IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Securing Demand Response Management: A Certificate based Access Control in Smart Grid Edge Computing Infrastructure

SHEHZAD ASHRAF CHAUDHRY[1], HOSAM ALHAKAMI[2], ABDULLAH BAZ[3], FADI AL-TURJMAN[4,5]

[1]Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University Istanbul, Avcılar, 34310 Istanbul, Turkey (e-mail: sashraf@gelisim.edu.tr)
[2]Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah, Saudi Arabia e-mail: (hhhakam@uqu.edu.sa)
[3]Department of Computer Engineering, College of Computer and Information Systems, Umm Al-Qura University, Makkah, Saudi Arabia e-mail: (aobaz01@uqu.edu.sa)
[4]Artificial Intelligence dept., Near East University, Nicosia, Mersin 10, Turkey (e-mail: Fadi.alturjman@neu.edu.tr)
[5]Research Center for AI and IoT, Near East University, Nicosia, Mersin 10, Turkey

Corresponding author: Shehzad Ashraf Chaudhry (sashraf@gelisim.edu.tr)

The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by grant code 18-COM-1-01-0001

ABSTRACT The edge computing infrastructure has enabled a massive amount of data in the smart grid environment by a large number of connected automated devices to be processed at the edge of the network in proximity to the data generation source. The demand response management is a fundamental requirement for an efficient and reliable smart grid environment, which can be accomplished by the transfer of data between smart devices and the utility center (UC) in a smart city, very frequently. However, this frequent data transfer is subject to multiple threats including the tempering. Several authentication schemes were proposed to secure smart grid environment. However, many such schemes are either insecure or lack the required efficiency. To counter the threats and to provide efficiency, a new authentication scheme for demand response management (DRMAS) is proposed in this paper. DRMAS provides all necessary security requirements and resists known attacks. The proposed DRMAS is provably secure under formal analysis supplemented by a brief discussion on attack resilience. Moreover, the DRMAS completes the authentication procedure in just 20.11 ms by exchanging only 2 messages.

INDEX TERMS Smart Grid Security, Key Establishment, Device Access, Certificate, ECC, Incorrectness, Random Oracle Model

I. INTRODUCTION

SMART grid (SG) is envisioned to be the next generation power systems providing a seamless integration of cyber physical systems, information and communication technologies (ICT), and power generation and distribution domains. This advanced power grid system provides a bidirectional flow of energy between clients and utility service providers, and as a result the power consumption may be controlled and optimized in accordance with the real-time needs of the customer, which is productive for both customer as well as power generation domains. In comparison with conventional power grid, the SG-based system has advanced sensing and computing devices including sensors, actuators etc., for generating and transmitting the bidirectional flow of power-related real-time information. In SG-based system, there exist various levels of data flow to manage the demand response (DR). The short range communication technologies such as Zigbee, Bluetooth, Infrared, and 6LowPAN constitute the first level of information flow, while medium and long-range wireless communication networks such as LTE/LTE-A, WiMax, WiFi, and cellular networks represent the second level of information flow [1], [2]. These two levels of information flow for respective technology networks provide intelligent communication architecture for bridging the gaps

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2996093, IEEE Access

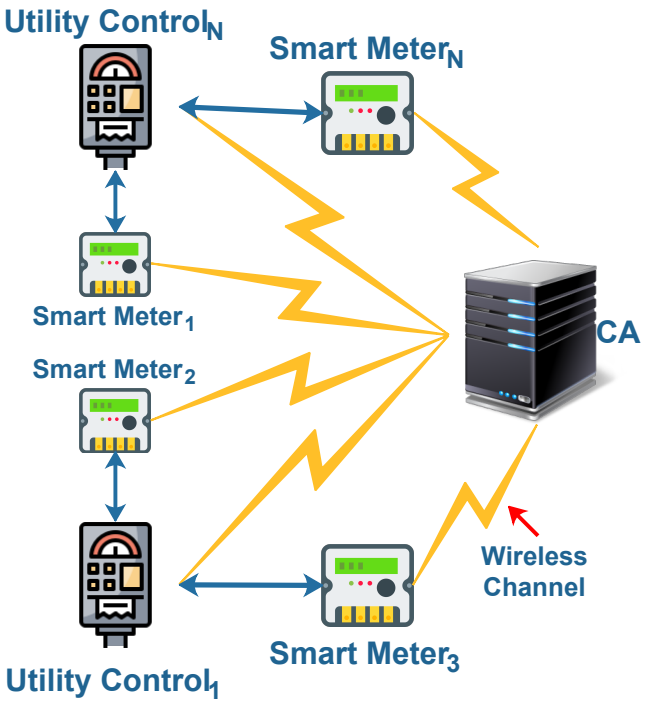

Figure 1: Demand Response Management

between demand and supply of electric power on real-time basis. A typical smart grid architecture is shown in Fig. 1. It is worthy to note that by utilizing DR the SG may convey the real-time information regarding the ideal price of electricity at regular time intervals (every 10-15 min) to enable the users to adjust the power usage accordingly. This could massively help the stakeholders in conserving energy and reducing overhead costs. Besides, the SG-based system increases the reliability, transparency and efficiency of the electric power system. The handling of SG-based big data with CPSS can greatly help in insightful decisions leading to more productivity for all stakeholders, and ultimately enrich the living environments as well as user experiences [3]. In the smart grid infrastructure, security has been one of the big concerns because most of the SG systems operate over insecure communication-based public network [4]–[7]. An adversary may comfortably intercept the information over these channels, and could initiate different attacks to recover the user's secret information. Such reliance of SG systems on public networks may land the stakeholders into troubles. To address those security issues, there must be robust communication infrastructure in the form of authentication protocols, supporting secure information exchange among the legitimate entities and maintaining the privacy as well [8]–[10].

