Correcting Design Flaws: An Improved and Cloud Assisted Key agreement scheme in Cyber Physical Systems

Shehzad Ashraf Chaudhry[1], Taeshik Shon[2], Fadi Al-Turjman[3,4], Mohammed H. Alsharif [5]

[1] *Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey*

[2] *Department of Cyber Security, Ajou University San 5, Woncheon-Dong, Yeongtong-Gu, Suwon 443-749, Korea*

[3] *Artificial Intelligence dept., Near East University, Nicosia, Mersin 10, Turkey*

[4] *Research Center for AI and IoT, Near East University, Nicosia, Mersin 10, Turkey*

[5] *Department of Electrical Engineering, College of Electronics and Information Engineering, Sejong University, 209 Neungdong-ro, Gwangjin-gu, Seoul 05006, Korea*

Note: This is accepted manuscript version published in Elsevier- Computer Communication 153 (2020) 527–537, The final Version is available at https://doi.org/10.1016/j.comcom.2020.02.025

Abstract

The on demand availability of resources in Cyber physical system (CPS) has emerged as a viable service providing platform to improve the resource usability and reducing the infrastructure costs. Nevertheless, the development recompenses can only be realized after avoiding security and privacy issues. A secure and reliable CPS can offer improved efficiency, usability and reliability along with autonomy. To secure such systems, in 2018 Challa et al. (**FGCS, DOI: 10.1016/j.future.2018.04.019, 2018**) proposed a security system to extend an authenticated key agreement between a user and a cloud server via trusted authority; as an application, they also customized their system to work with autonomous smart meter and cloud sever. Challa et al. then claimed the security of their proposed scheme through formal, informal and automated validations. However, this paper unveils the weaknesses of their scheme and shows that their scheme cannot facilitate in forming a session key between the user/smart meter and the cloud server. Precisely, in the presence of more than one registered users/smart meters, the latter in their scheme may never receive a response message because of a critical design error. Moreover, their scheme lacks the untraceable anonymity and the lack of request verification on cloud server side may also lead to replay and/or denial of services attack. The article then introduces an improved and secure authentication system free of correctness issues, to facilitate a key agreement between user and cloud server via trusted authority. As an application, the proposed system also works for smart meter and cloud server to reach a key agreement. Based on the hardness assumption of Elliptic Curve Decisional Diffi-Hellman Problem (ECDDHP), the formal Random oracle model proves the security of the proposed scheme. Moreover, the robustness of the scheme is explained through informal analysis. The proposed system while providing all known security features has slightly increased the computation and communication costs as compared with the scheme of Challa et al. The proposed scheme completes a cycle of authentication by exchanging 2080 *bits* in just 13.4066 *ms*.

Keywords: Cyber Physical System, Authentication, Anonymity, Elliptic Curve Cryptography, Security, Smart Meter, Authenticated Key Agreement, Incorrectness, Random Oracle Model

1. Introduction

The needs of modern society have been increasingly relying on variants of cyber-physical systems (CPS) and internet of things based technologies. The wide emergence of CPS and IoT-based systems has made possible the design and development of sophisticated CPS applications which collect and communicate a tremendous amount of real-time data towards servers. The CPS system is a networked system encompassing cyber (communication and computing) as well as physical components (actuators and sensors). The capability of computing and communication is increasingly embedded into the entities and objects of physical environment. Alternatively, the CPS systems have bridged the cyber world of computing and communication with the physical world. The CPS has not only transformed the physical world around us but also the ways of human interaction with the physical objects, since CPS systems have become very integrated in our environment, i.e., from nano-world to large scale wide area systems. It has found extensive applications in our environment such as medical devices and systems, transportation and intelligent highways, aerospace and defense systems, robotic systems and factory automation, construction, hazardous environment and control, smart devices with internet of things, power and smart girds, etc. etc. However, as much as this integration intensifies, the significance of security for these systems also increases [6] and to implement CPS tech-

Citation Information: S. A. Chaudhry, T. Shon, F. Al-Turjman, M. H. Alsharif, Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems, Computer Communications, Volume 153, 2020, Pages 527-537, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2020.02.025.

