Blockchain-Based Cyber-Physical Security for Electrical Vehicle Aided Smart Grid Ecosystem

Kuljeet Kaur, *Member, IEEE*, Georges Kaddoum, *Member, IEEE*, and Sherali Zeadally, *Senior Member, IEEE*

***Abstract*— The ever-growing trend of making the traditional power grids smarter than before has resulted in their gradual evolution to more sophisticated grids, referred to as Smart Grids (SGs) Cyber-Physical Systems with complex networking technologies. The integration of Information and Communication Technologies with power grids fosters seamless data sharing between different SG entities, which supports effective and smart governance in terms of demand response management, frequency support, and voltage stabilization. Nonetheless, this integration opens up several security and privacy concerns, namely, electricity theft, power loss, battery exhaustion, infrastructure mapping, *etc*. These issues become even more important with the addition of distributed energy sources, *e.g.* electric vehicles (EVs), battery energy storage systems, and renewable energy sources, into the SGs. We present a framework based on Software Defined Networking (SDN) and BlockChain (BC) to address two challenging issues of EV-aided SG ecosystems, namely, privacy assurance and power security. We leverage the capabilities of SDN to handle the complex interactions between different subsystems of the SG. Furthermore, we also employ BC and smart contracts' properties to secure energy transactions and data communications. We design a secure and efficient mutual authentication protocol based on Elliptic Curve Cryptography (ECC) and BC for privacy preservation during smart energy trading. We also proposed a BC-based smart contract for effective Demand Response Management (DRM) during bidirectional energy transfer between EVs and SG. Finally, we present experimental evaluations to validate the proposed framework's performance. The results obtained demonstrate the improved performance of the proposed scheme compared with current state-of-the-art approaches. The mutual authentication protocol designed is not only secure against major attack vectors (namely, session key security, message integrity, anonymity, forward secrecy, and so on), but it is also cost-efficient in terms of communication and computational costs. Additionally, the SC designed assures power security and maintains an adequate balance between demand and supply.**

***Index Terms*— Blockchain, electric vehicles, energy security, Ethereum, smart contract, smart grid, privacy.**

Manuscript received April 27, 2020; revised October 6, 2020; accepted November 23, 2020. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) and in part by the Tier 2 Canada Research Chair on the Next Generations of Wireless IoT Networks. The Associate Editor for this article was M. Guizani. *(Corresponding author: Kuljeet Kaur.)*

Kuljeet Kaur and Georges Kaddoum are with the Department of Electrical Engineering, École de Technologie Supérieure, Université du Québec, Montréal, QC H3C 1K3, Canada (e-mail: kuljeet.kaur@ieee.org; georges.kaddoum@etsmtl.ca).

Sherali Zeadally is with the College of Communication and Information, University of Kentucky, Lexington, KY 40506 USA (e-mail: szeadally@uky.edu).

Digital Object Identifier 10.1109/TITS.2021.3068092

NOMENCLATURE

$\mathbb{E}^{DEP}_{Base}(t)$	Baseline energy capacities of DEPs for DRM at t
$\mathbb{E}^{EV}_{DRM}$	An EV's energy contribution to the DRM
$\mathbb{E}^{EV}_{Rated}$	Battery rated capacity of an EV
$\mathbb{E}^{SG}_{Demand}(t)$	Total energy demand of SG at t
$\mathbb{E}^{SG}_{DRM}(t)$	Total energy needed for DRM at t
$\mathbb{E}^{SG}_{Supply}(t)$	Total energy consumed by SG's consumers at t
$\mathbb{I}(t)$	Rate of incentive associated for effective DRM at t
$\mathbb{I}^{*}(t)$	Incentives for the participating entities $(*)$ at t for effective DRM
$\mathbb{RS}^{DEP}(t)$	Demand response signal for the DEPs at t
$\mathbb{RS}^{DEP}(t)$	Energy that can be withdrawn or reduced by a particular DEP at time t for effective DRM
$\mathbb{RS}^{EV}(t)$	SC computed response signal for an EV at t
$\mathbb{RS}^{*}_{met}(t)$	Demand response signal met by the participating entities $(*)$ at t
$\mathbb{S}oC_{Char}$	SoC to fully charge an EV's battery
$\mathbb{S}oC_{curr}$	Current SoC of the EV's battery
$\mathbb{S}oC_{Dis}$	SoC that can be discharged by an EV's battery
$\mathbb{S}oC_{Max}$	Maximum SoC level of the EV's battery
$\mathbb{S}oC_{Min}$	Minimum SoC level of the EV's battery
$\mathcal{I}_i$	Identities of the SM/SDN controller
$\mathcal{T}_i$	Time-stamp for SM/SDN controller
a, b	Coefficients of E
$Auth_i$	Intermediate authentication tokens for SM/SDN controller
cur	Current
d_i	Private key of SM/SDN controller
E	The Elliptic curve considered
G	Finite prime field
$H_1(.)$	One-way collision resistant hash function
$H_2(.)$	One-way collision resistant hash function
n	Large prime number
P	Generator point of the curve
Q_i	Public key of SM/SDN controller
r_i	Pseudo random numbers for SM/SDN controller
SDN_j	j^{th} SDN controller referenced
SM_i	i^{th} SM referenced

SoC	State of Charge
T	Time
t	A time instant
t_h	Computation time for performing a one-way hash function
T_m	Computation time for performing a ECC point-multiplication
t_{add}	Computation time for performing a point addition
T_{bp}	Computation time for performing a bilinear pairing
T_{ed}	Computation time for performing encryption and decryption
T_{exp}	Computation time for performing a exponentiation operation
T_{mac}	Computation time for computing a message authentication code
vol	Voltage
BC	BlockChain
BESS	Battery Energy Storage System
CA	Certificate Authority
CU	Commercial Unit
DApps	Decentralized applications
DEPs	Distributed Energy Pro-consumer
DES	Distributed Energy Source
DRM	Demand Response Management
ECC	Elliptic Curve Cryptography
EV	Electric Vehicle
FHMQV	Fully Hashed Menezes-Qu-Vanstone
P2P	Peer-to-Peer
PBFT	Practical Byzantine Fault Tolerance
RES	Renewable Energy Source
SC	Smart Contract
SDN	Software Defined Network
SG	Smart Grids
SH	Smart Home
SM	Smart Meter
V2G	Vehicle-to-Grid

I. Introduction

WITH the evolution of Smart Grids (SGs), the conventional power grids have been revamped to enable easier management, higher efficiency, and enhanced reliability. Additionally, the SG paradigm also provides a bi-directional flow of power and information, which not only supports the smooth transfer of energy from the producers to consumers but also eases the fault diagnosis mechanism because data can be instantly retrieved. However, one of the crucial challenges associated with these power networks is their security. In the past, there have been several instances where the power grids have been compromised or attacked. For instance, in 2016, the US Department of Homeland Security admitted that one of their grids was compromised by the Russians [1]. Since the SGs are completely automated and equipped with remote access, even one minute of security lapse can significantly impact the entire community and ultimately result in cascading blackouts.

Thus, with the growing cyber-attacks on SGs, these power networks' security has gained substantial attention from academia and industry. In this context, the BlockChain (BC) technology is expected to bring disruptive changes by improving the security standards related to connectivity, data transfer, and access control. The technology of BC is based on the distributed ledger wherein all the nodes of the network maintain a copy of this ledger. The blocks in this ledger are cryptographically linked with each other, which makes the ledger immutable. The concept of BC was initially limited to the use of cryptocurrencies. However, with the advent of Smart Contracts (SC), BCs are being applied to numerous application domains, such as the Internet of Things, SG, Vehicle-to-Grid (V2G), Autonomous Vehicles, etc [2]. In this work, we focus on the application of BC and SC to secure SG operations.

A. Related Work

Musleh *et al.* in [3] reviewed different advantages of using BC in SG ecosystems. The authors also discussed various models proposed in the literature with their associated advantages and challenges. Additionally, the authors identified four potential sub-domains for using BC for higher stability, sustainability, and resiliency of SGs, namely, energy trading, cyber-and-physical security, and Electric Vehicles (EV). We review state-of-the-art results about these sub-domains below.

