BPPS:Blockchain-Enabled Privacy-Preserving Scheme for Demand-Response Management in Smart Grid Environments

KiSung Park, JoonYoung Lee, Ashok Kumar Das, *Senior Member, IEEE*, and Youngho Park, *Member, IEEE*

Abstract—With the ongoing revolutionary growth of the industrial Internet of Things and smart grid networks, smart grid (SG) communication has been acknowledged as a next-generation network for intelligent and efficient electric power transmission. In SG networks, smart meters (SMs) generally send requests for electricity demand to service providers (SPs), which deal with the requests for efficient energy distribution. However, SGs experience many security issues with the deployed SMs and untrusted wireless communication. To tackle these security issues, we propose a privacy-preserving authentication scheme for demand response management in SGs, called BPPS. It can resist various attacks and achieve secure mutual authentication with key agreement; moreover, it provides integrity of demand-response data using blockchain. Moreover, we perform the informal and formal (mathematical) security analysis to confirm that BPPS is secure against various attacks and achieves session key security, respectively. Furthermore, we conduct the performance and simulation analysis for SGs using NS3 and Ethereum testnet. Consequently, BPPS provides high-level security and can be applied to actual SG networks.

Index Terms—Authentication, blockchain, demand-response management, key agreement, smart grid

1 Introduction

In the last few decades, traditional grid systems have been confronted with several major issues such as efficient energy distribution, security, and environmental pollution. The traditional grid system generally adopted a top-down energy distribution model, which supplies power demands whenever electricity is required through long-distance transmission. Therefore, the energy efficiency of the traditional grid gradually decreases when a central power plant transports electrical energy to users [1].

Smart grid (SG), as a new power management system with embedded and internet and communication technologies, has attracted considerable attention in many fields because it provides reliable, efficient, and sustainable power management. SG networks try to resolve the limitations of traditional grid systems such as blackouts, inefficient energy management, and time-consuming demand response (DR). With the development of multiple SG devices, efficient and reliable energy distribution of the electrical system has become a major issue, and it compels an ideal balance between energy demand and supply in real time [2].

In 2007 and 2019, the U.S. Department of Energy put forward that the electricity demand is predicted to increase by almost 20% during the next few decades [3], and the International Energy Agency showed that global electricity demand will increase at 2.1% per year up to 2040 [4]. However, the capacity of transmission networks has grown by only 15% [3]. Considering these situations, to achieve reliable and efficient energy management, SMs have become the essential element of a SG environment because it enables the real-time monitoring and collection of a large amount of data related to SG through a wireless network. For these reasons, in 2020, International Finance Corporation expected that 269 million smart meters (SMs) will be installed in emerging markets, between 2019 and 2023 and the value of the global SM market will be $7.06 billion by 2023 [5]. Because of the large amount of data generated using SMs and the increasing communication cost, Big Data analysis, Big Data processing, and electricity demand management are still challenging assignments in SGs.

Recently, blockchain technology has been researched in several application fields such as SG, smart home, smart healthcare, banking, and access control. As a major application in SG, the blockchain could provide a key solution to resolve the challenging assignments, including energy trading, DR management, and protection of security. In particular, the requirement for decentralized energy management technology and system architecture is broadly accepted [6], [7], [8], [9], [10].

- *KiSung Park is with Blockchain Research Section, Electronics and Telecommunications Research Institute, DaeJeon 34129, South Korea. E-mail: ks.park@etri.re.kr.*
- *JoonYoung Lee is with the School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, South Korea. E-mail: harry250@knu.ac.kr.*
- *Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India. E-mail: ashok.das@iiit.ac.in.*
- *Youngho Park is with the School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea. E-mail: parkyh@knu.ac.kr.*

Manuscript received 9 Sept. 2021; revised 9 Mar. 2022; accepted 24 Mar. 2022. Date of publication 29 Mar. 2022; date of current version 14 Mar. 2023.
This work was supported by the Electronics and Telecommunications Research Institute (ETRI) Grant funded by the Korean Government under Grant 22ZR1330, through Research on Intelligent Cyber Security and Trust Infra.
(Corresponding author: Youngho Park.)
Digital Object Identifier no. 10.1109/TDSC.2022.3163138

In the context of security and privacy, there is a major SG security issue to provide reliable and efficient services. SG devices such as SMs and micro-sensors can be easily compromised by an adversary because they are physically deployed in SGs. Moreover, because SG services are provided through insecure networks, they are vulnerable to various attacks such as replay, man-in-the-middle, impersonation, and session key (SK) disclosure attacks. In this study, to guarantee user privacy and resolve these issues, we propose a privacy-preserving authentication scheme for blockchain-based DR management in SG using an elliptic curve cryptosystem (ECC)-BPPS.

1.1 Motivation

Multiple studies have proposed data management technologies in SG networks to analyze and process the data generated by various smart devices [11], [12], [13]. However, the data generated by smart devices are vulnerable to attacks because these technologies are provided through an open channel. If a smart device is compromised by a malicious adversary, the adversary can break a balance between power demand and response, manipulating the data of the smart device. Furthermore, prediction models designed to guarantee efficient DR management may fail to properly work. Hence, there is a requirement for a privacy-preserving authentication scheme in SG to provide proper DR management and alleviate various attacks. However, most existing schemes control and supervise DR using centralized approaches, which is not efficient to manage DR [14], [16], [23]. Therefore, a privacy-preserving authentication scheme that supports decentralized DR management is an essential security requirement.

1.2 Contributions

In this study, we propose a privacy-preserving authentication scheme for blockchain-based DR management in SG using ECC to address the above-mentioned issues. The main contributions are as follows.

1) The proposed scheme achieves the legitimacy of the SMs and DR control unit (DRCU). After successful mutual authentication between SMs and DRCU, the relevant and sensitive data are exchanged. Thus, it provides secure and reliable power management services to users.
2) The proposed scheme achieves the integrity of power demand and response messages using blockchain technology. It provides a DR condition checking mechanism that DRCU reads the DR data on blockchain generated by a power plant and SM.
3) The informal and formal (mathematical) security analysis under the generally accepted real-or-random (ROR) model [17] of the proposed scheme is performed to prove its security. Moreover, the simulation analysis of the proposed protocol is performed using the broadly accepted network performance analysis tool-network simulator 3 (NS3). We also construct our scheme on Ethereum testnet (KOVAN) to evaluate performance and validation of smart contract.

2 Related Work

Recently, many authentication protocols for SG networks have been proposed to ensure privacy. Odelu *et al.* [14] demonstrated that the previous scheme [18] is vulnerable to SK disclosure and impersonation attacks, and then proposed a provably secure authenticated key agreement (AKA) scheme for SG to resolve it. Then, Doh *et al.* [19] proposed an authenticated key exchange (AKE) scheme that provides secure mutual authentication between SM and controller, and Sexena *et al.* [20] presented an authentication and authorization scheme for SG networks to ensure system security against insider and outsider threats. He *et al.* [21] proposed a key management (KM) protocol using ECC, which guarantees anonymity for entities in the system and has low computational costs compared with the previous scheme [18]. Moreover, Mohammadali *et al.* [22] proposed an identity-based KM protocol for using ECC to improve the security level of SG systems. Mahmood *et al.* [15] demonstrated that Mohammadali *et al.*'s scheme is vulnerable to various attacks, and then proposed a lightweight KM protocol to overcome these security weaknesses; they also presented a pairing-based KM protocol for SG networks [23]. However, Abbasinezhad-Mood and Nikooghadam [24] and Liang *et al.* [25] showed security flaws of Mahmood *et al.*'s schemes [15] and [23]. Very recently, Chaudhry *et al.* [26] proposed cloud-assisted AKA protocol for cyber-physical systems and Kumar *et al.* [27] presented an AKE protocol for DR management. However, Chaudhry *et al.*'s scheme requires the intervention of a trusted third party for making the SK between two SMs and Kumar *et al.*'s scheme has no correct utility control initial verification [28]. To resolve the above-mentioned problems, Chaudhry *et al.* [16] proposed an AKA scheme for securing DR management in SG networks. However, their scheme does not provide integrity of DR records and is not efficient in SG networks because it adopted the traditional power grid system.