nologies, the requirement to improve the system stability, computational cost efficiency, flexibility and fault tolerance must be fulfilled [1]. One of the promising paradigms, cloud computing nearly fulfills all of these requisites. Other than those stated requirements, the cloud computing provides scalability, interactivity expansion as well as reduces the complexity of the system. Also the cloud computing framework enables to boost the system's uptime and security. In smart grid technologies, the data grows dynamically [7]; the data centers in cloud computing framework may offer resource scalability according to requirement. At the same time, the real time computation is necessary to balance the loads on time, and trigger appropriate alarms for preventing outage problems. In this manner, it greatly reduces the infrastructure cost and ensures privacy, security, as well as quality of service. However, as per [1] the cloud-oriented services for CPS should be secure enough to ensure reliability, and must bear 1) Availability of the system to ensure resistance to denial of service (DoS) attacks, 2) Confidentiality of the sensitive data like billing and power/resource consumption and 3) Integrity from tempering, modification or any sort of fabrication of data in smart grids or other scenarios.

1.1. Related Work

Humayed et al. [8] illustrated different security aspects of CPS. They discussed many drawbacks including attacks in contemporary schemes by laying focus on few security requisites for smart grid, industrial systems, and smart cars. Later Giraldo et al. [9] pointed some privacy and security problems besides introducing a few defense mechanisms adopted in current CPS-based schemes. Ashibani and Mahmoud [10] presented a thorough analysis on various security properties being implemented at different levels of CPS architecture. Lee et al. [11] introduced a cyber-security testbed with respect to IoT and CPS to embed novel security models in industrial framework. Later Vegh and Miclea [12, 13] employed steganography to boost the CPS security. Thereafter, Choo et al. [14] came up with further innovations and improvements in security features of embedded CPS. Likewise, Hu et al. [15] demonstrated different techniques for building robust CPS systems. Rho et al. [16] presented several up-to-date implementations of different CPS technologies. Next, Socievole et al. [17] evaluated the progress in CPS in relation to mobile networking-based CPS. Mehar et al. [18] highlighted electric vehicular needs with respect to renewable energy in transport sector. Mondal et al. [19] presented a mobile smart grid-based energy trading algorithm designed on game theory principles. Later, Misra et al. [20] and Kumar et al. [22] demonstrated smart grid schemes to compute the price on dynamic pricing strategy. However, these schemes could only be applied in distributed cloud-based environment. Fang et al. [21] presented many smart gird-based challenges related to cloud computing. Sun et al. [23] designed an authentication protocol for mobile client-server architecture; however, despite low computational cost this scheme is vulnerable to stolen smart card and replay threats besides lacking password and biometric modification procedure. Next, Li et al. [25] presented a authenticated key agreement scheme for cloud computing framework. Nevertheless, this scheme is prone to stolen smart card, replay and privileged insider threats. Furthermore, Zhu and Liu [26] introduced an authenticated key agreement protocol based on elliptic curve cryptography (ECC). This scheme achieved the property of mutual authentication and session key establishment effectively; however this could not resist privileged insider attack on the other hand. Chang and Le [27] presented another authentication protocol for wireless sensor networks utilizing two-factor authentication. This scheme comprised two variants of the protocol, and both failed to resist offline password-guessing attack as well as session-specific temporary information attack, while one of those may not resist session-key breach attack [28]. To remedy the discussed flaws in [27], Das et al. [28] presented a novel authentication protocol in wireless sensor networks utilizing 3-factor authentication. Later, Amin et al. [29] suggested another authenticated key agreement protocol for distributed cloud computing framework having IoT-supported gadgets. However, the scheme may not resist forgery attack and privileged insider attack. Al-Turjman [32] conducted a survey on sensors of mobile phone with its alternative design techniques to support scalable actions. In this study the author performed analysis on the statistics for mobile phone and its context, and evaluated offline mobility detection applications against the online applications. It also examines the femtocell communication networks in IoT infrastructure with respect to energy consumption and efficiency along with other related parameters. The presented authentication solutions in WSN might be helpful in IoT for cloud-based multiple applications [34]. Al-Turjman et al. [34] designed an architecture titled as the seamless secure application and key agreement (S-SAKA), which employed ECC and bilinear pairing operations. This scheme warrants significant security features including user's privacy, mutual session key establishment, mutual authentication and confidentiality of the data. Elgedawy and Al-Turjman [35] demonstrated a seamless context sensitive and multi-modal identity provisioning framework (IdProF) with respect to latest mobile sensors and devices. The IdProF mitigates the identity compromise hazards, besides considering other resident's access, usage and behaviors. Chu et al. [36] designed a wireless oriented device to device (D2D) communication scheme in a hostile environment of malicious adversaries. By employing the two formalizations of Stackelberg game the authors infer that energy trading-based interactions among the D2D and mobile cellular networks are more significant in comparison with non-trading schemes.