In recent years many authentication protocols for SG environment can be witnessed. In this connection, a key distribution protocol for identity-based signature and encryption has been demonstrated by Tsai and Lo [11]. This protocol supports mutual authentication by constructing an agreed session key between smart meters (SMs) and the utility service provider. However, according to Odelu et al. [12] the scheme proposed in [11] is vulnerable to session specific temporary information threat, and in return may compromise the privacy of SMs on revealing secret credentials. Besides, countering the security drawbacks in [11], the Odelu et al. presented an improved SG-based authentication protocol. Later, Doh et al. [13] designed an authenticated key agreement scheme ensuring mutual authenticity to both participants, SM and UC. Afterwards, Saxena et al. [14] presented a scheme for smart grid systems making certain the security against insider and outsider threats as posed to the SG environment. Later, He et al., [15] presented an elliptic curve cryptography (ECC)-based key distribution protocol for SGs ensuring anonymity to the stakeholders. This scheme has comparatively low computational and communicational overheads in comparison with Tsai and Lo's scheme [11]. In [16], Mohammadali et al. presented an identity-based key management scheme employing elliptic curve cryptography to enhance the security of smart grid systems. However, Mahmood et al. [17] found that the scheme presented in [16] has serious weaknesses including the exposure of trusted authority's master key and is prone to many related attacks. Similarly, Mahmood et al. [18] also employed ECC to present a lightweight authenticated key agreement protocol to secure the interaction among clients and substations in the smart grid system. Nevertheless, Abbasinezhad-Mood and Nikooghadam [19] found that [18] does not comply with perfect forward secrecy, and was proved to be susceptible under CK adversarial model. Mahmood et al. presented another scheme [20], the authors in [21] argued that Mahmood et al.'s scheme [20] is vulnerable to ephemeral secret leakage and impersonation attacks. In 2018, another scheme [22] to provide security in SG environment was proposed by Challa et al. However, Chaudhry et al. [23] stated that the scheme [22] is unable to provide authentication between two entities of SG and has some other critical issues. The scheme of Chaudhry et al. [23] requires intervention of third party for establishing a secure connection between two SG devices. In 2019, Kumar et al. [24] proposed yet another temporal credential and ECC based authentication scheme for securing demand response management. However, the inherited incorrectness in their scheme to accommodate only one smart meter may restrict it's practical deployments and the obvious lack of initial verification on UC side, can encourage an adversary to force UC to process illegal requests [25].

A. MOTIVATIONS AND CONTRIBUTIONS

The SG-based system relies on internet-oriented communication and networking which renders the SG infrastructure vulnerable to several attacks including forgery attacks, impersonation attacks, man-in-the-middle attacks and replay attacks. This strong reliance of deployed smart meters (SMs) on ICT raise the same security concerns as already posed to ICT-based paradigms. These security loopholes may create

gaps between demand and supply of power if exploited by malicious intruders. Furthermore, these might lead to misleading forecasting models and findings related to DR management. Thus, there is dire need to restrain the probability of different known threats to provide a smooth flow to smart grid operations in terms of DR and data analytics. Most of the existing schemes for securing DR in SG environments are either vulnerable to many security threats or suffer from high computation and communication costs; mainly due to underlying pairing based operations. Therefore, we desperately need an authenticated key agreement protocol for SG environment supporting the SG device validation as well as the dynamic addition of Utility Centre (UC).For securing the demand response (DR) management, in this paper, we propose an authentication scheme $DRMAS$ which can mitigate pitfalls of existing schemes. The research contributions are illustrated as under:

1) A new certificate based authentication scheme $DRMAS$ is proposed to manage demand response in smart grid-based systems, which makes certain the exchange of sensitive information only after a mutually agreed session key is established between SG device and UC. The proposed scheme is free of any costly pairing based operations and completes authentication by exchanging only two messages.
2) We employed a universally accepted Real-or-Random (ROR) model [26], [27] to formally verify the security features.
3) The informal security analysis of the contributed scheme is also presented to prove the resistance of the scheme against all known attacks.
4) We compare the performance and security features of the proposed $DRMAS$ and related schemes.

B. THREAT MODEL

We employ the Dolev-Yao threat model [26] in our proposed protocol. Employed in a variety of protocols, [28]–[34], this model assumes an insecure public channel that is used by the communicating participants. Precisely, An adversary A may take this opportunity to misuse the intercepted communication data, since A might eavesdrop, replay, alter or delete any data during transmission by acting as an intermediary between the legal parties. Assuming, the smart devices are not tamper resistant, and the adversary could recover the stored contents from SG devices using power analysis attacks [35], [36]. We assume the trust authority (TA) to be fully trusted, and the utility centre (UC) as semi-trusted since both of these entities may not be compromised by the attacker.

II. DRMAS: PROPOSED SCHEME

This section explains the proposed $DRMAS$ for securing demand response management in smart grid environments. Proposed $DRMAS$ as depicted in Fig. 2 is detailed as follows:

Table 1: Notation guide

Notations	Description
$SD_i, UC_j, \mathcal{TA}$	SG device,Utility control, Trusted Authority
ID_i, ID_j	Identities of SD_i, UC_j
RTS_i, RTS_j	Registration Time-stamps of SD_i, UC_j
$p, Z_p, E_p(\alpha, \beta)$	large prime, finite field over p, Elliptic Curve
$G, k.G$	A point over $E_p(\alpha, \beta)$, scalar multiplication
$x, Q = x.G$	TA's key pair
P_{ri}, P_{rj}	Private keys of SD_i, UC_j
P_{ui}, P_{uj}	Public keys of SD_i, UC_j
C_k	certificate of k^{th} entity
$\mathcal{A}, \Delta T$	Attacker, delay tolerance
T_1, T_2, T_3	Time stamps
$\|\|, \oplus$	concatenation and xor functions
$\stackrel{?}{=}, h(.)$	Equality Check, Hash function

A. SYSTEM SETUP

To accomplish the setting up of the system, the trusted authority $\mathcal{TA}$ selects an elliptic curve $E_p(\alpha, \beta)$ over finite field Z_p along with a base point $G \in E_p(\alpha, \beta)$ of large order n s.t. $n.G = O$ (a point at infinity). The p is selected as a very large prime number satisfying $4\alpha^3 - 27\beta^2 \neq 0 mod\ p$. $\mathcal{TA}$ then selects x as private and $Q = xG$. as its' own public key.$\mathcal{TA}$ also selects a secure one way function $h(.)$ and finally, publishes $\{E_p(\alpha, \beta), G, Q, h(.)\}$.

B. UC REGISTRATION

For registering each $UC_j : \{j = 1, 2..n\}$, $\mathcal{TA}$ selects unique ID_j, private key p_{rj} and computes public key $P_{uj} = p_{rj}G$. $\mathcal{TA}$ finally, stores $\{ID_j, p_{rj}, P_{uj}, G, Q, ID_i : \{i = 1, 2, ...m\}, RID_i : \{i = 1, 2, ...m\}, h(.), E_p(\alpha, \beta)\}$ in the memory of UC_j.