To resolve abovementioned challenges, we propose a novel privacy-preserving scheme for reliable and secure DR management using blockchain in a SG environment. The proposed BPPS achieves data integrity and transparency of DR messages using blockchain with the help of the smart contracts. Moreover, BPPS prevents various potential attacks, such as impersonation, man-in-the-middle, SK disclosure, identity disclosure, and tracing attacks. Thus, BPPS provides reliable and secure DR management services for SG.

3 Preliminaries

In this section, we discuss preliminaries, including an adversarial model and fundamental concepts of ECC, to help understand the proposed scheme. We thus present the notations and abbreviations used in the following Table 1 and 2, respectively.

3.1 Adversarial Model

We have adopted the well-known Dolev-Yao adversarial model [29] for estimating the security of our scheme under compromised situations. In this model, the entities exchange data among each other through insecure channels; thus, the

TABLE 1
Notations Used in This Paper

Notation	Description
H	A collision-resistant secure one-way cryptographic hash function
$PID_i, PCUID_j$	Pseudo identities for SM and DRCU, respectively
k_{SP}	A master key of SP
$E(a,b)$	An elliptic curve over a finite field $\mathbb{Z}_p$
G	A base point of elliptic curve
T_x	Blockchain transaction
$SK_{ij,ji}$	The session key between SM and DCRU
r_1, r_2	A random number
p	A large prime number
$\oplus$	Exclusive-OR operation
$\stackrel{?}{=}$	Verification function
$\|\|$	A concatenation operation

TABLE 2
Abbreviations Used in This Paper

Abbreviation	Description
SM	Smart meter
DRCU	Demand response control unit
SP	Service provider
AKE & AKA	Authenticated key exchange, and and authentication and key agreement, respectively
NS3	Network Simulator 3
ROR	Real-or-Random model
SG	Smart Grid
KM	Key management
ECC	Elliptic curve (EC) cryptosystem
DR	Demand response
SK	Session key
KOVAN	KOVAN Ethereum Testnet
EDD	End-to-end delay
IDE	Integrated Development Environment

capability of an adversary $\mathcal{A}$ is defined. $\mathcal{A}$ can catch, delete, and store all messages in the communication networks. $\mathcal{A}$ can modify, forge, and insert malicious contents into the transmitted messages among entities. Moreover, we assume that the end-entities such as SM and DRCU are not trusted.

3.2 Elliptic Curve Cryptography

An elliptic curve (EC) E_p over a finite field $\mathbb{Z}_p$ is defined as $E(a,b): y^2 = x^3 + ax + b$, where p are large prime, $a, b \in \mathbb{Z}_p$ $(= \{0, 1, 2, \ldots, p-1\})$ and $4a^3 + 27b^2 \pmod{p} \neq 0$. The additive group G is defined as $G = \{(x,y) : x, y \in \mathbb{Z}_p\ (x,y) \in E \cup \mathcal{O}$, where $\mathcal{O}$ is point at infinity which is the identity element of G. The scalar multiplication is defined by repeated addition operation as $\alpha G = G + G + G + G + \cdots + G(\alpha$ times), where G is an EC point and $\alpha \in \mathbb{Z}_p^* (= \{1, 2, \ldots, p-1\})$ is an integer. The detailed descriptions of EC operations refer to [30].

3.3 System Model

This section introduces the proposed system model for blockchain-based DR management in SG networks. In these networks, there are three entities-SM, DRCU, and SP-as shown Fig. 1. First, SP registers SM and DRCU, and then pre-deploys them in the SG networks to provide efficient electricity distribution services. Next, SM collects the information, including the amount of electric consumption, electricity used time, and behavior, and then writes the amount of electric consumption on the blockchain and transmits electricity used time, consumption, and behavior, to DRCU. DRCU reads the information recorded by SM on the blockchain. Then, the DRCU process uses these data, which evaluates the electric capability of SG networks and provides efficient DR and real-time pricing. However, SM is vulnerable to various potential attacks because it sends the above-mentioned sensitive data to DCRU via open networks. A malicious attacker can intercept, modify, and replay such data to violate user privacy and manipulate DR data. Therefore, a privacy-preserving authentication scheme in SG networks should be presented to achieve a secure mutual authentication and ensure the integrity of DR data.

Fig 1 also shows the AKE process of BPPS in the SG network to provide privacy. The SP issues credentials with unique identity for SM and DRCU and then pre-deploys them in SG networks. After registration, the SM and DRCU perform the secure mutual authentication and establish the SK to exchange information, including the amount of electric consumption, electricity used time, and behavior. Therefore, the entities in BPPS securely exchange data using an established SK.

4 Proposed Scheme

The proposed scheme comprises four phases-initialization, SM and DRCU registration, AKE phase, and DR transaction writing phases.

4.1 Initialization Phase

In this phase, the SP generates all system initialization parameters for subsequent phases. The detailed step of this phase is mentioned below.

Step 1. The SP chooses non-singular elliptic curve $E: y^2 = x^3 + ax + b$ over $\mathbb{Z}_p$ and base point G.
Step 2. The SP selects a collision resistant hash function H and a private key $x \in \mathbb{Z}_p$.
Step 3. The SP computes a public key $PK_{SP} = x \cdot G$ and broadcasts $\{E(a,b), PK_{SP}, H(\cdot)\}$.

4.2 Registration Phase

SP first registers and pre-deploys SM_i and DRCU_j in the SG networks to provide reliable, efficient, and sustainable power management services. Fig. 2 presents this phase and its detailed steps are as follows:

4.2.1 SM Registration Phase

The following steps need to be executed in this phase:

Step 1. The SP chooses $SMID_i$ and then computes $PID_i = H(SMID_i || k_{SP})$ and $LS_{SM_i} = H(SMID_i || k_{SP} || T_{current})$, where $SMID_i$, PID_i and $T_{current}$ are the unique identity, pseudo-identity of SM_i, and long-term secret of SM_i with current timestamp $T_{current}$, respectively.

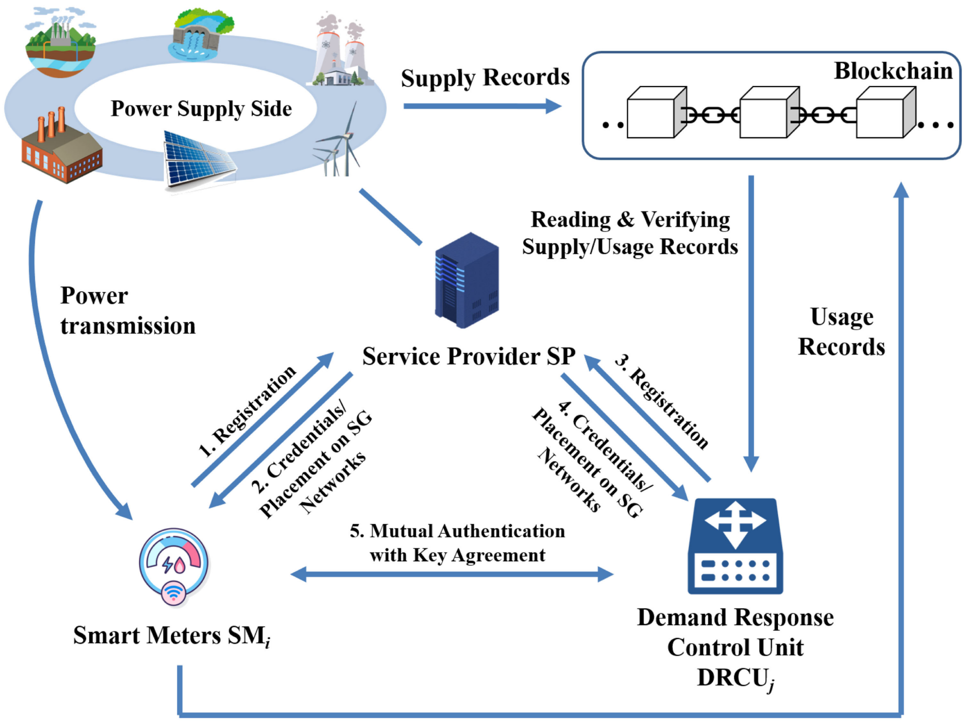

Fig. 1. System model of BPPS.

