencourt, J., Sahai, A., & Waters, B., "Ciphertext-policy attribute-based encryption.", In 2007 IEEE symposium on security and privacy (SP'07), pp. 321-334, IEEE, 2007.
[9] A. Sahai and B. Waters., "Fuzzy Identity Based Encryption.", InAdvances in Cryptology – Eurocrypt, volume 3494 ofLNCS, pp. 457–473, Springer, 2005
[10] Schanzenbach, M. et al., "reclaimID: Secure, self-sovereign identities using name systems and attribute-based encryption.", 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), IEEE, 2018.
[11] Soltani, Reza, et al., "Data Capsule: A Self-Contained Data Model as an Access Policy Enforcement Strategy.", 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), IEEE, 2021.
[12] Xiao, Min, et al., "Privacy-Preserving and Scalable Data Access Control Based on Self-sovereign Identity Management in Large-Scale Cloud Storage.", International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Springer, Cham, 2020.

AUTHORS

TaeHoonKime received the M.S degrees in Department of Software Convergence from Soonchunhyang University (SCH), Asan, South Korea, in 2021, respectively. He is now a Ph.D. candidate in Department of Software Convergence from Soonchunhyang University (SCH), Asan, South Korea. His research interests include Information Security, Blockchain, Privacy, Decentralized Identifier, etc.

Im-Yeong Lee is corresponding author. He received the B.S. degree in electronic engineering from Hongik University, Seoul, in 1981, and the M.S. and Ph.D. degrees in information and communication engineering from Osaka University, Osaka, Japan, in 1986 and 1989, respectively. He is currently a Professor with the Department of Computer Software Engineering, Soonchunhyang University (SCH), Asan, South Korea. His research interests include information security, cryptographic protocol, and data communication.