Wang *et al.* in [4] proposed an energy trading mechanism in crowdsourced energy systems using the concept optimization and BC. In this work, the authors employed the IBM Hyperledger Fabric as a baseline distributed ledger technology. Aitzhan *et al.* in [5] also used B for secure and anonymous energy trading along with multi-signatures and anonymous encrypted messaging streams. The authors in [6] used private BC for energy trading in the local electricity market. Likewise, the V2G energy trading mechanism also proposed an effective approach for valley filling and peak shaving. Considering this trend, Garg *et al.* [7] devised a hierarchical authentication scheme based on BC for securing the V2G trading environment.

Gupta *et al.* [8] reviewed cyberphysical attacks targeted on modern IoT-enabled power grids and identified some of the potential attack vectors as financial frauds, denial of service attacks, false data injection, and physical attacks. Working in the same direction, Minoli and Occhiogrosso [9] identified BC's use for securing IoT-enabled ecosystems. In this work, the authors discussed different application domains of BCs (such as SGs, Intelligent Transportation Systems, e-health, insurance, and banking). They emphasized the flexibility of BCs, which can be supported at both the communication model's physical and application layers. Likewise, the authors in [10] proposed a BC-envisioned secure solution for modern-day Smart Homes (SH). Along the same lines, mutual authentication is also considered crucial for securing SG ecosystems [11], [12]. Some of the notable contributions in this direction can be found in [7].

In [13], Liu *et al.* employed the concept of decentralized Blockchain for managing the charging/discharging activities and schedules of EVs in a SG setup. This work has focused

on reducing the power fluctuations at the grid level due to the unpredictable penetration of a large number of EVs. Besides, the work also focused on reducing the cost associated with the charging/discharging of EVs' batteries. In the latter work, the authors developed an adaptive BC mechanism based on the Iceberg order execution algorithm. Likewise, Jin *et al.* [14] identified the problem of charging electric taxis during working periods while simultaneously catching up with their advanced bookings. Thus, in this work, the authors used consortium BC to design an effective charging architecture for electric taxis to deal with charging disconnection and trust issues between different charging stations. Working in the same direction, in [15], the authors also used consortium BC for efficient charging of hybrid EVs. Some of the other contributions that leveraged BC technologies' advantages for generating charging/discharging schedules for EVs are presented in [16], [17].

B. Motivation

SG ecosystems are the next-generation power networks that rely on Information and Communication Technology to offer bi-directional energy and information transfer. The innovative technologies of SG and BC have significantly changed the power system industry's landscape in terms of enhanced efficiency and reliability [18]. However, with the emerging focus on distributed energy sources (such as renewable energy sources, SHs, EVs), the need to devise effective decentralized management solutions for SG has become mainstream. In this context, Software Defined Networks (SDNs) can play an essential role in significantly reducing the network management challenges and separating the control plane from the data plane. The SG environments are thus expected to benefit from the decentralization of the underlying network [19], [20]. Henceforth, in this work, we combine the benefits of decentralized BC and SDN paradigms to the SG ecosystem to enhance security and energy trading.

C. Research Contributions of This Work

The key research contributions of the proposed work are as follows.

1) We present a sophisticated framework based on SDN and BC to handle two challenging issues of SG ecosystems, *i.e.,* privacy assurance and power security.
2) For privacy preservation, we present an efficient mutual authentication and key agreement protocol based on Elliptic Curve Cryptography (ECC) and BC.
3) We then devise a secure energy trading mechanism based on BC for effective Demand Response Management (DRM).
4) Finally, we extensively evaluate the efficacy of the proposed scheme in terms of overhead, security features, and demand response.

D. Organization

The rest of the paper is structured as follows. We present some background information and the system model in Sections II and III, respectively. We describe the proposed scheme in Section IV while we present experimental evaluation results in Section V. Finally, Section VI concludes the work.

II. Background

In this section, we present some background information about BC and SC that are employed in our proposed scheme.

BC is a state-of-the-art technology that is essentially a shared digital ledger and is characterized by its property of immutability and decentralization. It is maintained by a peer-to-peer network which in turn, stores the history of transactions executed by the different peers using cryptographically linked blocks. In simpler words, BC can be understood as a chain of blocks wherein each block carries the transaction data, a predefined hash function, and a hash to the block preceding it. Since it is operated by a Peer-to-Peer (P2P) network, where there is no central control authority. This implies that all the nodes of the network conjointly work together to ensure that the chain is not altered and only legitimate transactions are incorporated into the chain. These interactions enable BC to invoke direct transactions between the nodes/individuals without the need to involve a third party in the overall process. The lack of any central authority in BC makes it attractive for deployment in different application domains to manage and keep track of the digital assets [21].

Thus, it is fair to say that BC is based on *"human trust"*. However, the highly secure framework of BC technology gains its tamperproof property because of the following assumption: *"any node can attack the BC at any given time frame"*. Thus, to safeguard the chain against intentional alteration, BC uses the concept of *"consensus protocol"*. These protocols work on the notion of democratic systems and ensure the correct operation of the network, even under malicious interventions.

Due to the above-mentioned security attributes, BC has been regarded as one of the most attractive technologies for various activities, such as cryptocurrency transactions, land records, healthcare, aviation, e-governance, data and network security, and many others [22], [23]. The global market of this disruptive technology is projected to reach almost USD 20 billion by 2024 [22]. In this vein, Gartner also forecasts that the business value associated with BC will flourish, reaching USD 176 billion by 2025. Recently, various countries, the Republic of Georgia, Sweden, and the UAE declared the potential use of BC for managing their digital assets related to property management, e-governance, and land registry, respectively.

In short, some of the distinguishing characteristics of BC are summarized as follows:

1) *Digital:* BC eliminates the use of manual documentation and maintains all the information in a digitized format.
2) *Distributed:* There is no central authority in BC, and thus all the nodes of the P2P network work in collaboration based on some set of predefined rules to validate the information to be added into the network. There is no single point of failure because the architecture of BC is highly distributed. In fact, the network continues to operate as usual even if one or more nodes fail.
3) *Immutable:* All the transactions in the BC network are cryptographically chained together using various

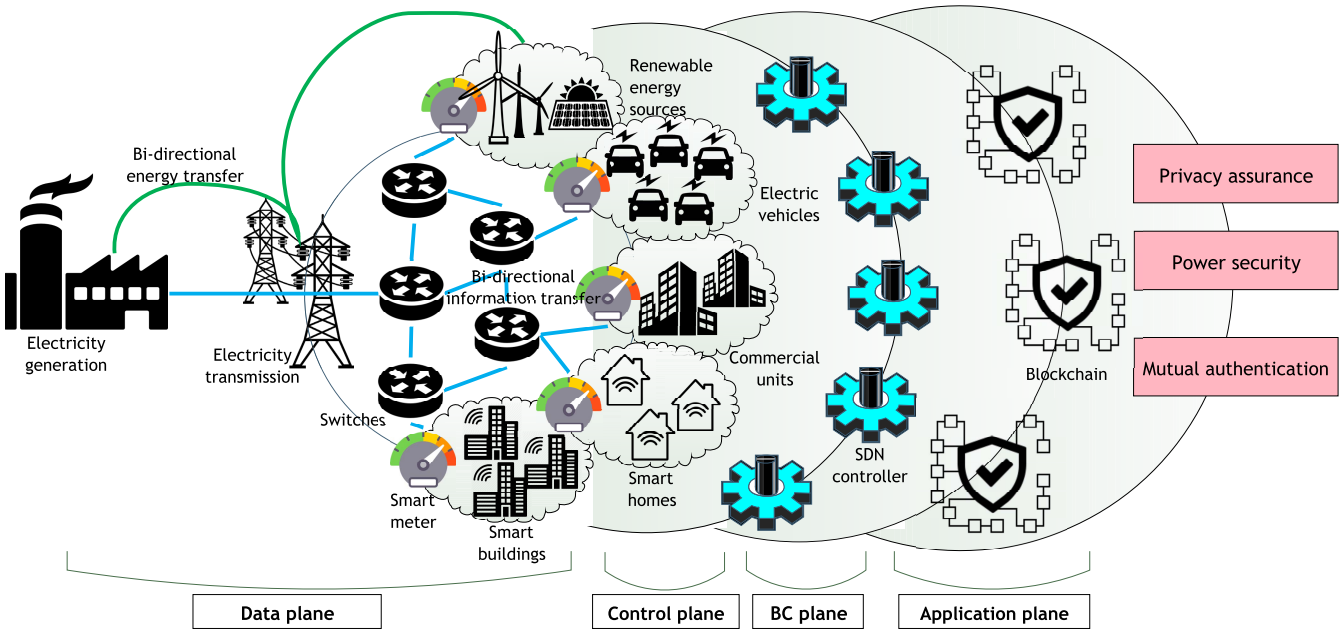

Fig. 1. An illustration of the proposed EV-aided SG using Blockchain and SDN.

parameters, namely, time, date, data, and hash of the previous block. Therefore, all the transactions to be recorded sequentially on the network, which makes them immutable.