1.2. Motivations and Contribution

Very recently, Challa et al. [1] proposed a CPS based scheme to provide key agreement between 1)user and cloud

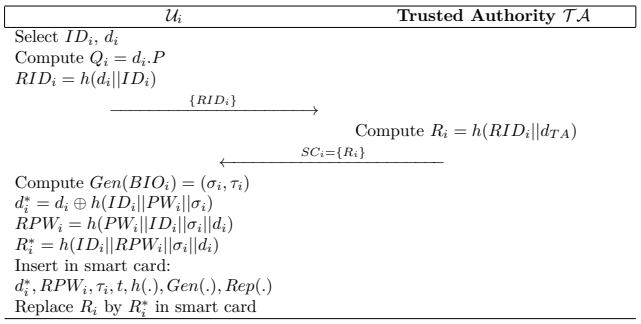

Figure 1: User Registration Phase in Challa et al.

server; and 2) smart meter and cloud server, both agremments are achieved by the help of intervening trusted authority. The security of their scheme was proved through formal, informal and automated AVISPA. Defiantly, it is to show in this paper that due to a critical design flaw, their scheme cannot work in CPS/IoT based environments. The scheme (if work) can only accommodate one user and cannot facilitate the key agreement between user/smart meter and a cloud server, if there are more than one users/smart meters registered with the system. Such type of one user system are not required in real world scenarios, where a smart grid may have hundreds or thousands of users. Moreover, this paper also unveils that the scheme of Challa et al. lacks untraceable anonymity and lack of verification on cloud server side may encourage the replay and/or denial of services attack. The article then introduces an improved and secure authentication system to facilitate a key agreement between user and cloud server via trusted authority. As an application, the proposed system also works for smart meter and cloud server to reach a key agreement. The security of the proposed scheme is discussed through formal and informal methods. The proposed system while providing all known security features has slightly increased the computation and communication costs as compared with the scheme of Challa et al. Rest of the paper is organized as follows: In Section 2 , the review of the scheme of Challa et al. is presented along with its' weaknesses in Section 3 . The proposed improved scheme is presented in Section 4 and the formal security analysis and discussion of security features is shown in Section 5 . The comparisons are made in Section 7 whereas, the conclusion is solicited in Section 8.

2. The Scheme of Challa et al.

This section briefly reviews the scheme proposed by Challa et al. along with it's application in smart meter scenario. Following subsections describe all the phase in detail, whereas; the employed notations in this article are solicited in Table 1:

2.1. System Setup

For setup purposes, $\mathcal{TA}$ picks an elliptic curve $E_p(x_1, x_2)$ over Z_p, and a point $P \in E_p(x_1, x_2)$ as base point, where p is a large prime number and $4x_1^3 - 27x_2^2 \neq 0 mod\ p$. $\mathcal{TA}$ then selects d_{TA} as private and $Q_{TA} = d_{TA}.P$ as $\mathcal{TA}$'s public key along with two biometric related functions $Gen(.)$ and $Rep(.)$ and a hash function $h(.)$. Subsequently, $\mathcal{TA}$ publishes $\{E_p(x_1, x_2), P, Q_{TA}, h(.), Gen(.), Rep(.), t\}$.