C. SG DEVICE REGISTRATION

For registering each SG device $SD_i : \{i = 1, 2..m\}$, $\mathcal{TA}$ selects unique ID_i and computes $RID_i = h(ID_i||x)$. $\mathcal{TA}$ then computes certificate parameter $C_i = x + H(ID_i||Q)x$. $\mathcal{TA}$ finally, stores $\{RID_i, C_i, E_p(\alpha, \beta), G, Q, P_{uj} : \{j = 1, 2, ...n\}, h(.)\}$ in the memory of SD_i.

D. AUTHENTICATION

In Proposed $DRMAS$ scheme, SD_i initiates authentication phase to furnish a secure session key with UC_j. The steps as illustrated in Fig. 2 and briefed below are performed between SD_i and UC_j to complete this phase:

PDR 1: $\boldsymbol{SD_i \rightarrow UC_j}$: $\boldsymbol{\{m_1\}}$

SD_i selects $r_i \in Z_p^*$ randomly and generates current timestamp T_1. SD_i then compute $U_i = r_iG$ and $W_i = r_iP_{uj} = r_ip_{rj}G$ along with the timestamp based random certificate $C_s = r_iT_1 + C_i = r_iT_1 + x + H(ID_i||Q)x$. Finally, SD_i computes $H_i = h(U_i||W_i||C_s||RID_i||T_1)$, dynamic pseudo identity $\overline{ID}_i = ID_i \oplus W_i$ and sends $m_1 = \{\overline{ID}_i, H_i, U_i, C_s, T_1\}$ to UC_j.

PDR 2: $\boldsymbol{UC_j \rightarrow SD_i}$: $\boldsymbol{\{m_2\}}$

UC_j after receiving m_1, first verifies message freshness by checking $|T_1 - T_1^*| \leq 0$, and upon success UC_j computes Compute $W_i^{'} = p_{rj}U_i$ and $ID_i = \overline{ID}_i \oplus W_i^{'}$.

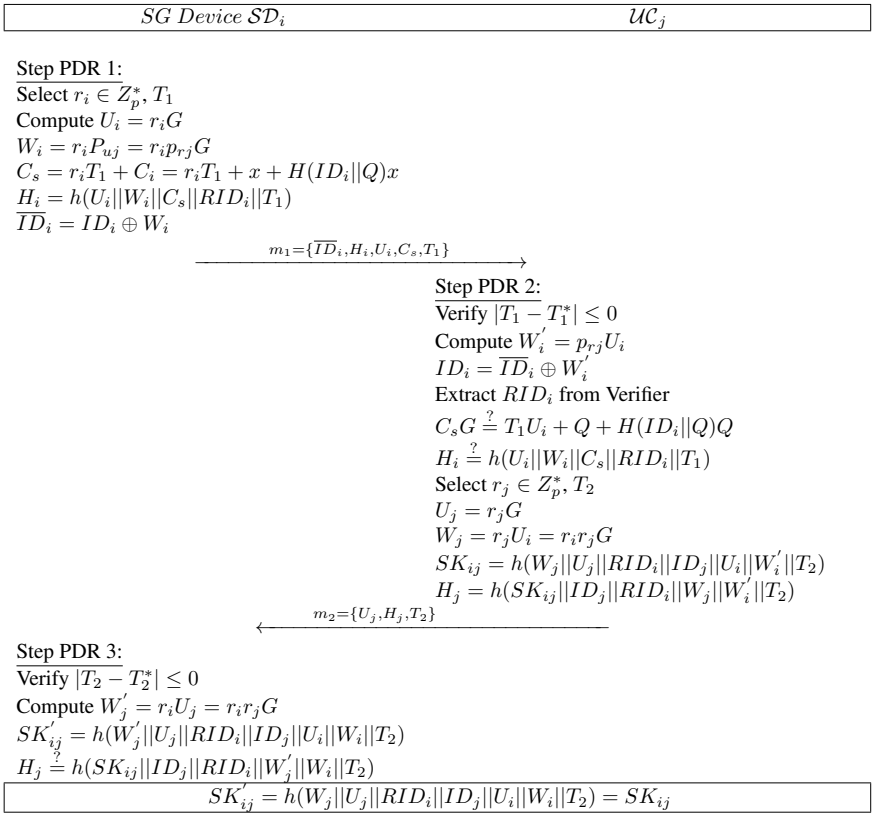

Figure 2: Proposed $DRMAS$

UC_j checks existence of ID_i in verifier database and on succes extracts RID_i. UC_j then checks the genuineness of random certificate as $C_s G \stackrel{?}{=} T_1 U_i + Q + H(ID_i||Q)Q$ and $H_i \stackrel{?}{=} h(U_i||W_i||C_s||RID_i||T_1)$, aborts the session, if any of these is invalid. Otherwise, UC_j select $r_j \in Z_p^*$, T_2 and computes $U_j = r_j G$, $W_j = r_j U_i = r_i r_j G$, and session key $SK_{ij} = h(W_j||U_j||RID_i||ID_j||U_i||W_i^{'}||T_2))$ along with $H_j = h(SK_{ij}||ID_j||RID_i||W_j||W_i^{'}||T_2)$. UC_j completes this step by sending $m_2 = \{U_j, H_j, T_2\}$ to SD_i.

PDR 3: UC_j after receiving m_2, first verifies message freshness by checking $|T_3 - T_3^*| \leq 0$, and upon success UC_j computes $W_j^{'} = r_i U_j = r_i r_j G$, and session key $SK_{ij}^{'} = h(W_j^{'}||U_j||RID_i||ID_j||U_i||W_i||T_2)$. UC_j then compares $H_j \stackrel{?}{=} h(SK_{ij}||ID_j||RID_i||W_j^{'}||W_i||T_2)$, on success UC_j considers SD_i as legal and authenticated device.