4) *Chronology:* All the blocks are sequentially recorded on the BC network and linked with the preceding block using hashing to maintain a perfect chronology.
5) *Consensus Based:* As a result of the consensus mechanism, the nodes of the underlying P2P anonymously participate in the voting mechanism to validate every transaction on the ledger.
6) *Persistence:* The distributed ledger of BC prohibits any invalid transaction. This implies that any transaction that has been written on the ledger cannot be altered or deleted. Once a transaction has been added to the ledger, everything related to that transaction is "cryptographically sealed". This feature ensures data persistence, high-end robustness, and trust.
7) *Anonymity:* All the users interact with the ledger using a designated address which in turn keeps their identities anonymous.

Some of the most popular cryptocurrency currencies based on BC include Bitcoin, Ethereum, Ripple, and Litecoin. Since this work aims to extend the notion of Ethereum for the SG paradigm, we, therefore, focus on Ethereum. The concept of Ethereum was first proposed by Vitalik Buterin and was released in 2015. Its inception was driven by BC and the goal was to extend its use beyond the financial domain. Today, Ethereum is being used in applications beyond trading and cryptocurrency using *"SCs"*. The concept of SC is based on a set of rules that the underlying nodes of the ledger use to interact with each other. The contract encompasses some pre-defined rules which automatically trigger an agreement if satisfied. The contract is implemented using the consensus mechanism. The inventors of Ethereum aimed to employ Ethereum to decentralize the Internet by using the concept of SC. These user-defined contracts can be used to develop decentralized applications (DApps) and are used in a plethora of domains.

Some of the main benefits of using Ethereum include:

1) A third party cannot make alterations to the data stored on Ethereum.
2) It is immutable.
3) It is characterized by high security.
4) It has almost zero downtime.

III. System Model

This section presents the high-level architectural diagram of leveraging the benefits of Ethereum and SC for establishing a secure SDN-enabled SG ecosystem.

A typical SG setup comprises of two components, *i.e.,* electricity producers and consumers. The former comprises the usual large-scale power generation plants, Renewable Energy Sources (RESs), and Distributed Energy Sources (DESs) such as EVs, and Battery Energy Storage Systems (BESS). The latter, on the other hand, incorporates SHs, smart buildings, industrial units, commercial plants as well as EVs and BESSs, also referred to as Distributed Energy Pro-consumers (DEPs). All these DEPs regularly consume energy from the SG. However, due to the evolution of SGs, these units can reduce their energy consumption and give the energy back to the grid whenever required for effective DRM. Figure 1 illustrates the key components of the proposed SG ecosystem equipped with the Ethereum, SC, and SDN functionalities. As the figure shows, the ecosystem considered is segregated into the following planes, namely, data plane, Control, BC, and application plane. We describe these planes below.

The lowest plane is the *"Data Plane"* which comprises the electricity consumers connected to SG via dedicated Smart Meters (SMs). SMs help in regulating and tracking the energy

consumption profile of all the pro-consumers in real-time. Above this layer lies the *"Control Plane"* which comprises the SDN controllers handling the control operations of the underlying network. Finally, above this layer resides the *"BC Plane"* which comprises different ledgers and SCs to maintain the transactions related to authentication and energy trading, respectively. Overall, the functionalities of Ethereum and SC have been used to accomplish the following tasks: i) enhancing the security of the SG ecosystem using an authentication-based mechanism and ii) securing the energy trading process used for DRM (the following section discusses these components in detail). It is worth mentioning here that SDN controllers serve as the nodes for the distributed ledger(s) and are responsible for validating the transactions and maintaining the entire ledger(s). The highest layer is the *"Application Plane"*, which provides various services to the ecosystem considered in terms of higher security and effective DRM.

IV. Proposed Scheme

This section explains the rationale behind the operation of the proposed scheme. Broadly, the proposed scheme executes the following phases:

A. Phase I: Ethereum for Secure and Mutual Authentication

The SMs deployed across the pro-consumer's premises are intelligent devices that relay their energy consumption patterns to the SDN controller on a real-time basis. However, the data being relayed to the SDN controller is crucial to a customer's privacy [24] and is prone to different attack vectors, *i.e.,* denial of service, man-in-the-middle, forward secrecy, and replay attack. Thus, it is essential to protect it against potential data tampering attacks. Thus the proposed scheme employs an efficient authentication and key agreement mechanism based on Ethereum and ECC. In the former phase, the mutual authentication between the SMs and SDN controllers takes place. Next, they compute a common session key to protect their future communications. Afterward, Ethereum is employed to keep track of all the authentication transactions using two ledgers, namely *Whitelist Ethereum* and *Blacklist Ethereum*. We present the related details below and Fig. 2 shows the steps involved.

Broadly, this phase can be categorized into the following steps:

1) Mutual authentication
2) Key agreement
3) Transaction generation and verification
4) Transfer of transactions to the ledger

The related details of these sub-steps is elaborated below.

1) Step 1 & 2: Mutual Authentication and Key Agreement: The initial phase incorporates mutual authentication and key agreement based on ECC. The details of this phase can be found in our previous work [12]. A short summary of these phases is detailed as follows and the related symbols are defined in the nomenclature.

The designed mechanism for mutual authentication and key exchange between the SMs and the SDN controllers leverages the hardness of the ECC and Fully Hashed

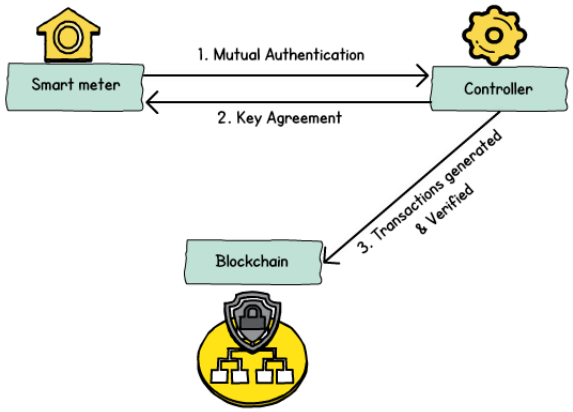

Fig. 2. Steps for secure and mutual authentication using BC.

SM	CA
-Select a random identity $\mathcal{I}_{SM}$	
$\xrightarrow{<\mathcal{I}_{SM}\ \text{Over Secure Channel}>}$	
	-Check the uniqueness $\mathcal{I}_{SM}$
	-If ($\mathcal{I}_{SM}$ is not unique)
	-Repeat
	-Else
	-Generate $d_{SM} \in Z_p^*$
	-Compute $\mathcal{Q}_{SM} = d_{SM}.P$
$\xleftarrow{<d_{SM}, \mathcal{Q}_{SM}\ \text{Over Secure Channel}>}$	
-Save $< d_{SM}, \mathcal{Q}_{SM} >$	

Fig. 3. An illustration of the SM registration Phase.