Step 2. The SP stores $\{PID_i, LS_{SM_i} H, E(a,b), G\}$ into the memory of SM$_i$.

Step 3. The SP deploys the SM$_i$ in the SG networks.

4.2.2 DRCU Registration Phase

In this phase, the following steps are required:

Step 1. The SP chooses $CUID_j$, and then computes $PCUID_j = H(CUID_j||k_{SP})$ and $LS_{DRCU_j} = H\ (CUID_i||k_{SP}||T_{current})$, where $CUID_j$, $PCUID_j$ and $T_{current}$ are a unique identity, a pseudo-identity of DRCU$_j$ and a long-term secret of DRCU$_j$ with current timestamp $T_{current}$, respectively.

Smart Meter (SM$_i$)	Service Provider (SP)
	Choose $SMID_i$, Compute $PID_i = H(SMID_i\|\|k_{SP})$, $LS_{SM_i} = H(SMID_i\|\|k_{SP}\|\|T_{current})$, Store $\{PID_i, LS_{SM_i} H, E(a,b), G\}$ into the SM$_i$ memory $\xleftarrow{SM}$ (via secure channel)
Deploy the SM$_i$ in SG	
Demand Response Control Unit (DRCU$_j$)	**Service Provider (SP)**
	Choose $CUID_j$, Compute $PCUID_j = H(CUID_j\|\|k_{SP})$, $LS_{DRCU_j} = H(CUID_j\|\|k_{SP}\|\|T_{current})$, Store $\{PCUID_j,\ H,\ E(a,b),\ G,\ PID_{i=1,\ldots,l}\}$ into the DRCU$_j$ memory $\xleftarrow{DRCU}$ (via secure channel)
Deploy the DRCU$_j$ in SG	

Fig. 2. Registration phase for BPPS.

Step 2. The SP stores $\{PCUID_j,\ H,\ E(a,b),\ G,\ PID_{i=1,\ldots,l}\}$ into the memory of SM$_i$.

Step 3. The SP deploys the DRCU$_j$ in the SG networks.

4.3 AKE Phase Between SM and DRCU

After the registration phase, SM$_i$ and DRCU$_j$ authenticate and establish the SK of each other for future secure communication. Fig. 3 describes this phase and its detailed steps are as follows:

Step 1. The SM$_i$ generates a random number r_1 and a current timestamp T_1.

1.1. Computes $R_i = r_1 \cdot G$, $RN_i = H(r_1\ ||LS_{SM_i}\ ||PID_i\ ||T_1) \oplus H(PID_i\ ||R_i\ ||T_1)$.

1.2. Sends $\{R_i, RN_i, T_1\}$ to DRCU$_j$.

Step 2. After receiving $\{R_i, RN_i, T_1\}$, the DRCU$_j$ confirms the validity of timestamp and follows the following

Smart Meter (SM$_i$)	Demand Response Control Unit (DRCU$_j$)
Generate r_1, T_1, Compute $R_i = r_1 \cdot G$, $RN_i = H(r_1\|\|LS_{SM_i}\|\|PID_i\|\|T_1) \oplus$ $H(PID_i\|\|R_i\|\|T_1)$, $\xrightarrow{\{R_i, RN_i, T_1\}}$	
	Compute $C_j = RN_i \oplus H(PID_i\|\|R_i\|\|T_1)$ Generate r_2, T_2 Compute $R_j = r_2 \cdot G$, $S_j = r_2 R_i = (r_1 r_2) \cdot G$, $SK_{ji} = H(S_j\|\|C_j\|\|H(PCUID_j\|\|r_2\|\|LS_{DRCU_j}\|\|T_2)$, $V_j = H(PCUID_j\|\|r_2\|\|LS_{DRCU_j}\|\|T_2) \oplus H(PID_i\|\|$ $R_i\|\|R_j\|\|T_2)$, $K_j = H(SK_{ji}\|\|PID_i\|\|T_1\|\|T_2)$ $\xleftarrow{\{R_j, V_j, K_j, T_2\}}$
$C_i = V_j \oplus H(PID_i\|\|R_i\|\|R_j\|\|T_2)$ $= H(PCUID_j\|\|r_2\|\|LS_{DRCU_j}\|\|T_2)$ $S_i = r_1 R_j = (r_1 r_2) \cdot G$ $SK_{ij} = H(S_i\|\|H(r_1\|\|LS_{SM_i}\|\|PID_i\|\|T_1)\|\|C_i\|\|T_2)$ $K_i = H(SK_{ij}\|\|PID_i\|\|T_1\|\|T_2)$ Check whether $K_i \stackrel{?}{=} K_j$, Generate T_3, Compute $V_i = H(SK_{ij}\|\|PID_i\|\|K_i\|\|T_2\|\|T_3)$ $\xrightarrow{\{V_i, T_3\}}$	
	Compute $V_i^* = H(SK_{ji}\|\|PID_i\|\|K_j\|\|T_2\|\|T_3)$ Checks whether $V_i^* \stackrel{?}{=} V_i$

Fig. 3. AKE phase for BPPS.

steps:

2.1. Computes $C_j = RN_i \oplus H(PID_i||R_i||T_1)$.

2.2. Generates a random number r_2 and a current timestamp T_2.

2.3. Computes $R_j = r_2 \cdot G$.

2.4. Calculates $S_j = r_2 R_i = (r_1 r_2) \cdot G$.

2.5. Calculates $SK_{ji} = H(S_j|| C_j|| H(PCUID_j ||r_2 ||LS_{DRCU_j} ||T_2)$.

2.6. Computes $V_j = H(PCUID_j ||r_2 ||LS_{DRCU_j} ||T_2) \oplus H(PID_i ||R_i ||R_j ||T_2)$.

2.7. Calculates $K_j = H(SK_{ji}||PID_i||T_1||T_2)$.

2.8. Sends $\{R_j, V_j, K_j, T_2\}$ to SM$_i$.

Step 3. On the receiving $\{R_j, V_j, K_j, T_2\}$, the SM$_i$ verifies the validity of timestamp and computes the following (Steps 3.1 to 3.4):

3.1. $C_i = V_j \oplus H(PID_i ||R_i ||R_j ||T_2) = H(PCUID_j ||r_2 ||LS_{DRCU_j} ||T_2)$,

3.2. $S_i = r_1 R_j = (r_1 r_2) \cdot G$,

3.3. $SK_{ij} = H(S_i|| H(r_1 ||LS_{SM_i} ||PID_i ||T_1) ||C_i ||T_2)$,

3.4. $K_i = H(SK_{ij} ||PID_i ||T_1 ||T_2)$.

3.5. Next, checks whether $K_i \stackrel{?}{=} K_j$, If it is correct, generates a current timestamp T_3.

3.6. Computes $V_i = H(SK_{ij} ||PID_i ||K_i ||T_2 ||T_3)$.

3.7. Sends $\{V_i, T_3\}$ to DRCU$_j$.

Step 4. After receiving $\{V_i, T_3\}$, the DRCU$_j$ verifies the validity of timestamp and computes $V_i^* = H(SK_{ji} ||PID_i||K j||T_2||T_3)$. Afterward, DRCU$_j$ checks if $V_i^* \stackrel{?}{=} V_i$. If it is correct, DRCU$_j$ and SM$_i$ successfully authenticate and establish the SK of each other.