E. SG DEVICE DYNAMIC ADDITION

The dynamic addition of a new device SD_i^{new} requires very similar procedure as of SG device registration. For dynamic addition of a device SD_i^{new} $\mathcal{TA}$ selects unique ID_i^{new} and computes $RID_i^{new} = h(ID_i^{new}||x)$. $\mathcal{TA}$ further computes certificate parameter $C_i = x + H(ID_i||Q)x$. $\mathcal{TA}$ then stores $\{RID_i, C_i, E_p(\alpha, \beta), G, Q, P_{uj} : \{j = 1, 2, ...n\}, h(.)\}$ in the memory of SD_i^{new} and deploys it in the system. $\mathcal{TA}$ finally, sends RID_i^{new} to each UC_j.

III. DISCUSSION ON FUNCTIONAL SECURITY

This section briefly discusses the functional security of the proposed scheme along with comparison of the security features extended by proposed and related schemes under the realistic adversarial model as mentioned in subsection I-B.

A. REPLAY ATTACK

An adversary A may eavesdrop the authentication request and reply messages, i.e., $m_1 = \{ID_i, H_i, U_i, C_s, T_1\}$ and $m_2 = \{U_j, H_j, T_2\}$ between SD_i and UC_j in mutual authentication phase. However, the involvement of timestamps T_1 and T_2 in respective authentication messages m_1 and m_2, refrains the adversary to store and initiate replay attack at some future time. In that case, the legal participants may check the timestamp of message and abort the session, thereafter. Hence, the contributed scheme is protected from replay attack.

B. STOLEN SG DEVICE ATTACK

An adversary may steal or physically compromise the SG device, since these devices are normally deployed in the proximity of home or nearby places. Then the former may

recover the critical contents of the SG device, such as $\{RID_i, C_i, Q, Pu_j : \{j = 1, 2, ...n\}, h(.)\}$ by using power analysis attacks [35]–[37]. Here, $RID_i = h(ID_i||x)$ and $C_i = x + H(ID_i||Q_x)$, $Q = xG$, and $Pu_j = Pr_j.G$. Using the RID_i and C_i parameters, it would be computationally hard for the adversary to recover the device identity ID_i without having access to UC_j's secret key x. It is worthy to note that RID_i is unique for different SG devices due to distinct identities ID_i for every SG device. Hence, despite accessing any stolen SG device contents, A could not compute the session key as established between UC and a non-compromised SG device. Therefore, our scheme is resistant to stolen SG device attack.

C. SG DEVICE IMPERSONATION ATTACK

An adversary may attempt to launch a SG device (SD_i)-impersonation attack by submitting an authentication request message towards UC_j. For constructing this message, it may generate a random integer $r_i^A \in Z_p^*$ and a fresh timestamp T_1, and then compute $U_i^A = r_i^A.G$ and $W_i^A = r_i^A.Pu_j$, where Pu_j is the public key of UC_i. However, to construction of a valid authentication request $m_1 = \{\overline{ID_i}, H_i, U_i^A, C_s, T_1\}$ it requires to compute C_s, H_i and $\overline{ID_i}$, i.e. $C_s = r_i^A T_1 + C_i$, $H_i = h(U_i||W_i^A||C_s||RID_i||T_1)$ and $\overline{ID_i} = ID_i \oplus W_i^A$, which is not possible until it gains access to some crucial parameters such as RID_i , C_i, and ID_i. This depicts that the proposed scheme is protected from SG device impersonation attack.

D. MAN-IN-THE-MIDDLE ATTACK

An adversary may attempt to maneuver the intercepted messages by introducing suitable modifications in the message contents to impersonate the legal parties on both ends. In our scheme, the adversary, upon receiving the authentication request $m_1 = \{\overline{ID_i}, H_i, U_i, C_s, T_1\}$ from SD_i, may generate a random integer $r_a \in Z_p^*$ and a fresh timestamp T_a, and then compute $U_a = r_a.G$. However, for constructing a legal authentication request $m_1 = \{\overline{ID_i}, H_i, U_a, C_s', T_a\}$ it requires to compute a valid parameters, i.e., C_s, H_i and $\overline{ID_i}$, i.e. $C_s' = r_a T_1 + C_i$, $H_i = h(U_a||W_i'||C_s'||RID_i||T_1)$ and $\overline{ID_i} = ID_i \oplus W_i'$, which is computationally not feasible until the secret credentials RID_i , C_i, and ID_i are accessed. Likewise, A may also attempt to modify the acknowledgment authentication message $m2 = \{U_j, H_j, T_2\}$ according to fresh timestamp T_2. However, the involvement of secret credential RID_i in the calculation of H_j refrains the adversary to construct a fake acknowledgment message. Hence, the contributed scheme is immune to man-in-the-middle attack.

E. UC IMPERSONATION ATTACK

To impersonate as UC_j, the adversary needs to construct a valid acknowledgment authentication message $m_2 = \{U_j, H_j, T_2\}$ with current timestamp T_2, where $U_j^A = r_j^A G$, $W_j^A = r_j^A.U_i$, $SK_{ij} = h(W_j^A||U_j^A||RID_i||U_i||W_i'||T_2)$, and $H_j = h(SK_{ij}||RID_i||W_j^A||W_i'||T_2)$. The adversary may generate a random number r_j^A and fresh timestamp T_2, then it may further compute $U_j^A = r_j^A G$, $W_j^A = r_j^A.U_i$. Nevertheless, the use of secret credential RID_i debars the adversary to compute SK_{ij} and in return H_j , which nullifies the chances of the adversary's constructing a valid $m_2 = \{U_j, H_j, T_2\}$ message. Thus, our scheme is protected from UC_j impersonation attack.

F. SESSION KEY SECURITY

In authentication phase of proposed model, the session key SK_{ij} is established with secure mutual communication between SD_i and UC_j as $SK_{ij} = h(W_j||U_j||RID_i||U_i||W_i||T_2)$, where $W_j = r_j U_i = r_i r_j G$, $U_j = r_j G$, RID_i, U_i and $W_i = pr_j U_i$. It is evident that the strength of computed session key is based upon two constituent factors: 1) temporary secrets r_i and r_j , and 2) long term secret parameters such as pr_j and RID_i. It is worthy to note that in our protocol, the identities such as ID_i and ID_j, and master secret key x of TA are only known to the TA. We may consider the following two cases regarding the robustness of session key.

Case 1. In case, the temporary session variables r_i and r_j are revealed to the adversary, the session key SK_{ij} is hard to compute for the adversary due to lacking long term secrets RID_i and pr_j.