Menezes-Qu-Vanstone (FHMQV) at its core. However, before the SMs and SDN controllers authenticate each other and establish a secure session key, it is essential for them to have certain pre-defined parameters and register themselves with the certificate authority (CA). The former is referred to as *'System Initialization'* while the latter is called *'Registration'*.

a) System Initialization: During the process of system initialization, important cryptographic parameters are defined by the CA. These parameters comprise a chosen Elliptic curve E along with its essential parameters $< P,\ n,\ G,\ a,\ b >$. Here, the parameters P and n refer to the generator point and a large prime number, respectively. On the other hand, G denotes the finite prime field and $< a,\ b >$ represents the coefficients of the curve [12]. These parameters are made public which are then used by the participating entities to establish authenticity and trust.

b) Registration: Following this, the SMs and the SDN controllers register themselves one by one with the CA. As the end result of this sub-phase, the legitimate entities are assigned unique identities ($\mathcal{I}_i$) along with a private-and-public key pairs ($d_i \in Z_p^*$ and $\mathcal{Q}_i = d_i.P$; wherein $i \in$ {SMs, SDN Controllers}). As illustration of this sub-phase is given below:

c) Mutual Authentication & Key Agreement: Finally, the registered SMs and SDN controllers then participate in a cryptographic challenge to mutually authenticate each other and establish a secure session key. The process comprises the

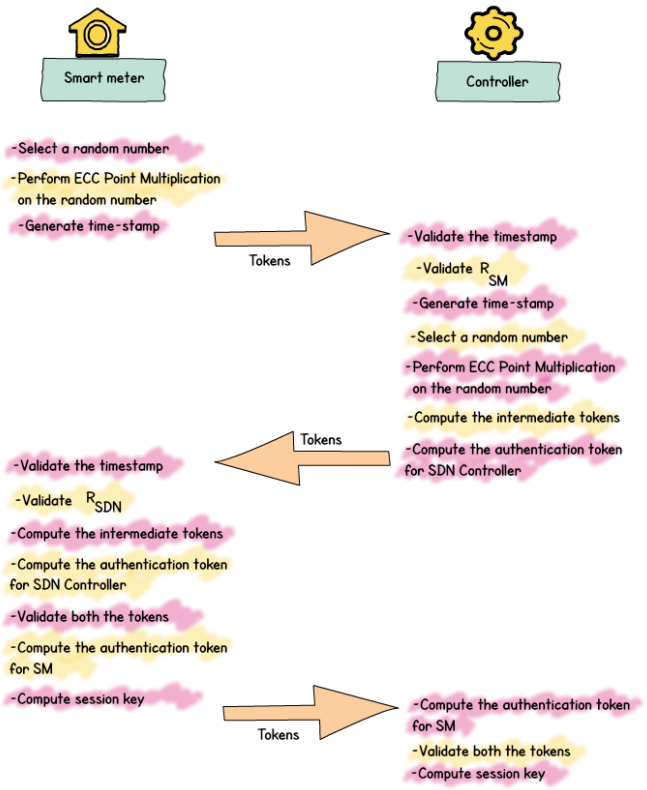

Fig. 4. An illustration of the mutual authentication and key agreement phase [12].

computation of the different intermediate tokens that are sent by the two parties to each other to authenticate each other and agree on a common session key if they trust each other. Fig. 4 illustrates these sub-phases. We present the intermediate steps below:

Step 1: The SM initiates the process by generating a random number, say $r_{SM} \in Z_p^*$. Following this, it performs an ECC point multiplication operation on r_{SM} ($\mathcal{R}_{SM} = r_{SM}.P$) and generates a timestamp $\mathcal{T}_{SM}$. After all these computations, the SM sends the tokens $< \mathcal{I}_{SM}, r_{SM}, \mathcal{R}_{SM}, \mathcal{T}_{SM} >$ to its respective SDN controller.

Step 2: After receiving these tokens, the SDN controller verifies the received $\mathcal{T}_{SM}$. If it is within the timeframe window, then it continues to authenticate; else it drops the connection. Then, it checks if $\mathcal{R}_{SM}$ belongs to G^*. Next, the SDN controller initiates the authentication process and generates a time-stamp $\mathcal{T}_{SDN}$ and a random number $r_{SDN} \in Z_p^*$. Then it computes $\mathcal{R}_{SDN} = r_{SDN}.P$ using an ECC point multiplication.

Step 3: Using the values of $\mathcal{R}_{SM}$, $\mathcal{R}_{SDN}$, $\mathcal{Q}_{SM}$, $\mathcal{Q}_{SDN}$, $\mathcal{T}_{SM}$, & $\mathcal{T}_{SDN}$, the SDN controller computes the following intermediate tokens according to the following sequence:

$$d = H_1(\mathcal{R}_{SM}, \mathcal{R}_{SDN}, \mathcal{Q}_{SM}, \mathcal{Q}_{SDN}, \mathcal{T}_{SM}, \mathcal{T}_{SDN}) \quad (1)$$

$$e = H_1(\mathcal{R}_{SDN}, \mathcal{R}_{SM}, \mathcal{Q}_{SM}, \mathcal{Q}_{SDN}, \mathcal{T}_{SM}, \mathcal{T}_{SDN}) \quad (2)$$

$$s_{SDN} = r_{SDN} + ed_{SDN} \bmod q \quad (3)$$

$$\sigma_{SDN} = s_{SDN}(R_{SM} + dQ_{SM}) \quad (4)$$

Finally, the above computed intermediate tokens are used to compute an authentication token for the SDN controller ($Auth_{SDN}$) as follows:

$$Auth_{SDN} = H_2(\sigma_{SDN}||\mathcal{T}_{SM}||d_{SDN}R_{SDN}) \quad (5)$$

Next, the message string $< r_{SDN}, \mathcal{R}_{SDN}, \mathcal{T}_{SDN}, Auth_{SDN} >$ is sent to the SM for authentication establishment.

Step 4: After receiving the above message, the SM first validates $\mathcal{T}_{SDN}$ and $\mathcal{R}_{SDN}$. Following successful validation, it generates the following intermediate tokens $(d, e, s_{SM}, \sigma_{SM})$ and an authentication token ($Auth^*_{SDN}$) to verify the SDN controller's authenticity.

$$d = H_1(\mathcal{R}_{SM}, \mathcal{R}_{SDN}, \mathcal{Q}_{SM}, \mathcal{Q}_{SDN}, \mathcal{T}_{SM}, \mathcal{T}_{SDN}) \quad (6)$$

$$e = H_1(\mathcal{R}_{SDN}, \mathcal{R}_{SM}, \mathcal{Q}_{SM}, \mathcal{Q}_{SDN}, \mathcal{T}_{SM}, \mathcal{T}_{SDN}) \quad (7)$$

$$s_{SM} = r_{SM} + dd_{SM} \bmod q \quad (8)$$

$$\sigma_{SM} = s_{SM}(R_{SDN} + eQ_{SDN}) \quad (9)$$

$$Auth^*_{SDN} = H_2(\sigma_{SM}||\mathcal{T}_{SM}||r_{SDN}Q_{SDN}) \quad (10)$$

Finally, the SM checks the equivalency of the computed ($Auth^*_{SDN}$) and the received authentication token ($Auth_{SDN}$), and following a successful verification, the SM considers the SDN controller as legitimate.

Step 5: In this step, the SM computes an authentication token for itself $Auth_{SM} = H_2(\sigma_{SM}||\mathcal{T}_{SDN}||d_{SM}.\mathcal{R}_{SM})$ following a common session key ($SK = kdf(\sigma_{SM}||\mathcal{T}_{SM}||\mathcal{T}_{SDN})$). The computed $< Auth_{SM} >$ is then transmitted to the SDN controller for verification.

Step 6: After receiving $< Auth_{SM} >$, the SDN controller verifies the received token where an equivalence establishes the legitimacy of the SM. After successful verification, the SDN controller computes its common session key $SK = kdf(\sigma_{SDN}||\mathcal{T}_{SM}||\mathcal{T}_{SDN})$.

2) Step 3 & 4: Transaction Generation, Verification, and Transfer to the Ledger: Following successful authentication, the SC related to the *Whitelist Ethereum* is invoked and the details of the associated SM and SDN controllers are transferred to the ledger using the consensus mechanism. In contrast, unsuccessful authentication attempts invoke the SC related to *Blacklist Ethereum* to record the related transactions on the ledger. After every successful authentication between a set of SMs and the SDN Controller, their respective IDs are transferred to the Blockchain whitelist ledger. Next time, if any authentication request is generated between the same parties, the server checks if the participating entities have been legitimate sources in the past (using the whitelist ledger). If so, the authentication mechanism can be ignored to reduce the overhead for mutually authenticating the parties. However, to ensure higher security, the SC checks the blacklist ledger in real-time and permits the authentication process to be skipped under certain timeframes only. The maintenance of these two ledgers helps streamline the authentication and key exchange process and reduce the overhead involved in key generation and authentication establishment for each communication. Moreover, with the vision of the blacklist ledger, the illegitimate sources can be kept at bay from the very beginning.