4.4 DR Transaction Writing Phase

First, the SM $_i$ collects the amount of electric consumption, electricity used time, and inhabitant's behavior. Then, SM$_i$ encrypts these data data$_{enc}$ using SK SK_{ij} as established in the AKE phase and sends it to DRCU$_j$. SM$_i$ computes the transaction $\mathrm{T}_i = H($ above-mentioned data$, PID, T_1)$ and starts the block creation process. If the transaction is committed, the block is recorded into the blockchain. DRCU$_j$ then decrypts the data$_enc$ and computes the hash value. Finally, DRCU$_j$ reads the data in the blockchain and verifies if the computed hash value is equal to the blockchain data. If they are equal, DRCU$_j$ process these data to provide efficient and reliable DR management. The Algorithm 1 shows the detailed steps of this phase and Table 3 shows the detailed block structure used in SG Network.

Algorithm 1. Smart Contract

Require: Sender.address, Data
1: **if** Sender.address $\stackrel{?}{=}$ Address of Smart Contract Owner **then**
2: Store Data in Smart Contract
3: **else**
4: Record the sender.address and terminate
5: **end if**

5 Security Analysis

In this section, we demonstrate that BPPS is secure against known attacks, and it provides SK security using formal (mathematical) and informal analysis.

TABLE 3
Block Structure Used in SG Networks

Block Header	
Software/Protocol Version	
Hash Value of Previous Block (Parent Hash)	
Root Value of Merkle Patricia Tree	
Timestamp	
Difficulty (Level of Mining Difficulty)	
Nonce	
Block Body	
Transaction No. 1	Tx_1
Transaction No. 2	Tx_2
⋮	⋮
Transaction No. N	Tx_N
Hash Value of Current Block(State_root)	H_{CB}
Value of ECDSA Digital Signature	$Sign_{ECDSA}$

5.1 Formal Security Analysis

The ROR model-based formal security [17] is one of the powerful security proof for cryptographic protocols to confirm if it achieves the SK security or not, which is applied in recent authentication protocols [31], [32], [33]. First, we present the basic description of this model and then prove the SK security afterward.

The executing participants involved in the protocol are 1) SM, DRCU, and SP. The following ingredients are used in the ROR model.

- *Participants*: Assume that Π^t_{SP}, Π^t_{SM}, and Π^t_{DRCU} present the t^{th} instance of SM, DRCU, and SP, respectively, and then Π^t_{SP}, Π^t_{SM}, and Π^t_{DRCU} are known as *oracles*.
- *Accepted state*: Instance Π^t reaches to an accepted state after receiving the last exchanged messages. When we concatenate all exchanged messages of instance Π^t_{SP} in order, it is session ID sid of Π^t_{SP} for the current session.
- *Partnering*: The instance $\Pi^{t_1}_{SP}$ and $\Pi^{t_2}_{SP}$ are known as partners if the following three statement are simultaneously satisfied: i) $\Pi^{t_1}_{SP}$ and $\Pi^{t_2}_{SP}$ are in accepted state; ii) $\Pi^{t_1}_{SP}$ and $\Pi^{t_2}_{SP}$ mutually authenticate each other in the same sid; and iii) $\Pi^{t_1}_{SP}$ and $\Pi^{t_2}_{SP}$ are partners to each other.
- *Freshness*: When the SK between SM$_i$ and DRCU$_j$ is not revealed to adversary $\mathcal{A}$ using the $Reveal(\Pi^t)$ query, then Π^t_{SP}, Π^t_{SM}, or Π^t_{DRCU} is fresh.
- *Adversary*: Under the ROR model, a malicious adversary $\mathcal{A}$ can fully control the communication network. $\mathcal{A}$ can intercept, modify, inject, or delete the messages in the current session. Moreover, $\mathcal{A}$ may execute the oracle queries, and the description of oracle queries is shown in Table 4.
- *Semantic Security*: The semantic security of the SK verifies whether $\mathcal{A}$ can distinguish an instance's real SK from a random number using $Execute$, $Reveal$, $Send$, and $Test$ queries. After finishing the game, $\mathcal{A}$ guesses the bit c. If the c is equal to c', $\mathcal{A}$ wins the game, which implies $\mathcal{A}$ is useful in breaking the semantic SK security of BPPS. We define the event $Succ$ which win the game and its advantage is

TABLE 4
Queries and Descriptions

Query	Descriptions
$Execute(\Pi_{SM}^{t_1}, \Pi_{DRCU}^{t_2}$	$\mathcal{A}$ can intercept the exchanged messages between the communicating entities SM_i and $DRCU_j$ through public channel, which is designated as an "eavesdropping attack."
$Reveal(\Pi^t)$	The current SK SK_ij/SK_ji between $\mathcal{P}^t$ and $\mathcal{A}$ is compromised to $\mathcal{A}$.
$Send(\Pi^t, Msg)$	$\mathcal{A}$ can send a message to $\mathcal{P}^t$, and in cooperation, it can receive the response from $\mathcal{P}^t$, which is designated as an "active attack".
$Test(\Pi^t)$	An unbiased coin c is tossed before the game. Under this outcome, the following results are obtained. $\mathcal{A}$ executes this query when SK_ij/SK_ji between $\mathcal{P}^t$ and $\mathcal{A}$ is fresh. If $c = 1$ or $c = 0$, $\mathcal{P}^t$ returns the correct SK or a random number. Otherwise, this query returns a null value $(\perp)$.

$Adv_{\mathcal{P}}^{AKE} = |2.Pr[W] - 1|$. Therefore, $\mathcal{P}$ is secure $Adv_{\mathcal{P}}^{AKE} \leq \tau$ when τ is negligible $\tau > 0$.

- *Random Oracle*: All participants and the malicious adversary in BPPS can access a collision-resistant one-way hash function H, which is a random oracle, say $Hash$ oracle.

First, we define the elliptic curve decisional Diffie-Hellman problem (ECDDHP) to confirm Theorem 1 and that BPPS achieves SK security.

Definition 1. *For $x, y, z \in E_p$, given three elliptic curve points xG, yG, and $zG \in G$, decide whether $zG = xyG$ or a uniform value.*

Theorem 1. *Assuming that $\mathcal{A}$ runs against BPPS scheme $\mathcal{P}$ in the polynomial time t in the ROR model, then the winning advantage of $\mathcal{A}$ that breaks the semantic security of SK is*

$$Adv_{\mathcal{P}}^{AKE} \leq \frac{q_h^2}{|Hash|} + 2Adv^{ECDDHP}(t)$$

where q_h is the number of $Hash$ queries; $Hash$ is range space of a collision-resistant one-way hash function H; and $Adv^{ECDDHP}(t)$ is the winning advantage of $\mathcal{A}$.

Proof. The proof comprises four games $G_i(i = 0, 1, 2, 3)$; the detailed proofs are given below.

- *Game G_0*: This game is a real attack executed by $\mathcal{A}$ against BPPS in this model. Since the bit c is chosen randomly before beginning of the game G_0, we have

$$Adv_{\mathcal{P}}^{AKE} = |2.Pr[Succ_0] - 1| \tag{1}$$

- *Game G_1*: In this game, $\mathcal{A}$ performs an eavesdropping attack on all transmitted messages $(\{R_i, RN_i, T_1\}, \{R_j, V_j, K_j, T_2\}, \{V_i, T_3\})$ between the participants using $Execute(\Pi_{SM}^{t_1}, \Pi_{DRCU}^{t_2})$ query. Then, $\mathcal{A}$ executes the $Test(\Pi^t)$ and obtain its output, which is used to decide if it is an actual SK or a random bit. In BPPS, the SK is established between SM_i and $DRCU_j$ and is given by $SK_{ij} = H(S_j||C_j||H(CUID_j||r_2||T_2))$. If $\mathcal{A}$ wants to derive a real SK, it must obtain short- and long-lived secrets, $\{r_1, r_2\}$ and $\{PID_i, CUID_j\}$, respectively. Therefore, the advantage of winning this game G_1 does not increase by this attack. Thus, it follows that

$$Pr[Succ_1] = Pr[Succ_2] \tag{2}$$

- *Game G_2*: In this game, $\mathcal{A}$ performs the active attack using $Send(\Pi^t, Msg)$ and $Hash$ query to impersonate a legal participants SM and DRCU. $\mathcal{A}$ can make several $Hash$ query for creating a hash collision condition. However, all transmitted messages $(\{R_i, RN_i, T_1\}, \{R_j, V_j, K_j, T_2\}, \{V_i, T_3\})$ include random number, long-lived secret, and timestamp. Moreover, $\mathcal{A}$ cannot report a hash collision in polynomial time by executing these queries. Therefore, the following result is obtained using the birthday paradox.