Case 2. Likewise, in case the long term secret parameters such as RID_i and pr_j are revealed to the adversary, the SK_{ij} still remains hard to compute for the adversary due to lacking temporary session variables r_i and r_j. While, these variables r_i and r_j are protected in U_i and U_j, respectively, since it is computational hard to recover r_i and r_j from U_i and U_j due to non-breakable security feature of elliptic curve discrete logarithm problem (ECDLP).

If we take the assumptions of both cases combined, i.e. the temporary session variables (r_i and r_j) as well as long term secret parameters (RID_i and pr_j) are revealed to the adversary, only then the later would be able to compute the legitimate session key. Moreover, if the current session key SK_{ij} as established between the participants, is revealed to the adversary, then the later may not be able to compute the session keys of other sessions between the same parties, since every authentication session bears the unique temporary session variables. Hence, it would be unlikely for the adversary to be able to compute the previous or future session keys from the current revealed session key. In this manner our scheme provides perfect forward as well as backward secrecy to the legal participants.

G. ANONYMITY AND UNTRACEABILITY

In proposed scheme, an adversary may eavesdrop the communication messages $m_1 = \{\overline{ID_i}, H_i, U_i, C_s, T_1\}$ and $m_2 = \{U_j, H_j, T_2\}$ over an insecure channel. However, A might not be able to derive the smart device's identity ID_i

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2996093, IEEE Access

from the exchanged messages, which is one of the crucial requirements in the security of smart grid system for the customer. Moreover, A may also be unable to distinguish the message contents of a session from other sessions either established between the same or different participants. This property ensures that a smart device may not be traced by the adversary. This is because of the fact, the parameters in m_1 and m_2 messages involve either current timestamps (T_1 and T_2) or fresh nonces (r_i and r_j), respectively.

IV. FORMAL SECURITY ANALYSIS

Over the past few years, the security analysis under formal methods has got popularity and is being considered as the main strong proofing method. The popular Real-Or-Random (ROR) [26], [27] model is adopted here to prove the security of propose $DRMAS$. In $DRMAS$, there are three entities of environment, $\mathcal{TA}$, SG device $\mathcal{SD}_i$ and $\mathcal{UC}_j$. In ROR model the following ingredients are described below.

Participants. Let $I^x_{\mathcal{TA}}$, $I^y_{\mathcal{SD}_i}$ and $I^z_{\mathcal{UC}_j}$ be the instances x, y and z of $\mathcal{TA}$, $\mathcal{SD}_i$ and $\mathcal{UC}_j$, which is called oracles.

Accepted State. I^x being an instance is considered as accepted, the accept state is achieved after last message is received during protocol execution. The (sid) of I^x is termed as session identifier and is the ordered concatenation of all communication messages (received or sent) for a current session.

Partnering. Let I^{x_1} and I^{x_2} are known to be partnered, once the following three states are occurred simultaneously.

1) I^{x_1} and I^{x_2} are in accept state.

2) I^{x_1} and I^{x_2} are mutual authenticate and share identical (sid) with each other.

3) Both I^{x_1} and I^{x_2} are mutual partners.

Freshness. Both instances $I^y_{\mathcal{SD}_i}$ and $I^z_{\mathcal{UC}_j}$ are fresh, if SK_{ij} (session key) between $\mathcal{SD}_i$ and $\mathcal{UC}_j$ is not exposed to an attacker $\mathcal{A}$ using the query $\mathcal{R}(I^x)$ defined below.

Adversary. Following ROR model, $\mathcal{A}$ is supposed to fully control all communications and can also use the following defined queries to eavesdrop, modify, manufacture and inject messages [27]:

1) Execute(I^x, I^y): It is simulated as eavesdropping attack in which after execution of such a query, $\mathcal{A}$ can collect the transmitted messages.

2) Reveal(I^x): The current session key SK_{ij} generated by Π^x (and its partner) is revealed to $\mathcal{A}$ on execution of this query.

3) Send(I^x, msg): By executing this, $\mathcal{A}$ being an active adversary can send msg to I^x and can also receive the response.

4) Test(I^x, msg): It represents the session key's (SK_{ij}) semantic security, under RoR's indistinguishability.

$\mathcal{A}$ gets SK_{ij} from I^x, on the successful running of an experiment involving an unbiased coin β flicked before start of the game, the output is known to $\mathcal{A}$ only, if SK_{ij} is fresh and $\beta = 1$. Otherwise, $\mathcal{A}$ gets null value.

Semantic security of the session key.

According to the requirements of ROR model, adversary needs to distinguish between an instance's original session key SK_{ij} and a random key. $\mathcal{A}$ can allow several test queries to either $I^y_{SD_i}$ or $I^z_{UC_j}$. Before the game finished, adversary returns the guessed bit b$'$ and $\mathcal{A}$ can win the game if condition b$'$=b is matched. If SUC represents an event that adversary can win the game, the advantage adv_P^{AKA} of adversary in breaking the semantic security of the session key SK_{ij} in our authenticated key-agreement AKA protocol, say P is represented and defined by $Adv_P^{AKA} = |2.Pr[SUC] - 1|.P$ is said to be secure, $Adv_P^{AKA} \leq \psi$, where $\psi > 0$ is a small real number.

Random Oracle. The legal entities as well $\mathcal{A}$ can access $h(.)$, which is simulated as random oracle say HSH [27]. Following definitions are referred to prove the Theorem 1:

Definition 1. Let a deterministic function $h : \{0,1\}^* \rightarrow \{0,1\}^u$ is collision resistant, which takes input $v \in \{0,1\}^*$ with arbitrary length and produces $h(v) \in \{0,1\}$ of fixed length [38]. The advantage of $\mathcal{A}$ to find collusion is represented and defined by $Adv_{\mathcal{A}}^{HSH}(x) = Pr[(b_1, b_2) \leftarrow R\mathcal{A} : b_1 \neq b_2$ and $h(b_1) = h(b_2)]$; here, $Pr[\mathcal{E}]$ $(b_1, b_2) \leftarrow R\,\mathcal{A}$ represents the probability of the event $\mathcal{E}$ represent. The the pair (b_1, b_2) is selected randomly by $\mathcal{A}$.The adversary $\mathcal{A}$'s advantage to made random choices within limited time bound tim is considered. The attack on collision resistance of $h(.)$ by an ψ, tim-adversary is at most $Adv_{\mathcal{A}}^{HSH}(tim) \leq \psi$.