The consensus mechanism adopted to transfer the details of SMs and the SDN controllers to the different ledgers is called the Practical Byzantine Fault Tolerance (PBFT). For PBFT, let us assume that we have k working peers (in our case, working peers are the SDN controllers), which will play a quintessential role in writing the authentication results to the ledger. In every consensus round, a WP is selected as the speaker while the rest takes up the role of congressmen. We present the detailed procedure below:

1) In the first step, a speaker is selected using the following relation: $i = (\text{height mod} k) + 1$ wherein i denotes the selection of the i^{th} WP as the speaker. This selection process is crucial because the speaker can host the consensus process n number of times although the speaker cannot affect the results of the consensus.
2) Next, any SMs or a SDN controller broadcast the results of the authentication (legitimate for the Whitelist and illegitimate for the Blacklist). All the WPs scan these broadcast messages and store their information in their corresponding memories.
3) Once the "block" for the transmitted message has been created (say after t seconds), the speaker sends a message to all the congressmen to cast their respective votes using the template: $< p_{req}$, height, WP_i, block, Sig_{WP_i}(block) $>$ wherein p_{req} denotes the request of the leader to all congressmen to cast their votes.
4) Next, the congressmen cast their votes for the generated block by sending the message $< p_{res}$, height, WP_j, block, Sig_{WP_j}(block) $>$.
5) If a WP receives Sig_{WP_j}(block) from at least $(k - f)$ peers, then the WP publishes the block; else the next round of consensus is executed. Here, the value of $f = \lfloor (k-1)/3 \rfloor$ denotes the upper limit on the number of erroneous WPs that can be part of the system.

B. Phase II: Ethereum for Secure and Anonymous Energy Trading

The DRM and the subsequent energy trading in the setup considered are achieved using the concept of SCs. In the proposed work, we define SC to enforce a delicate balance between the grid's load and production. In other words, the SC's rules define the situation and will allow the DEPs to participate in DRM by withdrawing/injecting energy, or reducing the current load. In the event of a substantial imbalance between the SG's load and generation profile, equivalent demand response is triggered by the SC. This signal, in turn, is communicated to the different DEPs along with the penalty and incentive attributes.

For instance, the following equation depicts the squid imbalance between electricity generation and consumption:

$$\mathbb{E}^{SG}_{DRM}(t) = \mathbb{E}^{SG}_{Demand}(t) - \mathbb{E}^{SG}_{Supply}(t). \tag{11}$$

In the above equation, $\mathbb{E}^{SG}_{Demand}(t)$ refers to the total energy demand of the SG at time t while $\mathbb{E}^{SG}_{Supply}(t)$ denotes the total energy being consumed by its consumers. The difference between these two attributes depicts the energy that needs DRM ($\mathbb{E}^{SG}_{DRM}(t)$). The related scenarios are illustrated below.

$$\mathbb{E}^{SG}_{DRM}(t) = \begin{cases} 0; & \text{SG is balanced} \\ > 0; & \text{Energy needs to be injected to SG} \\ < 0; & \text{Energy can be withdrawn from SG} \end{cases} \tag{12}$$

In the first case, no DRM is required. However, in the latter two scenarios, the participating DEPs can change their energy consumption patterns to participate in the grid regulation mechanism. It is worth mentioning here that the energy computations for the EVs are different from the rest of the DEPs because they support a bi-directional flow of energy. We provide the related details below.

The amount of energy needed to charge or discharge an EV's battery is dependent on the current ($\mathbb{S}oC_{curr}$), maximum ($\mathbb{S}oC_{Max}$), and minimum State of Charge ($\mathbb{S}oC_{Min}$) as described below [25].

$$\mathbb{S}oC_{Char} = \mathbb{S}oC_{Max} - \mathbb{S}oC_{curr} \tag{13}$$

$$\mathbb{S}oC_{Dis} = \mathbb{S}oC_{curr} - \mathbb{S}oC_{Min} \tag{14}$$

here, $\mathbb{S}oC_{Char}$ depicts the SoC to fully charge an EV's battery while $\mathbb{S}oC_{Dis}$ represents the SoC that can be discharged by an EV. Consequently, their charging and discharging energy levels are computed using the following equation:

$$\mathbb{E}^{EV}_{DRM} = \frac{\mathbb{S}oC_* \times \mathbb{E}^{EV}_{Rated}}{100};\ \mathbb{S}oC_* \in \{\mathbb{S}oC_{Char}, \mathbb{S}oC_{Dis}\} \tag{15}$$

where, $\mathbb{E}^{EV}_{DRM}$ depicts EV energy contribution to the DRM and $\mathbb{E}^{EV}_{Rated}$ represents the battery rated capacity of the EV. Based on the computed value of $\mathbb{E}^{EV}_{DRM}$, the SC computes its equivalent demand response signal ($\mathbb{RS}^{EV}(t)$) as follow.

$$\mathbb{RS}^{EV}(t) = \mathbb{E}^{EV}_{DRM}(t) * \frac{|\mathbb{E}^{SG}_{DRM}(t)|}{|\sum_x \mathbb{E}^{EV}_{DRM}(t) + \sum_y \mathbb{E}^{DEP}_{Base}(t)|}. \tag{16}$$

The other participating DEPs share their baseline energy capacities for DRM ($\mathbb{E}^{DEP}_{Base}(t)$). Consequently, the demand response signal ($\mathbb{RS}^{DEP}(t)$) is computed for all the DEPs as follows:

$$\mathbb{RS}^{DEP}(t) = \mathbb{E}^{DEP}_{Base}(t) * \frac{|\mathbb{E}^{SG}_{DRM}(t)|}{|\sum_x \mathbb{E}^{EV}_{DRM}(t) + \sum_y \mathbb{E}^{DEP}_{Base}(t)|} \tag{17}$$

here, $\mathbb{RS}^{DEP}(t)$ depicts the energy that can be withdrawn or reduced by a particular DEP at time t for effective DRM.

The SDN controller then relays the computed regulation signals to the respective DEPs, which participate in the DRM process by serving the response signal ($\mathbb{RS}^*_{met}(t)$). Accordingly, the SC computes their respective incentives ($\mathbb{I}^*(t)$) wherein $\mathbb{I}(t)$ is the incentive associated for effective DRM at time t.

$$\mathbb{I}^*(t) = \mathbb{RS}^*_{met}(t) \times \mathbb{I}(t);\ (*) \in \{DEP,\ EV\} \tag{18}$$

Once the DEPs transfer the required energy and balance the demand-supply curve, the SDN controllers then create the

necessary transactions. These transactions are then verified using the consensus mechanism, then the block is added to the ledger and the associated incentives, also known as ethers, are transferred to the respective DEPs.

Smart Contract Employed: The proposed framework presents a trusted and secure medium for the participants to communicate and share their energy profiles in real-time. Additionally, it also supports an autonomous and decentralized platform of BC for monitoring and executing transactions using SCs. Using the SC designed, the participating entities (in this case SG, DEPs, and EVs) can contribute to effective DRM to maintain higher grid stability without relying on a centralized third party and enforce an efficient trading mechanism.

To enforce smart and efficient energy trading among the SG, DEPs, and EVs, we use the concept of SC. The SC designed incorporates different functions, which are discussed as follows. The function *generateEnergyLoadCurve()* runs on a periodic basis and checks the demand-supply gap according to Eq. (11). Next, the SC triggers a positive or negative response signal to the DEPs and EVs. Here, the positive response signal indicates a higher energy supply and lower consumption and vice versa. Upon receiving the response signal, the DEPs and EVs compute their individual baseline energy capacities using the function *computeBaseCapacities()*. The computation results are then relayed from the DEPs to the SC via the SDN Controller. The SC then computes DEPs' respective response signals and incentives (using the *computeResponseSignal()* and *computeIncentives()* functions). After a successful energy trade, the incentives are transferred by the SC using the BC ledger to the concerned parties. For the sake of clarity, we highlight the components of the SC designed using Algorithm 1.