$$|Pr[Succ_1] - Pr[Succ_2]| \leq \frac{q_h^2}{2|Hash|} \tag{3}$$

- *Game G_3*: This is the final game executed by $\mathcal{A}$ and it is an additional active attack. According to G_1, $\mathcal{A}$ must obtain short- and long-lived secrets, $\{r_1, r_2\}$ and $\{PID_i, CUID_j\}$, respectively, to correctly guess SK. However, after eavesdropping R_i, R_j, $\mathcal{A}$ must break the ECDDHP problem to distinguish between $r_1 r_2 \cdot G$ and a nonce. Therefore, $\mathcal{A}$ does not yield $SK_{ij} = H(S_j||C_j||H\ (CUID_j|| r_2||T_2))$, and it is given that

$$|Pr[Succ_2] - Pr[Succ_3]| \leq Adv_{\mathcal{P}}^{ECDDHP}(t) \tag{4}$$

As all games (G_0, G_1, G_2, G_3) are finished, $\mathcal{A}$ tries to guess the bit c correctly. Then, it follows that:

$$Pr[Succ_3] = \frac{1}{2} \tag{5}$$

From the (1) and (2), we can obtain following result.

$$\begin{aligned}\frac{1}{2}.Adv_{\mathcal{P}}^{AKE} =& |Pr[Succ_0] - \frac{1}{2}| \\ =& |Pr[Succ_1] - \frac{1}{2}|\end{aligned} \tag{6}$$

We can then obtain the following result using the triangular inequality and (3), (4) and (5) lead to the following result:

$$\begin{aligned}|Pr[Succ_1] - \frac{1}{2}| =& |Pr[Succ_1] - Pr[Succ_3]| \\ \leq& |Pr[Succ_1] - Pr[Succ_2]| \\ &+ |Pr[Succ_2] - Pr[Succ_3]| \\ \leq& \frac{q_h^2}{2|Hash|} + Adv_{\mathcal{P}}^{ECDDHP}(t)\end{aligned} \tag{7}$$

Finally, we can obtain the required result by multiplying both sides of (7) by a factor of 2:

$$Adv_{\mathcal{P}}^{AKE} \leq \frac{q_h^2}{|Hash|} + 2Adv^{ECDDHP}(t)$$

□

TABLE 5
Computation Cost

Scheme	Total computation cost
Mahmood *et al.* [23]	$10T_{smp} + 6T_{ap} + 6T_h \approx 22.447$ ms
Chaudhry *et al.* [26]	$7T_{smp} + 18T_h$ $+T_{se} + T_{sd} + T_{fz} \approx 17.859$ ms
Chaudhry *et al.* [16]	$9T_{smp} + 2T_{ap} + 8T_h \approx 20.110$ ms
BPPS	$4T_{smp} + 11T_h \approx 8.9293$ ms

TABLE 6
Communication Cost

Scheme	Total communication cost (in bits)
Mahmood *et al.* [23]	2304
Chaudhry *et al.* [26]	2048
Chaudhry *et al.* [16]	1504
BPPS	1376

5.2 Informal Security Analysis

In this section, we analyze the security of BPPS to demonstrate that BPPS is secure against the following attacks.

5.2.1 SM Impersonation Attack

We assume that $\mathcal{A}$ wants to impersonate a legitimate entity $\mathcal{A}$ by generating and sending valid authentication and key agreement messages to DRCU$_j$. $\mathcal{A}$ must successfully compute $\{R_i, RN_i, T_1\}$, and $\{V_i, T_3\}$. However, $\mathcal{A}$ cannot compute RN_i without knowing PID_i and LS_{SM_i}. Thus, BPPS scheme is secure against SM impersonation attack because $\mathcal{A}$ cannot generate these valid messages.

5.2.2 DRCU Impersonation Attack

If $\mathcal{A}$ want to generate valid response messages to impersonate a legal DRCU, $\mathcal{A}$ generates $R_j^A = r_2 \cdot G$, T_2^A, and $S_j = r_2 R_i$, and then can generate $\{R_j, V_j, K_j, T_2\}$. However, $\mathcal{A}$ cannot generate valid response messages because it should obtain $PCUID_i$ and LS_{DRCU_j} for the computation. Hence, BPPS resists DRCU impersonation attack.

5.2.3 Man-in-The-Middle Attack

When $\mathcal{A}$ attempts to perform man-in-the-middle attack, $\mathcal{A}$ first intercepts the authentication request messages $\{R_i, RN_i, T_1\}$. Then, $\mathcal{A}$ generates a random number r_a, a current timestamp T_2^A, and $R_a = r_a \cdot G$ to compute $C_j = RN_i \oplus H(PID_i||R_i||T_1)$. However, $\mathcal{A}$ cannot compute C_j without obtaining PID_i and LS_{SM_i}. Therefore, $\mathcal{A}$ cannot manipulate it as valid authentication request messages. In a similar way, $\mathcal{A}$ cannot manipulate $\{R_j, V_j, K_j, T_2\}$, and $\{V_i, T_3\}$ without knowing the secret parameters ($PCUID_i$ and LS_{DRCU_j}). Therefore, BPPS is secure against man-in-the-middle attack.

5.2.4 SK Disclosure Attack

In BPPS, the SM$_i$ and DRCU$_j$ authenticate and establish the SK of each other. It is calculated as follows $SK_{ij} = H(S_i||H(r_1||LS_{SM_i}||PID_i||T_1)||C_i||T_2)$, including the short- and long-lived secrets $\{r_1, r_2\}$ and $\{LS_{SM_i}, LS_{DRCU_j}, PID_i, PCUID_i\}$, respectively. We assume that the short-lived secrets are compromised to $\mathcal{A}$, and $\mathcal{A}$ want to compute the valid SK. It is difficult for $\mathcal{A}$ to calculate SK_{ij} because $\mathcal{A}$ does not know the long-term secrets. Moreover, we assume that the long-live secrets are compromised to $\mathcal{A}$, and $\mathcal{A}$ attempts to calculate SK_{ij}. In a similar way, $\mathcal{A}$ cannot compute SK_{ij} without knowing the short-lived secrets. Moreover, the long-lived secrets involve the real identity $\{SMID_i, CUID_i\}$ and the server's master secret k_{SP}, which are only known to SP. Therefore, BPPS protects the SK disclosure attack.

5.2.5 Identity Disclosure and Trace Attacks

If $\mathcal{A}$ intercepts all transmitted messages ($\{R_i, RN_i, T_1\}$, $\{R_j, V_j, K_j, T_2\}$, $\{V_i, T_3\}$) in the networks, $\mathcal{A}$ tries to trace the entities and disclose their real identities. However, during the AKE phase, all transmitted messages are changed for every session because they are masked with the current timestamp ($\{T_1, T_2, T_3\}$) and short-lived secrets. Therefore, BPPS resists identity disclosure and trace attacks.

5.2.6 Integrity of DR Records

In the DR transaction writing phase, the SMs encrypts the collected data using the shared SK SK_{ij} and sends it to DRCU. The collected data are hashed by a collision-resist one-way hash function and SMS writes the data into the blockchain. Then, DRCU verifies the validity of the data received by SMs compared with the value on the blockchain. It has the important advantage that provides data transparency and provenance. If $\mathcal{A}$ wants to violate the data integrity of our scheme, they must change the data into blockchain. Therefore, BPPS achieves the integrity of data.

6 Comparative Analysis

This section presents the performance of BPPS and compares it with previous schemes [16], [23], [26].