Definition 2. Let $G \in E_p(\alpha, \beta)$ is a point and given a quadruple (G, r_iG, r_jG, wG), decide whether $w = r_ir_j$ or not is termed as the $ECDDHP$.

Theorem 1. Consider a polynomial time (tim) bound adversary $\mathcal{A}$ against the introduced $DRMAS$ under ROR model If q_{hsh} and $|hsh|$ denote maximum numeral and range space of HSH queries and $adv^{ECDDHP}(x)$ expresses $\mathcal{A}$'s advantage to break $ECDDHP$. The advangate carried by $\mathcal{A}$ to break semantic security of SK_{ij} in $DRMAS$ is $adv_{DRMAS}^{AKA} \leq \frac{q_h^2}{|hash|} + 2adv^{ECDDHP}(x)$.

The number of $HASH$ queries, the range space of hash function $h(.)$ and the advantage of $\mathcal{A}$ in breaking the semantic security of the session key SK_{ij} in $\mathcal{P}$ is $adv_{\mathcal{P}}^{AKA} \leq \frac{q_h^2}{|hash|} + 2adv^{ECDDHP}(x)$.

$Proof$. The proof resembles to the same presented in [24] and [27]. The in-sequences games $G_i : \{i = 1, 2, 3, 4\}$ are demarcated for the purpose of security analysis. Let SUC_i be an event wherein $\mathcal{A}$ can correctly guess random bit β in G_i. Details are as follows:

$Game_1$ (G_1): G_1 simulates the actual attack launched by $\mathcal{A}$ against $DRMAS$ under ROR model. Therefore, we have:

$$Adv_{DRMAS}^{AKA} = |2.Pr[G_1] - 1|. \quad (1)$$

$Game_2$ (G_2): simulates actual eavesdropping launched by $\mathcal{A}$. The $\mathcal{A}$ can perform a query to $Execute(I^x, I^y)$ oracle. To complete G_2, $\mathcal{A}$ queries the $test$ oracle and result of $test$ can confirm the correctness of SK_{ij}. Note that SK_{ij} is calculated by both $\mathcal{SD}_i$ and $\mathcal{UC}_j$ as $SK_{ij} = h(W_j||U_j||RID_i||ID_j||U_i||W_i^{'}||T_2)$. To calculate session key SK_{ij} requires pair $\{y, z\}$ (the ephemeral secrets), and

$W_i^{'}$, RID_i and W_j (the long-term secrets). Without this knowledge, deriving the session key SK_{ij} is an impossible problem for $\mathcal{A}$. Hence, winning chance of G_2 has not benefited by eavesdropping. Therefore, we have:

$$Pr[SUC_1] = Pr[SUC_2]. \tag{2}$$

$Game_3$ (G_3): G_3 models the real and active attack with additional $Send(I^x, msg)$ and hsh query simulations. $\mathcal{A}$ intends that a participant may accept the forged message. $\mathcal{A}$ is considered as capable enough to make different HO queries for examining the collision existence in hash. However, in login and authentication phase, all the messages $\{\overline{ID}_i, H_i, U_i, C_s, T_1\}$, $m_2 = \{U_j, H_j, T_2\}$ and $SK_{ij}^{'}$ contain respective participant's identity, timestamps and random number. Hence, querying $Send$ oracle do not return collision to $\mathcal{A}$. The results of birthday paradox gives:

$$Pr[SUC_2] - Pr[SUC_3] \leq q_{hsh}^2/(2|hash|). \tag{3}$$

$Game_4$ (G_4): G_3 is transformed into G_4, where G_4 is the last game. it is modeled further as an active attack. As illustrated in G_2, To calculate session key SK_{ij} requires the ephemeral secrets y and z, and the long-term secrets $W_i^{'}$, RID_i and W_j. Having the eavesdropping $U_i = r_iG$ and $U_j = r_jG$, adversary requires to differentiate between r_ir_jG and a random number, which reduces to the $ECDDHP$ problem. Hence, it is clear that the computation of SK_{ij} depends on the $ECDDHP$ problem. Its' result follow that

$$Pr[SUC_3] - Pr[SUC_4] \leq Adv_x^{ECDDHP}(t). \tag{4}$$

In G_4, all the random oracles are simulated. $\mathcal{A}$ is only left to guess β for winning the game after querying the $Test$ oracle. Therefore, we have:

$$Pr[SUC_4] = \frac{1}{2}. \tag{5}$$

From Equations 1 and 2, we have

$$\frac{1}{2}.Adv_{DRMAS}^{AKA} = |Pr[SUC_1] = \frac{1}{2}| = |Pr[SUC_2] - \frac{1}{2}|. \tag{6}$$

The triangular inequality and equations 3, 4, 5 give the following:

$$\begin{aligned} |Pr[SUC_2] - \frac{1}{2}| &= |Pr[SUC_2] - Pr[SUC_4]| \\ &\leq |Pr[SUC_2] - Pr[SUC_3]| \\ &\quad + |Pr[SUC_3] - Pr[SUC_4]| \\ &\leq \frac{q_{hsh}^2}{2|hsh|} + Adv_x^{ECDDHP}. \end{aligned} \tag{7}$$

From equations 6 and 7 finally, we have

$$Adv_{\mathcal{P}}^{AKA} \leq \frac{q_{hsh}^2}{2|hash|} + 2Adv_x^{ECDDHP}. \tag{8}$$

Table 2: Computational Cost Analysis

Scheme	Total	Running time
[20]	$4T_{epm} + 2T_{ex} + 3T_{pb} + 7T_h$	$\approx 34.0531\ ms$
[22]	$2T_{epm} + 20T_h$	$\approx 4.498\ ms$
[23]	$5T_{epm} + 2T_{en} + 18T_h$	$\approx 11.1806\ ms$
[11]	$7T_{epm} + 2T_{ex} + 2T_{pb} + 10T_h$	$\approx 34.9273\ ms$
[12]	$5T_{epm} + 2T_{ex} + 2T_{pb} + 12T_h$	$\approx 30.4796\ ms$
[24]	$4T_{epm} + 12T_h$	$\approx 8.9316\ ms$
$DRMAS$	$9T_{epm} + 2T_{epa} + 8T_h$	$\approx 20.11\ ms$

V. COMPARATIVE SECURITY AND PERFORMANCE ANALYSIS

Following subsections present the computation and communication efficiencies comparison of $DRMAS$ with scheme proposed in [11], [12], [20], [22]–[24].