Algorithm 1 Smart Contract for Effective DRM

function `main()`**:**
  Execute `generateEnergyLoadCurve()`
  Execute `computeBaseCapacities()`
  Execute `computeResponseSignal()`
  Execute `computeIncentives()`
  Execute `computeIncentives()`

function `generateEnergyLoadCurve(`t`)`**:**
  Extract $\mathbb{E}^{SG}_{Demand}(t)$ for t
  Extract $\mathbb{E}^{SG}_{Supply}(t)$ for t
  Compute $\mathbb{E}^{SG}_{DRM}(t)$ using Eq. (11)
  return $\mathbb{E}^{SG}_{DRM}(t)$

function `computeBaseCapacities(`$\mathbb{E}^{SG}_{DRM}(t)$, t`)`**:**
  for *each EV* x **do**
    Compute $\mathbb{E}^{EV}_{DRM}$ using Eq. (15)
  for *each DEP* y **do**
    Compute $\mathbb{E}^{DEP}_{Base}$
  return $\mathbb{E}^{EV}_{DRM}$, c, $\sum_x \mathbb{E}^{EV}_{DRM}$, $\sum_y \mathbb{E}^{DEP}_{Base}$

function `computeResponseSignal(`$\mathbb{E}^{SG}_{DRM}(t)$, $\mathbb{E}^{SG}_{DRM}(t)$, $\sum_y \mathbb{E}^{DEP}_{Base}$`)`**:**
  if $|\mathbb{E}^{SG}_{DRM}(t) \leq (|\sum_x \mathbb{E}^{EV}_{DRM}| + |\sum_y \mathbb{E}^{DEP}_{Base}|)$ **then**
    Set $\mathbb{RS}^{EV}(t)$ using Eq. (16); $\forall x$
    Set $\mathbb{RS}^{DEP}(t)$ using Eq. (16)$\forall y$
  else
    Set $\mathbb{RS}^{EV}(t) = \mathbb{E}^{EV}_{DRM}$
    Set $\mathbb{RS}^{DEP}(t) = \mathbb{E}^{DEP}_{Base}$
  return $\mathbb{RS}^{EV}(t), \mathbb{RS}^{DEP}(t)$

function `computeIncentives(`$first$, $second$`)`**:**
  for *each EV* x **do**
    Compute $\mathbb{I}^{EV}(t)$ using Eq. (18)
  for *each DEP* y **do**
    Compute $\mathbb{I}^{DEP}(t)$ using Eq. (18)
  return $\mathbb{I}^{*}(t)$

V. Experimental Evaluations

The proposed scheme comprises two different phases, *i.e.,* mutual authentication and energy trading for effective DRM. Thus, the parameters used for the evaluation of the two phases differ and are described below.

A. Evaluation of Phase I

The first phase incorporates the security aspect of the proposed scheme which helps in mutual authentication and deriving a secure session key for high data security. Thus, it is evaluated based on computation, communication, and energy overheads along with the security features supported.

1) Baseline Protocols Used for Evaluation: SMs form an important part of the SG ecosystem and use bidirectional communication between the pro-consumers and the utility provider. These communication channels between the two parties enable easier exchange, management, and control of the energy transfer. Nonetheless, the open channel is susceptible to different attack vectors and we need to maintain the anonymity of the SM. Thus, the works in [26]–[29] proposed the use of secure authentication and key agreement protocols between the participating entities to combat different security attacks and ensure SM anonymity. For instance, Tsai and Lo in [26] concentrated their attention on lightweight and secure authentication followed by a key exchange in the SMI network. In this work, two identity-based cryptosystems were used to attain the desired objectives. Odelu *et al.* [27] also extended the same notion and used ECC and identity-based encryption for the underlying encryption. Likewise, the authors of [28] proposed the concept of authentication and key exchange based on identity-based cryptography using

TABLE I

THE COMPUTATIONAL COST ASSOCIATED WITH DIFFERENT CRYPTOGRAPHIC OPERATIONS [29]

Cryptographic Operations	Time (ms)
Bi-linear Pairing	8700
ECC point multiplication	2900
Encryption	3.8
Decryption	41.1
One-way hash	39
MAC	8.6

ECC. The main focus of this work too was on securing the communication between the SMs and the utility providers. Kumar *et al.* [29] also employed the concept of a lightweight and energy-efficient authentication and key agreement for SMs using hybrid cryptographic algorithms.

Since the above-mentioned schemes work on identifying the challenges of SM anonymity and securing the communication from the SG perspective, like ours, we chose them for performance comparisons. The authentication and key exchange protocols proposed in these existing schemes have similar security and overhead challenges that we took into consideration in our proposed approach. Thus, we present a detailed analysis of the proposed mutual authentication mechanism by comparing it with state-of-the-art approaches described in [26]–[29].

2) Experimental Settings: For the experimental evaluation, we used a SMI network comprising a SM and a SDN controller similar to those used in [29]. We used a 2AA battery powered TelsoB mote along with a SM with the following configuration: 16 bit processor running at 8 MHz of clock frequency with 48 KB ROM and 10 KB RAM. We used a laptop (equipped with Intel 2.59 GHz processor and 16 GB of RAM) as the SDN controller. In our performance analysis, we have considered the following metrics: computational cost, communication cost, energy cost, and security features supported.

-Computation Cost Analysis: For the computational cost analysis, we consider the number of different cryptographic operations executed by the protocols and the time taken for their analysis. The computational cost of the different cryptography operations on the SMs (resource constraint) was computed by using different libraries and functions (e.g., TinyECC library with MD5 function and Advanced Encryption Standard symmetric-key algorithm). Amongst all these operations, the bi-linear pairing operation is considered to be the most expensive function and its computational complexity is approximately thrice that of the ECC point multiplication operation. Table I presents the computational costs associated with the execution of the different cryptographic operations on SMs. The results obtained show that the proposed scheme is the most efficient in terms of computational overhead.

The proposed protocol incurs a total computational overhead of 11,912 msec with a total of 4 ECC point multiplication and 8 one-way hash functions. Out of these operations, both the SM and the SDN controller executed 2 ECC point multiplication and 4 one-way hash functions. The detailed comparison is depicted in Table II and the results indicate that the proposed protocol leads to the minimum computational burden on the SMs and SDN controllers.

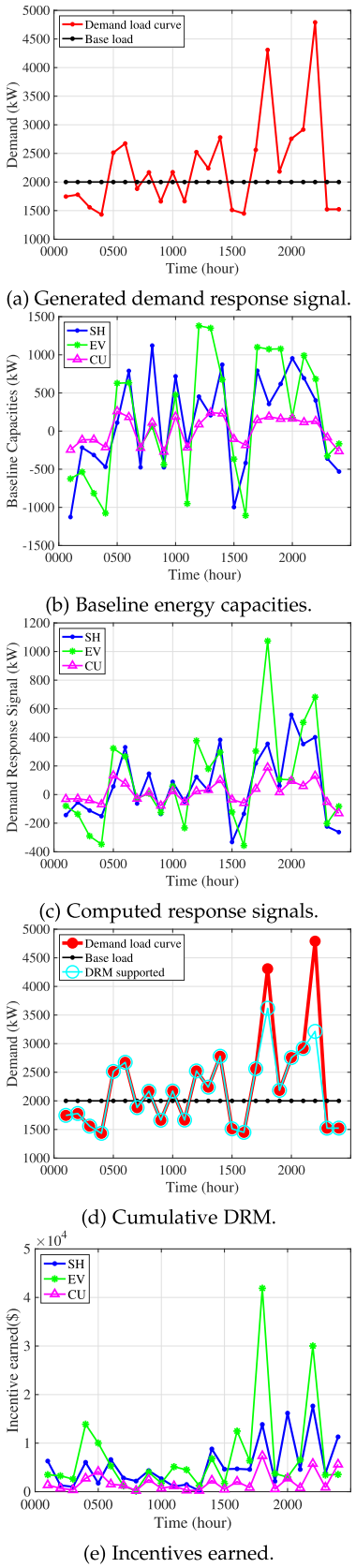

Fig. 5. An illustration of the DRM using the SHs, EVs, and CUs.

TABLE II
AN ANALYSIS OF THE COMPUTATIONAL COST

Schemes	SM	SDN Controller	Total Computational Cost
Tsai & Lo [26]	$4T_m + 1T_{add} + 1T_{exp} + 5T_h$	$3T_m + 2T_{bp} + 1T_{add} + 1T_{exp} + 5T_h$	$7T_m + 2T_{add} + 2T_{bp} + 2T_{exp} + 10T_h$
Odelu *et al.* [27]	$3T_m + 3T_{add} + 1T_{exp} + 6T_h$	$2T_m + 2T_{bp} + 3T_{add} + 1T_{exp} + 6T_h$	$5T_m + 6T_{add} + 2T_{bp} + 2T_{exp} + 12T_h$
He *et al.* [28]	$4T_m + 1T_{add} + 5T_h$	$6T_m + 2T_{add} + 6T_h$	$10T_m + 3T_{add} + 11T_h$
Kumar *et al.* [29]	$4T_m + 2T_{ed} + 2T_{mac} + 4T_h$	$3T_m + 2T_{ed} + 2T_{mac} + 5T_h$	$6T_m + 4T_{ed} + 4T_{mac} + 9T_h$
Ours	$2T_m + 4T_h$	$2T_m + 4T_h$	$4T_m + 8T_h$

T_m - ECC point-multiplication; T_{bp} - bilinear pairing; t_{add} - point addition; T_{exp} - exponentiation operation; t_h - one-way hash function; T_{ed} - encryption and decryption; T_{mac} - message authentication code.