We consider the AKE phase for BPPS and other schemes to perform the comparative analysis. Tables 5 and 6 present computation and communication overheads, respectively.

We utilize message sizes transmitted in AKE phase to analyze communication overheads. We define a random number/nonce, identity, and hash function are 160 bits [34], elliptic curve point is 320 bits, and timestamp is 32 bits. In BPPS, the exchanged messages $\{R_i, RN_i, T_1\}$, $\{R_j, V_j, K_j, T_2\}$ and $\{V_i, T_3\}$ require $(320 + 160 + 32) = 512$ bits, $(320 + 160 + 160 + 32) = 672$ bits, and $(160 + 32) = 192$ bits, respectively. Therefore, the total cost requires for BPPS $(512 + 672 + 192)$ $= 1376$ bits. As a result, BPPS demands 1376 bits communication cost. On the other hand, [23], [26], [16] demand 2304, 2048 and 1504, respectively.

We define the notations for computational costs comparison based on the experimental results presented in [26], [35]. $T_h(\approx 0.0023$ ms) denotes the time required for a "collision resistant one-way hash function," $T_{se/sd}(\approx 0.0046$ ms) denotes the time required for a symmetric encryption/decryption, $T_{smp}(\approx 2.226$ ms) denotes the time required for a scalar multiplication, $T_{ap}(\approx 0.0288$ ms) denotes the time for a point addition, $T_{bp}(\approx 5.811$ ms) denotes the time

TABLE 7
The Experimental Environments for NS3

Parameter	Description
Operating System	Ubuntu 16.04 LTS
RAM	2 GB
CPU	Intel Core i5-9500 3.00 GHz
Tool	NS3 3.29
Wireless protocol	802.11
Number of DRCU point (for all cases)	1
Number of SMs	10 (case-1) 20 (case-2) 30 (case-3)
Simulation time	1800 seconds
Network simulation area	Radius 150 meters
Routing protocol	Optimized link state routing

required for a bilinear pairing, and $T_{fz}(\approx 2.226$ ms) denotes the time required for fuzzy extractor operation. BPPS needs the computation cost $4T_{smp}(\approx 8.904$ ms) + $11T_h(\approx 0.0253$ ms) = 8.9293 ms, On the other hand, the other schemes, such as [23], [26] and [16] require 22.447 ms, 17.859 ms and 20.110 ms, respectively. The computation cost of BPPS has 151.39%, 100%, and 125.21% lower than related schemes. Moreover, the related scheme [16], [23], [26] has the critical issues. The [23] is insecure against a session key disclosure attack. The [26] has inefficient AKE procedure because their scheme requires the intervention of a trusted third party for making the session key. The [16] does not provide a integrity of DR data and has adopted the traditional power grid environments. Therefore, BPPS has better security and performance than the previous schemes.

7 Practical Simulation

This section performs the practical simulation using NS3 simulator to evaluate the network performance in various scenarios, which is well-known for network simulation tool. BPPS is also practically simulated on a Ethereum network to estimate the cost of smart contract.

7.1 NS3 Simulation

We consider three scenarios in the NS3 simulation and have taken one DRCU. The number of SM were taken as 10 (scenario 1), 20 (scenario 2) and 30 (scenario 3). We also perform the NS3 simulation using optimized link state routing protocols. We simulate this experiment on a local PC running Ubuntu 16.04 LTS on an Intel Core i5-9500 3.00 GHz with 2 GB RAM. The experimental environments are briefly described in Table 7.

7.2 End-to-End Delay

We measure the End-to-End Delay (EDD) which is the average time that the messages reached the destination entity from the source entity. EDD is defined as follows.

$$\sum_{i=1}^{\nu_p}(T_{Recv_i} - T_{Send_i})/\nu_p,$$

where ν_p, T_{Recv_i} and T_{Send_i} are the total number of messages, the receiving and the sending packet time of i, respectively.

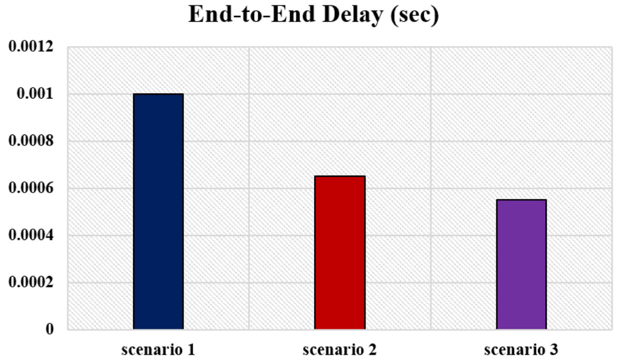

Fig. 4. End-to-end delay of BPPS.

Fig. 4 presents the EDD in various scenarios. It is viewed that when the number of SM is increased, the EDD is decreased because the stationary entities (SM and DRCU) are deployed in SG network and exchange the data with the closest entity. The EDDs are 0.1, 0.065 and 0.055 seconds for scenario 1$\sim$3 respectively. This result is worthy of notice that the EDD values decreases with the growing number of SMs because the decrement of distant among entities.

7.3 Throughput

Throughput is another parameter to estimate network performance, which is calculated as the number of packets (bit) transmitted per unit of time. Throughput is defined as follows.

$$\frac{N_{recv} \times |Size_{packet}|}{T_{total}},$$

where T_{total}, $|Size_{packet}|$ and N_{recv} are the total time (sec), total number of received packet and size of packet, respectively. The throughput values of BPPS also are 765.431, 437.836 and 516.637 bps for scenario 1$\sim$3, receptively. This result is shown in Fig. 5 and presents that the throughput values are decreased with the increment of SM because the deployed nodes exchange the messages using optimum course selection.

7.4 Blockchain Simulation

This section simulates the smart contract of our scheme on Remix Integrated Development Environment (IDE) to examine the feasibility and efficiency. Remix IDE is open-source web and desktop application for Ethereum Testnet

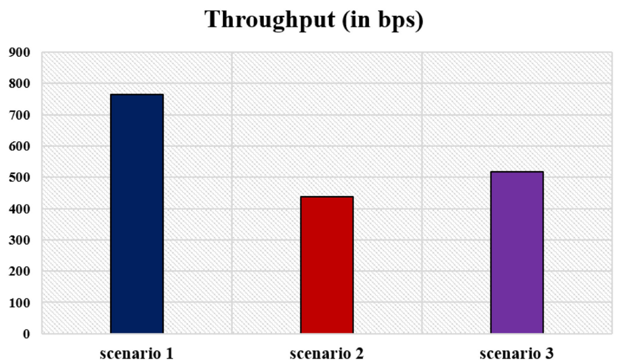

Fig. 5. Throughput of BPPS.

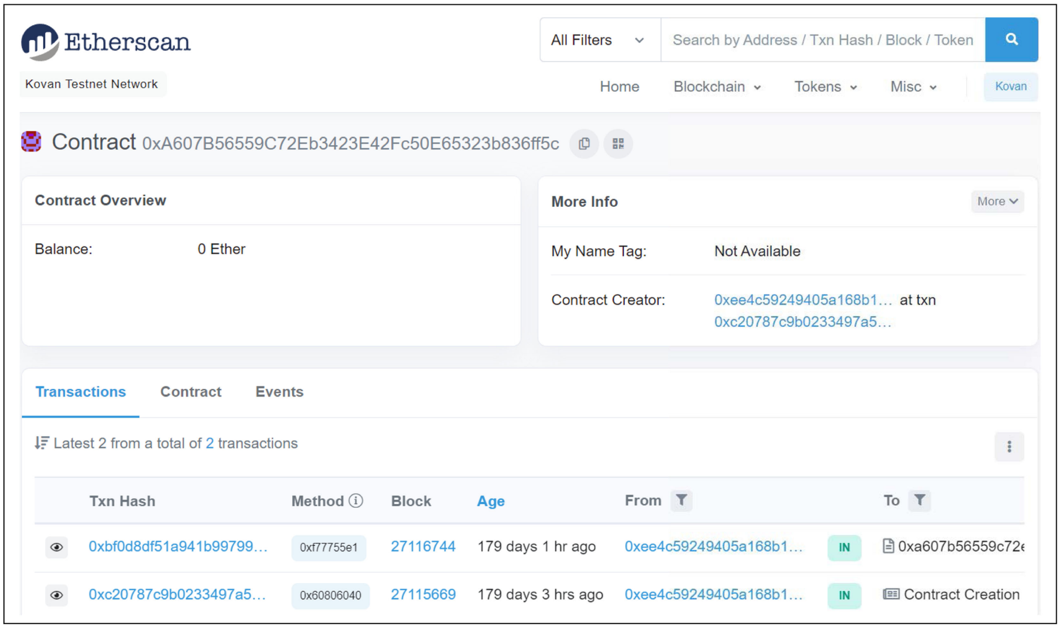

Fig. 6. Deployment result of smart contract (KOVAN).

environments (KOVAN), which is supports development tools for deploying smart contracts [36]. We used the Remix Solidity Compiler (0.8.7+commit.e28d00a7) using Algorithm 1 and the detailed results of this implementation are as follows.