A. COMPUTATION COST

For computation cost analysis, some notations are introduced. $T_{epm}, T_{epa}, T_h, T_{pb}, T_{ex}$ and T_{en} represent ECC point multiplication, addition, hash, bilinear operation, exponentiation and symmetric encryption/decryption operations. For computation cost analysis, the experiment conducted on a PC with DUAL CPU $E2200$, 2.20 GHz processor, 2048 MB of RAM implemented over Ubuntu OS with PBC Library by Kilinc and Yanik [39] is considered. As per [39], the running time of $T_{bp} = 5.811$ ms, $T_{ex} = 3.85$ ms, $T_{epm} = 2.226$ ms, $T_{epa} = 0.0288$ ms, $T_{en} = 0.0046$ ms and $T_h = 0.0023$. $DRMAS$ has quite low computation cost as compared with [11], [12], [20] and has incurred extra computation time as compared with [22]–[24]. $DRMAS$ complete a complete cycle of authentication in just $\approx 20.11\ ms$.

B. COMMUNICATION COST

For communication cost comparisons, some common assumptions regarding the sizes of different transmitted parameters are considered as: identity size is fixed at 160 bits, $SHA-1$ is selected with 160 bits digest size, 160 bits long random number generation is selected; while the size of timestamp is taken as 32 bits long and the ECC points with 320 bits length are considered to provide same security as of RSA 1024 bits. Proposed $DRMAS$ completes authentication through transmission of two messages: 1) $m_1 = \{\overline{ID}_i, H_i, U_i, C_s, T_1\}$ from SD_i to UC_j, and $m_2 = \{U_j, H_j, T_2\}$ from UC_j to SD_i. The length of m_1 is $\{160+160+160+320+32\} = 832$ bits and the size of m_2 is $\{320+160+32\} = 512$. Therefore, total communication cost of $DRMAS$ is 1344 bits, whereas, communication cost of scheme proposed by Kumar et al. [24] is 1376 bits. The communication costs of [11], [12], [20], [22] is 1408, 1920, 1536 respectively; whereas, the communication cost of scheme [23] is 2080 bits. Table 3 shows that $DRMAS$ has lowest communication cost as compared with competitive scheme. Moreover, proposed $DRMAS$ completes whole authentication process in just 2 messages, while all other schemes [11], [12], [20], [22]–[24] complete the same in 3 messages.

Table 3: Communication Cost Analysis

Scheme	Messages Exchanged	Bits Exchanged
Mahmood et al. [20]	3	1340
Challa et al. [22]	3	1536
Chaudhry et al. [23]	3	2080
Odelu et al. [11]	3	1920
Tsai and Lu [12]	3	1408
Kumar et al. [24]	3	1376
$DRMAS$	2	1344

C. SECURITY FEATURES

The security features comparisons of the proposed $DRMAS$ and competing schemes proposed in [11], [12], [20], [22]–[24] is depicted in Table 4 under the threat model (DY model) solicited in subsection I-B. The Table 4 mentions that only proposed $DRMAS$ resists known attacks and provides known security features under DY threat model. Due to the non-verification of initial message from SD_i, UC_j, the scheme proposed by Kumar et al. can become prey of an attacker bombardment of randomly generated illegal messages, which can eventually cause denial of services attack. As proved in [23], the scheme proposed in [22] suffers from incorrectness and no initial verification issues as of Kumar et al.'s scheme [24], the scheme proposed in [22] also lacks direct device to device (D2D) communication and requires intermediate party, which can become bottleneck for efficiency. Nevertheless, the scheme proposed in [23] also lacks direct D2D communication and scheme proposed in [20] lacks initial verification of request message. The scheme proposed in [12] lacks the procedure to add post-deployment dynamic addition of devices; whereas, citing [12], the scheme proposed in [11] is weak against privileged insider and does not provide anonymity and session key security. The scheme proposed in [11] also lacks the initial request message verification. Therefore, proposed scheme is best suitable for deployment in smart grid environments.

Table 4: Security Features

	Ours	[24]	[11]	[12]	[20]	[22]	[23]
$\mathcal{S}_{f1}$	✓	✗	✓	✓	✓	✗	✓
$\mathcal{S}_{f2}$	✓	✓	✓	✓	✓	✓	✓
$\mathcal{S}_{f3}$	✓	✓	✓	✓	✓	✓	✓
$\mathcal{S}_{f4}$	✓	✓	✓	✓	✓	✗	✗
$\mathcal{S}_{f5}$	✓	✓	✓	✗	✓	✓	✓
$\mathcal{S}_{f6}$	✓	✓	✓	✓	✓	✓	✓
$\mathcal{S}_{f7}$	✓	✓	✓	✗	✓	✓	✓
$\mathcal{S}_{f8}$	✓	✓	✗	✓	✓	✓	✓
$\mathcal{S}_{f9}$	✓	✓	✓	✗	✓	✓	✓
$\mathcal{S}_{f10}$	✓	✗	✓	✗	✗	✗	✓
$\mathcal{S}_{f11}$	✓	✓	✓	✓	✓	✓	✓

Note: $\mathcal{S}_{f1}$: Correctness; $\mathcal{S}_{f2}$: Resist Impersonation; $\mathcal{S}_{f3}$: Resists Replay; $\mathcal{S}_{f4}$:D2D Direct Communication ; $\mathcal{S}_{f5}$: Resists Privileged Insider; $\mathcal{S}_{f6}$: man in the middle $\mathcal{S}_{f7}$: Session key Security; $\mathcal{S}_{f8}$: Dynamic node addition; $\mathcal{S}_{f9}$: Device anonymity; $\mathcal{S}_{f10}$: Initial Device Verification; $\mathcal{R}_{s11}$:Perfect Forward Secrecy ✓: Secure or extends; ✗:Insecure against or not provides

VI. CONCLUSION

In smart grid (SG), the demand response is maintained dynamically through exchanging data between entities. However, this data transfer requires an efficient and secure authentication scheme to avoid any modification over open channel. To secure demand response management, we proposed an authentication scheme (DRMAS) using ECC based certificate. To prove the robustness, DRMAS is analyzed formally along with a discussion on security requirements to confirm formally and informally the robustness of the proposed scheme. DRMAS performs better in communication cost and achieves authentication in just 2 message exchanges. It is also shown that DRMAS provides best tradeoff between security and performance.