2.2. Smart Meter Pre-deployment phase

For registering a smart meter $\mathcal{SM}_k$, the $\mathcal{TA}$ selects ID_k as identity and $d_k \in Z_p$ as private key of $\mathcal{SM}_k$. Then $\mathcal{TA}$ computes $\mathcal{SM}_k$'s public key $Q_k = d_k.P$ along with pseudo identity $RID_k = (d_k||ID_k)$. Finally, $\mathcal{TA}$ stores $\{ID_k, d_k, RID_k\}$ in $\mathcal{SM}_k$'s memory and $\{ID_k, Q_k, RID_k\}$ in verifier maintained by $\mathcal{TA}$.

2.3. Registration

Following subsections describe the registration of both the Cloud Server and User:

2.4. Cloud Server Registration

The cloud server $\mathcal{CS}_j$, selects identity ID_j alongwith and $d_j \in Z_p$ and $Q_k = d_k.P$ as it's respective public, private key pair. $\mathcal{CS}_j$ then computes pseudo identity $RID_j = (d_j||ID_j)$ and sends RID_j to $\mathcal{TA}$ on secure channel. On reception, $\mathcal{TA}$ stores $\{ID_j, RID_j\}$ in the verifier maintained by $\mathcal{TA}$.

2.5. User Registration

To register with the system, $\mathcal{U}_i$ selects an identity ID_i and $\{d_i \in Z_p^*, Q_i = d_i.P\}$ as his private and public key pair. $\mathcal{U}_i$ computes and sends $RID_i = h(d_i||ID_i)$ to $\mathcal{TA}$. In response to received request, $\mathcal{TA}$ computes $R_i = h(RID_i||d_{TA})$, personalize a smart card SC_i with R_i and sends SC_i back to $\mathcal{U}_i$. The $\mathcal{U}_i$ on receiving SC_i selects a password PW_i and computes $Gen(BIO_i) = (\sigma_i, \tau_i)$, $d_i^* = d_i \oplus h(ID_i||PW_i||\sigma_i)$, $RPW_i = h(PW_i||ID_i||\sigma_i||d_i)$ and $R_i^* = h(ID_i||RPW_i||\sigma_i||d_i)$. Further, $\mathcal{U}_i$ Insert $\{d_i^*, RPW_i, \tau_i, t, h(.), Gen(.), Rep(.)\}$ in smart card and replaces R_i by R_i^* in smart card. The summary of this phase is also shown in Fig. 1.

2.6. Login Phase

$\mathcal{U}_i$ initiate login phase. Following steps are executed between smartcard/reader and $\mathcal{U}_i$:

Step LC 1: $\mathcal{U}_i$ insert SC_i into reader and inputs the pait $\{ID_i,\ PW_i\}$ and imprints his BIO_i.

Step LC 2: In response to login request, SC_i computes $\sigma_i = Rep(BIO_i, \tau_x)$, $d_i = d_i^* \oplus h(ID_i||PW_i||\sigma_i)$, $RPW_i^* = h(ID_i||PW_i||\sigma_x||d_i)$. SC_i aborts the session in case $RPW_i^* \neq RPW_i$. Otherwise, $\mathcal{U}_i$ login attempt is successful and SC_i selects $\alpha \in Z_p^*$ & T_i and computes $RID_i = h(d_i||ID_i)$, $R_i = R_i^* \oplus h(ID_i||RPW_i||\sigma_i||d_i)$, $DID_j = ID_j \oplus h(R_i||\alpha||T_i)$, $\alpha^* = \alpha \oplus h(R_i||T_i)$ and $V_i = h(ID_j||R_i||\alpha||T_i||RID_i)$. Then SC_i sends the tuple $\{RID_i, DID_j, \alpha^*, T_i, V_i\}$ to $\mathcal{TA}$.