1) We firstly generate the account (0xee4c59249405a168b1c6ec72587518b53ed5f0ed) for SM for our implementation. According to Section 4.4, Algorithm 1 is deployed in blockchain using the smart contract with Remix IDE. The smart contract address is 0xa607b56559c72eb3423e42fc50e65323b836ff5c and its deployment results are shown in Fig. 6 (KOVAN) and Fig. 7 (Remix IDE).
2) We simulates that SM records the amount of electric consumption (19921 kWh), and then DRCU can retrieve the data from the blockchain using 'eth_call' function. The results of recording and retrieve data are shown in Fig. 8 and Fig. 9, respectively.

According to this simulation, we can evaluate the cost of transaction fee for deployment and writing operation and its results is shown in Table 8. The transactions executed on Ethereum testnet incur a transaction cost (Gas) to process a specific operation. According to the exchange market (UTC/GMT -04:00, 12:20), ETH price (3,484 USD) is very much higher than usual price, which raises average price of Gas because Gas price can fluctuate depending on the date and time. Therefore, in this analysis, we have utilize the general average price of gas (20 Gwei). Table 8 shows that the deployment cost of smart contract and data writing cost are 6.30 (USD) and 3.03 (USD), respectively. Thus, since the smart contract deployment is executed only once, one SM spends about 3.03 USD for writing data in blockchain and it is considered to use practical environments.

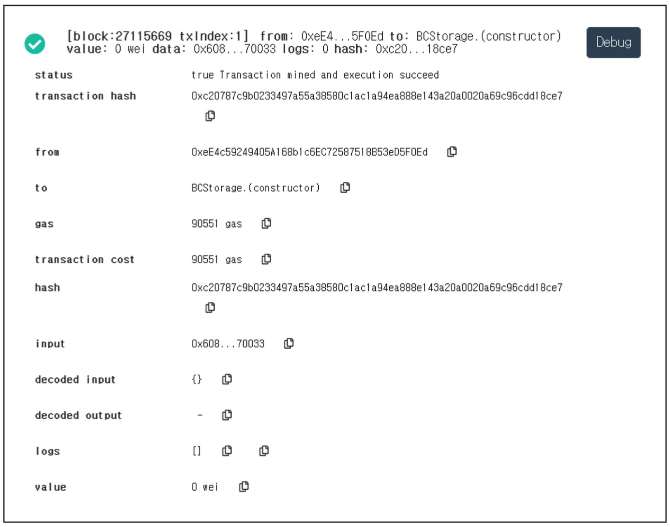

Fig. 7. Deployment result of smart contract (Remix IDE).

Fig. 8. Result of recording data.

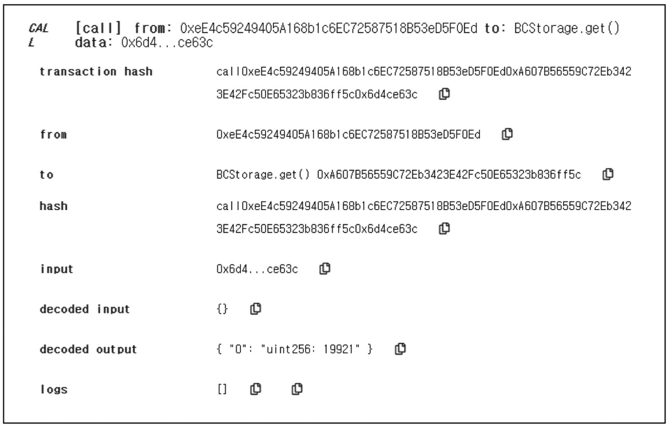

Fig. 9. Result of reading data.

TABLE 8
Practical Transaction Cost (Fee)

Function	Gas used	Ether Cost	USD
Deployment	90551	0.001448816 ETH	6.30 USD
Writing	43528	0.0000696448 ETH	3.03 USD

8 Conclusion and Future Work

This study presented a new privacy-preserving scheme for blockchain-based demand-response management in SG networks-BPPS. In BPPS, after authenticating and establishing the SK between SM and DCRU, SM securely transmits the collected data to DRCU using the shared SK, and then SM write this value into a blockchain to ensure privacy and integrity. Moreover, DRCU can provide efficient and reliable DR management using the data recorded on the blockchain. We demonstrated that BPPS resists various attacks, such as SM impersonation, DRCU impersonation, man-in-the-middle, SK disclosure, identity disclosure, and trace attacks. Furthermore, it achieves secure mutual authentication, anonymity, and integrity of DR data. The formal security analysis using the ROR model mathematically confirmed that BPPS guarantees SK security. Moreover, we performed a comparative analysis with contemporary schemes to confirm that the cost of BPPS is comparable with those of the others and has a high-security level and enhanced functionalities. We also perform the practical simulation analysis using NS3 and Ethereum testnet to evaluate performances for network and smart contract. Therefore, BPPS can be applied to practical SG networks.

In future work, we have planned to deploy the SMs and DRCUs in a practical SG network, and then apply our scheme using main Ethereum network to evaluate and enhance reliability and efficiency.

References

[1] M. A. Rahman, M. H. Manshaei, E. Al-Shaer, and M. Shehab, "Secure and private data aggregation for energy consumption scheduling in smart grids," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 2, pp. 221–234, Jun. 2017.

[2] A. Mahmood, N. Javaid, and S. Razzaq, "A review of wireless communications for smart grid," *Renewable Sustain. Energy Rev.*, vol. 41, pp. 248–260, Jan. 2015.

[3] "The SMART GRID: An introduction - exploring the imperative of revitalizing america's electric infrastructure," U.S. Department of Energy, 2009. [Online]. Available: https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf

[4] World Energy Outlook 2019, "Part of world energy outlook," 2019. [Online]. Available: https://www.iea.org/reports/world-energy-outlook-2019/electricity

[5] "Artificial intelligence and the future for smart homes, international finance corporation," 2020. [Online]. Available: https://openknowledge.worldbank.org/bitstream/handle/10986/33615/Artificial-Intelligence-and-the-Future-for-Smart-Homes.pdf?sequence=1

[6] "EWEA:Wind in power 2015 european statistics," Accessed: Apr. 20, 2021. [Online]. Available: https://windeurope.org/wp-content/uploads/files/about-wind/statistics/EWEA-Annual-Statistics-2015.pdf

[7] J. M. Guerrero, M. Chandorkar, and T. L. Lee, "Advanced control architectures for intelligent microgrids-part I:decentralized and hierarchical control," *IEEE Trans. Ind. Electron.*, vol. 60, no. 4, pp. 1254–1262, Apr. 2013.

[8] N. Hatziargyriou, *Microgrids: Architectures and Control*. Hoboken, NJ, USA:Wiley, 2014.