References

[1] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," IEEE Transactions on Industrial Informatics, vol. 7, no. 4, pp. 529–539, 2011.

[2] A. Metke and R. Ekl, "Security technology for smart grid networks," IEEE Transections on Smart Grid, vol. 1, no. 1, pp. 99–107, 2010.

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

[4] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, "Smart contract privacy protection using ai in cyber-physical systems: Tools, techniques and challenges," IEEE Access, vol. 8, pp. 24746–24772, 2020.

[5] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles," IEEE Access, vol. 8, pp. 43711–43724, 2020.

[6] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M. A. Latif, F. Al-Turjman, and L. Mostarda, "Cyber security threats detection in internet of things using deep learning approach," IEEE Access, vol. 7, pp. 124379–124389, 2019.

[7] S. H. Islam, "A provably secure id-based mutual authentication and key agreement scheme for mobile multi-server environment without esl attack," Wireless Personal Communications, vol. 79, no. 3, pp. 1975–1991, 2014.

[8] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. Najmus Saqib, "Security and key management in iot-based wireless sensor networks: An authentication protocol using symmetric key," International Journal of Communication Systems, vol. 32, no. 16, p. e4139, 2019.

[9] A. Irshad, S. A. Chaudhry, M. Shafiq, M. Usman, M. Asif, and A. Ghani, "A provable and secure mobile user authentication scheme for mobile cloud computing services," International Journal of Communication Systems, vol. 32, no. 14, p. e3980, 2019.

[10] S. H. Islam and G. Biswas, "A more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," Journal of Systems and Software, vol. 84, no. 11, pp. 1892–1898, 2011.

[11] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," IEEE Transactions on Smart Grid, 2016.

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

[13] I. Doh, J. Lim, and K. Chae, "Secure authentication for structured smart grid system," in International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-15), (Fukuoka, Japan), pp. 200–204, 2015.

[14] N. Saxena, B. J. Choi, and R. Lu, "Authentication and authorization scheme for various user roles and devices in smart grid," IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp. 907–921, 2016.

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

[16] A. M. ali, 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 Transactions on Smart Grid, vol. 9, no. 4, pp. 2834–2842, 2018.

[17] K. Mahmood, J. Arshad, S. A. Chaudhry, and S. Kumari, "An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure," International Journal of Communication Systems, vol. 32, p. 16, 2019.

[18] 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 Generation Computer Systems, vol. 81, pp. 557–565, 2018.

[19] 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 Generation Computer Systems, vol. 84, pp. 47–57, 2018.

[20] K. Mahmood, X. Li, S. A. Chaudhry, H. Naqvi, S. Kumari, A. K. Sangaiah, and J. J. Rodrigues, "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," Future Generation Computer Systems, vol. 88, pp. 491–500, 2018.

[21] X.-C. Liang, T.-Y. Wu, Y.-Q. Lee, C.-M. Chen, and J.-H. Yeh, "Cryptanalysis of a pairing-based anonymous key agreement scheme for smart grid," in Advances in Intelligent Information Hiding and Multimedia Signal Processing, pp. 125–131, Springer, 2020.

[22] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, E. Yoon, and A. V. Vasilakos, Design and analysis of authenticated key agreement scheme in cloud-assisted cyber-physical systems. Future Generation Computer Systems, 2018.

[23] S. A. Chaudhry, T. Shon, F. Al-Turjman, and M. H. Alsharif, "Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems," Computer Communications, vol. 153, pp. 527 – 537, 2020.

[24] 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," in IEEE Transactions on Industrial Informatics, vol. 15, pp. 6572–6582, December 2019.

[25] 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), Taylor and Francis, CRC, 2020. Inpress.

[26] M. Abdalla, P. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in th International Workshop on Theory and Practice in Public Key Cryptography (PKC-05), Lecture Notes in Computer Science (LNCS), vol. 3386, Switzerland pp. 65-84, vol. 8, 2005.

[27] C. C. Chang and A. P. S. H. D. Le, "Efficient and flexible authentication scheme for ad hoc wireless sensor networks," IEEE Transactions on Wireless Communications, vol. 15, no. 1, pp. 357–366, 2016.

[28] D. He, N. Kumar, H. Wang, L. Wang, K.-K. R. Choo, and A. Vinel, "A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 633–645, 2016.

[29] Z. Ali, A. Ghani, I. Khan, S. A. Chaudhry, S. H. Islam, and D. Giri, "A robust authentication and access control protocol for securing wireless healthcare sensor networks," Journal of Information Security and Applications, vol. 52, p. 102502, 2020.

[30] M. N. Aman, M. H. Basheer, and B. Sikdar, "Data provenance for iot with light weight authentication and privacy preservation," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10441–10457, 2019.

[31] C. Chen, B. Xiang, Y. Liu, and K. Wang, "A secure authentication protocol for internet of vehicles," IEEE Access, vol. 7, pp. 12047–12057, 2019.

[32] S. Hussain and S. A. Chaudhry, "Comments on "biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment"," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10936–10940, 2019.

[33] K. Mansoor, A. Ghani, S. A. Chaudhry, S. Shamshirband, S. A. K. Ghayyur, and A. Mosavi, "Securing iot-based rfid systems: A robust authentication protocol using symmetric cryptography," Sensors, vol. 19, no. 21, p. 4752, 2019.

[34] M. N. Aman, M. H. Basheer, and B. Sikdar, "Two-factor authentication for iot with location information," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3335–3351, 2019.

[35] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," IEEE Transactions on Computers, vol. 51, no. 5, pp. 541–552, 2002.

[36] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in Advances in Cryptology CRYPTO 99, pp. 388–397, Springer, 1999.

[37] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. Shalmani, "On the power of power analysis in the real world: A complete break of the keeloq code hopping scheme," in Advances in Cryptology, pp. 203–220, Springer Berlin Heidelberg vol. 5157, 2008.

[38] P. Sarkar, A. Simple, and G. Construction, "of authenticated encryption with associated data," ACM Transactions on Information and System Security, vol. 13, no. 4, pp. 1–16, 2010.

[39] H. H. Kilinc and A. T. Yanik, "survey of sip authentication and key agreement schemes," IEEE Commun Surv Tutorials, vol. 16, no. 2, pp. 1005–1023, 2014.