TABLE III
AN ANALYSIS OF THE COMMUNICATION COST

Schemes	Sent (Bits)	Received (Bits)
Tsai & Lo [26]	2240	1184
Odelu *et al.* [27]	1248	672
He *et al.* [28]	832	800
Kumar *et al.* [29]	544	544
Ours	157	352

TABLE IV
AN ANALYSIS OF SM ENERGY UTILIZATION [12]

Schemes	Energy utilization (in μJ)
Tsai & Lo [26]	2572
Odelu *et al.* [27]	1443
He *et al.* [28]	1247
Kumar *et al.* [29]	832
Proposed protocol	398.16

-*Communication Cost Analysis:* Along similar lines, the communication cost analysis was also performed in terms of the number of tokens and bits transmitted between the SM and the SDN controller. The size of different tokens was considered as follows: ID = 1 byte (B), hash values = 16B, pseudo random numbers = 8B, MAC = 4B, time-stamp = 4B, and key size = 16 B [29]. Using these values, we calculated the communication costs of different schemes. For instance, the proposed scheme incurred 509 bits during the transmission of authentication tokens. More precisely, the SDN controller received a total of 157 bits and sent 352 bits during the authentication phase. Table III summarizes the results. Based on the results obtained, we note that the proposed protocol incurs the least amount of communication overhead.

-*Energy Cost Analysis:* The SMs are devices that are installed within the customer's premises and extract the energy from their households to support their routine operations. Thus, it is essential to minimize their energy consumptions. In this work we consider the energy required by the SMs in performing different cryptographic operations. For the computation purpose, we consider the following relation between voltage (vol), current (cur), and time (T) to perform different cryptographic functions at the SM.

$$vol \times cur \times T. \tag{19}$$

In the above equation, we set the values of vol and $curr$ to 3V and 1.8μ A, respectively, for a standard TelsoB SM. The detailed analysis is illustrated in Table IV. It is apparent from the obtained results that the proposed scheme incurs the least amount of energy consumption.

TABLE V
AN ANALYSIS OF THE SECURITY FEATURES PROVIDED

Security Feature/Protocol	[26]	[27]	[28]	[29]	Ours
F1	✓	✓	✓	✓	✓
F2	Weak	✓	✓	✓	✓
F3	–	–	✓	✓	✓
F4	✓	✓	–	✓	✓
F5	✓	✓	✓	✓	✓
F6	✓	✓	✓	✓	✓
F7	–	–	✓	✓	✓
F8	–	–	✓	✓	✓
F9	–	–	–	✓	✓

-*Security Feature Evaluation:* The proposed scheme provides the following security features: it supports mutual authentication (F1), session key security (F2), message integrity (F3), anonymity (F4), forward secrecy (F5), and replay protection (F6). Additionally, it resists impersonation attacks (F7), Man-in-the-Middle attacks (F8), and Denial of Service (F9). More detailed information about these security features is described in Table V.

B. Evaluation of Phase II: A Case Study of DEPs and EVs

To evaluate phase II of the proposed scheme, we considered the demand response provided by the cumulative support of DEPs and EVs. For this analysis, we assumed a simulation setup with 50 SHs, 20 commercial units (CUs), and 50 EVs. The EVs' batteries are assumed to have energy rating capacities in the range of 12 to 36 kWh. The load profile for the SHs and commercial units is adopted from the publicly available US open energy information [30]. Accordingly, we construct the load profile of the SG ecosystem considered as shown in Fig. 5(a). We considered a constant power supply of 2000 kW in our evaluation. From the figure, we note that the grid undergoes significant demand-supply imbalances over time. Thus, to reduce these fluctuations, we leverage the advantages of DEPs and EVs using the proposed approach. The SC designed first computes the baseline capacities of the participating SHs, EVs, and CUs for effective DRM management using the function *computeBaseCapacities()*. Fig. 5(b) shows the related results. For instance, at 1200 hours, the baseline capacities for the SHs, EVs, and CUs were 452, 1380, and 87 kWh, respectively. Next, the system executes the function *computeResponseSignal()* to compute the respective demand response signals for the SHs, EVs, and CUs (at 1200 hours,

computed as 123.21, 376.17, and 23.715 kWh respectively). Due to the active participation of the EVs and DEPs, the proposed approach was able to manage the demand response in most instances. For example, at 1200 hours, the proposed scheme was able to fully manage the demand-supply fluctuations by 523.1 kWh. After the energy transfer, the SC executes the function *computeIncentives()* to transfer the incentives to the EVs and DEPs based on their individual participation. Fig. 5(e) shows the results obtained. At 1200 hours, SHs, EVs, and CUs earned $ 284.58, 1478.52, and 4514.64 for energy trading. Thus, these results demonstrate the efficacy of our proposed scheme, which can be adopted for effective DRM.

VI. Conclusion

The main focus of this work was on privacy preservation and energy security using Blockchain technology. Coupled with the use of Blockchain, this work also applied the benefits of SDN to the SG ecosystem to implement a decentralized control mechanism. The proposed scheme employed *Ethereum* and *Smart Contracts* to support data security along with effective DRM. The data security was ensured using an ECC and Ethereum-based authentication and key agreement mechanism. On the other hand, DRM was ensured by transmitting well-computed demand response signals to the pro-consumers. Following this, the rewards were communicated to the pro-consumers involved using Ethereum anonymously. The experimental evaluation results support the applicability of the proposed scheme in the SG ecosystem.

Acknowledgment

The authors would like to thank the anonymous reviewers for the valuable comments which helped us improve the content, organization, and quality of this article.

References

[1] A. Arnold. (Apr. 2018). *How Blockchain Can Help Increase The Security Of Smart Grids*. Accessed: Jan. 2020. [Online]. Available: https://www.forbes.com/sites/andrewarnold/2018/04/16/how-blockchain-can-help-increase-the-security-of-smart-grids/#7d8c1c98b489

[2] S. Rasool *et al.*, "Blockchain-enabled reliable osmotic computing for cloud of things: Applications and challenges," *IEEE Internet Things Mag.*, vol. 3, no. 2, pp. 63–67, Jun. 2020.

[3] A. S. Musleh, G. Yao, and S. M. Muyeen, "Blockchain applications in smart grid–review and frameworks," *IEEE Access*, vol. 7, pp. 86746–86757, 2019.

[4] S. Wang, A. F. Taha, J. Wang, K. Kvaternik, and A. Hahn, "Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 8, pp. 1612–1623, Aug. 2019.

[5] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep. 2018.

[6] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: Towards sustainable local energy markets," *Comput. Sci.-Res. Develop.*, vol. 33, nos. 1–2, pp. 207–214, Feb. 2018.

[7] S. Garg, K. Kaur, G. Kaddoum, F. Gagnon, and J. J. P. C. Rodrigues, "An efficient blockchain-based hierarchical authentication mechanism for energy trading in V2G environment," 2019, *arXiv:1904.01171*. [Online]. Available: http://arxiv.org/abs/1904.01171

[8] A. Gupta, A. Anpalagan, G. H. Carvalho, L. Guan, and I. Woungang, "RETRACTED: Prevailing and emerging cyber threats and security practices in IoT-enabled smart grids: A survey," *J. Netw. Comput. Appl.*, vol. 132, pp. 118–148, Apr. 2019.

[9] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet Things*, vols. 1–2, pp. 1–13, Sep. 2018.

[10] A. Qashlan, P. Nanda, and X. He, "Automated ethereum smart contract for block chain based smart home security," in *Smart Systems and IoT: Innovations in Computing*. Singapore: Springer, 2020, pp. 313–326.