[9] C. S. Karavas, G. Kyriakarakos, K. G. Arvanitis, and G. Papadakis, "A multi-agent decentralized energy management system based on distributed intelligence for the design and control of autonomous polygeneration microgrids," *Energy Convers. Manag.*, vol. 103, pp. 166–177, Oct. 2015.

[10] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 1, pp. 162–182, Jan. 2018.

[11] X. Wang, L. T. Yang, J. Feng, X. Chen, and M. J. Deen, "A tensor-based big service framework for enhanced living environments," *IEEE Cloud Comput.*, vol. 3, no. 6, pp. 36–43, Dec. 2016.

[12] L. Kuang, F. Hao, L. T. Yang, M. Lin, C. Luo, and G. Min, "A tensor-based approach for Big Data representation and dimensionality reduction," *IEEE Trans. Emerg. Top. Comput.*, vol. 2, no. 3, pp. 280–291, Sep. 2014.

[13] L. T. Yang, L. Kuang, J. Chen, F. Hao, and C. Luo, "A holistic approach to distributed dimensionality reduction of Big Data," *IEEE Trans. Cloud Comput.*, vol. 6, no. 2, pp. 506–518, Jun. 2018.

[14] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1900–1910, May 2018.

[15] K. Mahmood, J. Arshad, S. A. Chaudhry, and S. Kumari, "An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure," *Int. J. Commun. Syst.*, vol. 32, no. 16, Aug. 2019, Art. no. e4137.

[16] S. A. Chaudhry, H. Alhakami, A. Baz, and F. Al-Turjman, "Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure," *IEEE Access*, vol. 8, pp. 101 235–101 243, May 2020.

[17] M. Abdalla, P. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. 8th Int. Workshop Theory Pract. Public Key Cryptogr.*, 2005, pp. 65–84.

[18] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 906–914, Mar. 2016.

[19] I. Doh, J. Lim, and K. Chae, "Secure authentication for structured smart grid system," in *Proc. 9th Int. Conf. Innov. Mobile Internet Serv. Ubiquitous Comput.*, Fukuoka, Japan, 2015, pp. 200–204.

[20] N. Saxena, B. J. Choi, and R. Lu, "Authentication and authorization scheme for various user roles and devices in smart grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 5, pp. 907–921, May 2016.

[21] D. He, L. Wang, H. Wang, and M. K. Khan, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography," *IET Commun.*, vol. 10, no. 14, pp. 1795–1802, Sep. 2016.

[22] A. Mohammadali, M. S. Haghighi, M. H. Tadayon, and A. Mohammadi-Nodooshan, "A novel identity-based key establishment method for advanced metering infrastructure in smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2834–2842, Jul. 2018.

[23] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Gener. Comput. Syst.*, vol. 81, pp. 557–565, Apr. 2018.

[24] K. Mahmood *et al.*, "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Gener. Comput. Syst.*, vol. 88, pp. 491–500, Nov. 2018.
[25] D. Abbasinezhad-Mood and M. Nikooghadam, "Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications," *Future Gener. Comput. Syst.*, vol. 84, pp. 47–57, Jul. 2018.
[26] S. A. Chaudhry, T. Shon, F. AL-Turjamn, and M. H. Alsharif, "Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems," *Comput. Commun.*, vol. 153, no. 1, pp. 527–537, Mar. 2020.
[27] N. Kumar, G. S. Aujla, A. K. Das, and M. Conti, "ECCAuth: A secure authentication protocol for demand response management in a smart grid system," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6572–6582, Dec. 2019.
[28] S. A. Chaudhry, K. Yahya, and F. Al-Turjman, "On the correctness of an authentication scheme for managing demand response in smart grid," in *Smart-Grid in IoT-Enabled Spaces-The Road to Intelligence in Power*. New York, NY, USA: Taylor and Francis, 2020.
[29] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inform. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.
[30] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. New York, NY, USA: Springer, 2006.
[31] S. Yu, J. Lee, K. Park, A. K. Das, and Y. Park, "IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment," *IEEE Access*, vol. 8, pp. 167 875–167 886, Sep. 2020.
[32] K. Park, Y. Park, A. K. Das, S. Yu, J. Lee, and Y. Park, "A dynamic privacy-preserving key management protocol for V2G in social Internet of Things," *IEEE Access*, vol. 7, pp. 76812–76832, Jun. 2019.
[33] K. Park *et al.*, "LAKS-NVT: Provably secure and lightweight authentication and key agreement scheme without verification table in medical Internet of Things," *IEEE Access*, vol. 8, pp. 119 387–119 404, Jun. 2020.
[34] P. Chandrakar and H. Om, "A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC," *Comput. Commun.*, vol. 110, pp. 26–34, Sep. 2017.
[35] H. H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes," *IEEE Commun. Surv. Tutor.*, vol. 16, no. 2, pp. 1005–1023, Oct. 2014.
[36] "Welcome to remix's documentation!," Accessed: Aug. 08, 2021. [Online]. Available: https://remix-ide.readthedocs.io/en/latest/

KiSung Park received the BS and MS degrees in electronics engineering, and the PhD degree in electronic and electrical engineering from Kyungpook National University, Daegu, South Korea, in 2015, 2017, and 2021, respectively. He is currently a researcher with Electronics and Telecommunications Research Institute, Daejeon, South Korea. His research interests include authentication, blockchain, anonymous credentials, decentralized identifier, Internet of Things, post-quantum cryptography, VANET, and information security.

JoonYoung Lee received the BS and MS degrees in electronics engineering in 2018 and 2020, respectively, from Kyungpook National University, Daegu, South Korea, where he is currently working toward the PhD degree with the School of Electronic and Electrical Engineering. His research interests include authentication, Internet of Things, and information security.

Ashok Kumar Das (Senior Member, IEEE) received the MSc degree in mathematics, the MTech degree in computer science, and the PhD degree in computer science and engineering from the Indian Institute of Technology Kharagpur (IIT Kharagpur), Kharagpur, India. He is currently an associate professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. He has authored more than 295 papers in international journals and conferences, including more than 250 reputed journal papers in his research field, which include cryptography, system and network security, security in vehicular ad hoc networks, smart grids, smart homes, Internet of Things (IoT), Internet of Drones, Internet of Vehicles, Cyber-Physical Systems (CPS) and cloud computing, intrusion detection, blockchain, and AI/ML security. He was the recipient of the Institute Silver Medal from IIT Kharagpur. He is included in the subject-wise ranking of top 2% scientists from India (all fields) in the area of networking and telecommunications, with Rank world-wide (by subject area): 321. He is also listed in the top H-Index for Scientists in the World for Computer Science database maintained by Research.com with World Ranking: 1645 and National Ranking (India): 9. He is on the editorial board of the *IEEE Systems Journal*, *Journal of Network and Computer Applications (Elsevier)*, *Computer Communications (Elsevier)*, *Journal of Cloud Computing (Springer)*, *Cyber Security and Applications (Elsevier)*, *IET Communications*, *KSII Transactions on Internet and Information Systems*, and *International Journal of Internet Technology and Secured Transactions (Inderscience)*, and was a program committee member in many international conferences. He was one of the Technical Program Committee chairs of the first International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, June 2019, International Conference on Applied Soft Computing and Communication Networks (ACN'20), October 2020, Chennai, India, and second International Congress on Blockchain and Applications (BLOCKCHAIN'20), L'Aquila, Italy, October 2020. He is also an advisory board member of 3rd International Congress on Blockchain and Applications (BLOCKCHAIN '21), Salamanca, Spain, 6-8 October, 2021.

Youngho Park (Member, IEEE) received the BS, MS, and PhD degrees in electronic engineering from Kyungpook National University, Daegu, South Korea, in 1989, 1991, and 1995, respectively. He is currently a professor with the School of Electronics Engineering and School of Electronic and Electrical Engineering, Kyungpook National University. During 1996–2008, he was a professor with the School of Electronics and Electrical Engineering, Sangju National University, South Korea. During 2003–2004, he was a visiting scholar with the School of Electrical Engineering and Computer Science, Oregon State University, USA. His research interests include computer networks, multimedia, and information security.