[11] S. Garg, K. Kaur, G. Kaddoum, F. Gagnon, S. H. Ahmed, and D. Nalin K. Jayakody, "LiSA: A lightweight and secure authentication mechanism for smart metering infrastructure," 2019, *arXiv:1907.08898*. [Online]. Available: http://arxiv.org/abs/1907.08898

[12] S. Garg, K. Kaur, G. Kaddoum, J. J. Rodrigues, and M. Guizani, "Secure and lightweight authentication scheme for smart metering infrastructure in smart grid," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3548–3557, May 2020.

[13] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25657–25665, 2018.

[14] Z. Jin, R. Wu, X. Chen, and G. Li, "Charging guiding strategy for electric taxis based on consortium blockchain," *IEEE Access*, vol. 7, pp. 144144–144153, 2019.

[15] X. Huang, Y. Zhang, D. Li, and L. Han, "An optimal scheduling algorithm for hybrid EV charging scenario using consortium blockchains," *Future Gener. Comput. Syst.*, vol. 91, pp. 555–562, Feb. 2019.

[16] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[17] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4601–4613, Jun. 2019.

[18] R. Talat *et al.*, "A decentralized system for green energy distribution in a smart grid," *J. Energy Eng.*, vol. 146, no. 1, Feb. 2020, Art. no. 04019036.

[19] M. Bräuning and R. Khondoker, "Analysis of SDN applications for smart grid infrastructures," in *SDN NFV Security*. Cham, Switzerland: Springer, 2018, pp. 99–110.

[20] K. Kaur, S. Garg, G. Kaddoum, S. H. Ahmed, F. Gagnon, and M. Atiquzzaman, "Demand-response management using a fleet of electric vehicles: An opportunistic-SDN-based edge-cloud framework for smart grids," *IEEE Netw.*, vol. 33, no. 5, pp. 46–53, Sep. 2019.

[21] S. Zeadally and J. B. Abdo, "Blockchain: Trends and future opportunities," *Internet Technol. Lett.*, vol. 2, no. 6, p. e130, Nov. 2019.

[22] G. K. Behara. (May 2019). *Why the Blockchain is so Secure*. Accessed: Jan. 2020. https://opensourceforu.com/2019/05/why-the-blockchain-is-so-secure/

[23] S. Rasool, A. Saleem, M. Iqbal, T. Dagiuklas, S. Mumtaz, and Z. U. Qayyum, "Docschain: Blockchain-based IoT solution for verification of degree documents," *IEEE Trans. Comput. Social Syst.*, vol. 7, no. 3, pp. 827–837, Jun. 2020.

[24] S. Zeadally, A.-S.-K. Pathan, C. Alcaraz, and M. Badra, "Towards privacy protection in smart grid," *Wireless Pers. Commun.*, vol. 73, no. 1, pp. 23–50, Nov. 2013.

[25] K. Kaur, S. Garg, N. Kumar, and A. Y. Zomaya, "A game of incentives: An efficient demand response mechanism using fleet of electric vehicles," in *Proc. 1st Int. Workshop Future Ind. Commun. Netw.*, 2018, pp. 27–32.

[26] 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.

[27] V. Odelu, A. Kumar 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.

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

[29] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, "Lightweight authentication and key agreement for smart metering in smart energy networks," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4349–4359, Jul. 2019, doi: 10.1109/TSG.2018.2857558.

[30] *Open Energy Information*. Accessed: Jan. 2020. [Online]. Available: http://en.openei.org/datasets/dataset/commercial-andresidential-hourly-load-profiles-for-all-tmy3-locations-in-theunited-states

Kuljeet Kaur (Member, IEEE) received the B.Tech. degree in computer science and engineering from Punjab Technical University, Jalandhar, India, in 2011, and the M.E. degree in information security and the Ph.D. degree in computer science and engineering from the Thapar Institute of Engineering and Technology (Deemed to be University), Patiala, India, in 2015 and 2018, respectively. She worked as a NSERC Post-Doctoral Research Fellow with the Department of Electrical Engineering, École de Technologie Supérieure, Université du Québec, Montréal, Canada. She is currently working as an Assistant Professor with the Department of Electrical Engineering, ÉTS, Montreal, and a Visiting Researcher with the School of Computer Science and Engineering (SCSE), Nanyang Technological University (NTU), Singapore. She has secured more than 50 research articles in top-tier journals, such as IEEE WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS (TII), IEEE TRANSACTIONS ON CLOUD COMPUTING (TCC), IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY (TVT), IEEE TRANSACTIONS ON MULTIMEDIA (TMM), IEEE TRANSACTIONS ON SMART GRID (TSG), IEEE SYSTEMS JOURNAL, IEEE INTERNET OF THINGS JOURNAL, *IEEE Communications Magazine*, IEEE WIRELESS COMMUNICATIONS, IEEE NETWORK, IEEE TRANSACTIONS ON POWER SYSTEMS (PS), *FGCS*, *JPDC*, and *PPNA* (Springer) and various International conferences, including IEEE Globecom, IEEE ICC, IEEE PES GM, IEEE WCNC, IEEE Infocom Workshops, ACM MobiCom Workshops, and ACM MobiHoc workshops. Her main research interests include cloud computing, energy efficiency, smart grid, frequency support, and vehicle-to-grid. She is a member of IEEE Communications Society, IEEE Computer, IEEE Women in Engineering, IEEE Software Defined Networks Community, IEEE Smart Grid Community, ACM, and IAENG. During her Ph.D., she received two prestigious fellowships, i.e., INSPIRE Fellowship from the Department of Science and Technology, India, in 2015, and a Research Scholarship from Tata Consultancy Services (TCS) from 2016 to 2018. She also received the IEEE ICC Best Paper Award in 2018 from Kansas City, USA, and the 2019 Best Research Paper Award from the Thapar Institute of Engineering and Technology, India. She serves as an Associate Editor for *Security and Privacy* (SPY) (Wiley) and *Journal of Information Processing Systems* (JIPS), *Human-centric Computing and Information Sciences* (HCIS) (Springer), and a Guest Editor for a Special Issue of IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS and IEEE OPEN JOURNAL OF THE COMPUTER SOCIETY (OJ-CS). She is a Website Co-Chair of the N2Women community. She also serves as the Vice-Chair for the IEEE Montreal Young Professionals Affinity Group.

Georges Kaddoum (Member, IEEE) received the bachelor's degree in electrical engineering from the École Nationale Supérieure de Techniques Avancées (ENSTA Bretagne), Brest, France, and the M.S. degree in telecommunications and signal processing(circuits, systems, and signal processing) from the Université de Bretagne Occidentale and Telecom Bretagne (ENSTB), Brest, in 2005, and the Ph.D. degree (Hons.) in signal processing and telecommunications from the National Institute of Applied Sciences (INSA), University of Toulouse, Toulouse, France, in 2009. In 2014, he was awarded the ÉTS Research Chair in physical-layer security for wireless networks. Since 2010, he has been a Scientific Consultant in the field of space and wireless telecommunications for several U.S. and Canadian companies. He is currently an Associate Professor and the Tier 2 Canada Research Chair with the École de Technologie Supérieure (ÉTS), Université du Québec, Montréal, QC, Canada. He has published over more than 170 journal articles and conference papers and has two pending patents. His recent research activities cover mobile communication systems, modulations, security, and space communications and navigation. He received the Best Papers Award from the 2014 IEEE International Conference on Wireless and Mobile Computing, Networking, Communications (WIMOB), with three coauthors, and the 2017 IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), with four coauthors. He received IEEE TRANSACTIONS ON COMMUNICATIONS Exemplary Reviewer Award for the years 2015 and 2017, and the Research Excellence Award from the Université du Québec in the year 2018 and the ÉTS in recognition of his outstanding research outcomes in the year 2019. He is currently serving as an Associate Editor for IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and IEEE COMMUNICATIONS LETTERS.

Sherali Zeadally (Senior Member, IEEE) received the bachelor's degree in computer science from the University of Cambridge, Cambridge, U.K., in 1991, and the Ph.D. degree in computer science from The University of Buckingham, Buckingham, U.K., in 1996.

He is currently working as an Associate Professor with the College of Communication and Information, University of Kentucky, Lexington, KY, USA.

Dr. Zeadally is a fellow of the British Computer Society and the Institution of Engineering Technology, U.K.