Table 1: Notation Guide

Notations	Description
$\mathcal{TA}$, $\mathcal{CS}_j$, $\mathcal{SM}_k$,$\mathcal{U}_i$	Trusted Authority, Cloud server, Smart Meter, User
PW_i, SC_i,ID_i, BIO_i	$\mathcal{U}_i$'s password, smartcard, identity & Biometrics
ID_j, ID_j, t	Identities of of $\mathcal{CS}_j$, $\mathcal{SM}_k$, Error tolerance threshold
σ_i, τ_i	Secret biometric key, Biometric reproduction parameter
$Gen(..)$, $Rep(..)$	Generation and Reproduction functions for fuzzy generator
p, Z_p, E_p	Large prime, Finite Prime Field, Elliptic curve Z_p
T_x, ΔT	Current time stamp of x^{th} party, Max. allowable delay
$h(.)$, $\oplus$, $\|$, SK_{ij}	Hash, XOR, Concatenation functions, Session key

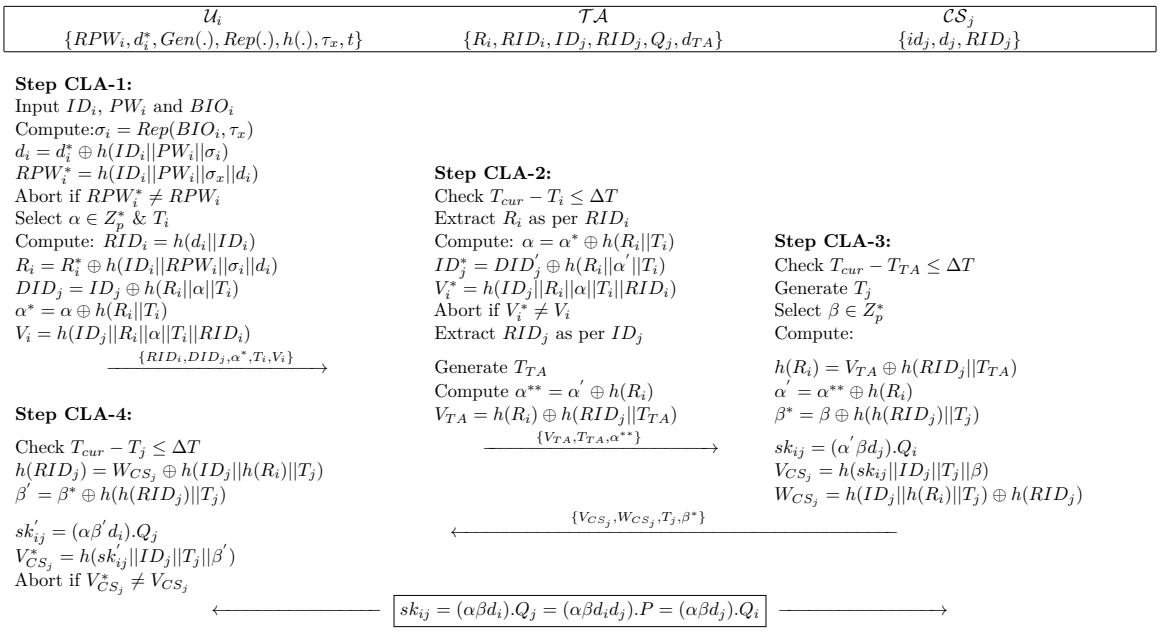

Figure 2: The Scheme of Challa et al.

2.7. Authenticated Key Agreement

In Challa et al.'s method, this phase is further bifurcated into following phases:

2.7.1. Authenticated Key Agreement

During this phase, $\mathcal{U}_i$ gets authenticated from $\mathcal{TA}$ and shares a session key with $\mathcal{CS}_j$ with the help of $\mathcal{TA}$. Following steps are executed in this phase:

Step AC 1: In response to authentication request, $\mathcal{TA}$ verifies the validity of T_i by comparing it with current timestamp $T_{cur} - T_i \leq \Delta T$, aborts the session if it goes beyond the threshold ΔT. In case, the T_i is proved as legal, $\mathcal{TA}$ extracts R_i corresponding to RID_i and computes $\alpha = \alpha^* \oplus h(R_i||T_i)$, $ID_j^* = DID_j^{'} \oplus h(R_i||\alpha^{'}||T_i)$ and $V_i^* = h(ID_j||R_i||\alpha||T_i||RID_i)$. The $\mathcal{TA}$ checks and aborts the session if $V_i^* \neq V_i$. Otherwise, $\mathcal{TA}$ extract RID_j corresponding to ID_j, generates T_{TA} and then computes $\alpha^{**} = \alpha^{'} \oplus h(R_i)$ and $V_{TA} = h(R_i) \oplus h(RID_j||T_{TA})$. $\mathcal{TA}$ completes this step by sending the tuple $\{V_{TA}, T_{TA}, \alpha^{**}\}$ to $\mathcal{CS}_j$.

Step AC 2: In response to the message by $\mathcal{TA}$, $\mathcal{CS}_j$ verifies the validity of T_{TA} by comparing it with current timestamp $T_{cur} - T_{TA} \leq \Delta T$, aborts the session if it goes beyond the threshold ΔT. In case, the T_{TA} is proved as legal, $\mathcal{CS}_j$ generates T_j, selects $\beta \in Z_p^*$ and computes $h(R_i) = V_{TA} \oplus h(RID_j||T_{TA})$, $\alpha^{'} = \alpha^{**} \oplus h(R_i)$, $\beta^* = \beta \oplus h(h(RID_j)||T_j)$, $sk_{ij} = (\alpha^{'}\beta d_j).Q_i$, $V_{CS_j} = h(sk_{ij}||ID_j||T_j||\beta)$ and $W_{CS_j} = h(ID_j||h(R_i)||T_j) \oplus h(RID_j)$. $\mathcal{CS}_j$ completes this step by sending the tuple $\{V_{CS_j}, W_{CS_j}, T_j, \beta^*\}$ to $\mathcal{U}_i$.

Step AC 3: After receiving the reply message from $\mathcal{CS}_j$, $\mathcal{U}_i$, verifies the validity of T_j by comparing it with current timestamp $T_{cur} - T_j \leq \Delta T$, aborts the session if it goes beyond the threshold ΔT. In case, the T_j is proved as legal, $\mathcal{U}_i$ computes $h(RID_j) = W_{CS_j} \oplus h(ID_j||h(R_i)||T_j)$, $\beta^{'} = \beta^* \oplus h(h(RID_j)||T_j)$, $sk_{ij}^{'} = (\alpha\beta^{'}d_i).Q_j$ and $V_{CS_j}^* = h(sk_{ij}^{'}||ID_j||T_j||\beta^{'})$. The $\mathcal{U}_i$ checks and aborts the session if $V_{CS_j}^* \neq V_{CS_j}$. Otherwise $\mathcal{U}_i$ consider authentication request successful and keep sk_{ij} as session key for secure communication between $\mathcal{U}_i$ and $\mathcal{CS}_j$.

2.7.2. Smart Meter Authentication Phase

During this phase, $\mathcal{SM}_k$ gets authenticated and shares a session key with $\mathcal{CS}_j$ with the help of $\mathcal{TA}$. Following steps are executed in this phase:

Step MAC 1: $\mathcal{SM}_k$ selects $a \in Z_p^*$ & T_a and computes $DID_j = ID_j \oplus h(ID_k||a||T_k)$, $a^* = a \oplus h(ID_k||T_k)$ and $V_k = h(ID_j||a||T_k||RID_k)$. Then $\mathcal{SM}_k$ sends the tuple $\{RID_k, DID_j, a^*, T_k, V_k\}$ to $\mathcal{TA}$.

Step MAC 2: In response to the received request, $\mathcal{TA}$ verifies the validity of T_k by comparing it with current timestamp $T_{cur} - T_k \leq \Delta T$, aborts the session if it goes beyond the threshold ΔT. In case, the T_k is proved as legal, $\mathcal{TA}$ extracts ID_k corresponding to RID_k and computes $a = a^* \oplus h(ID_k||T_k)$, $ID_j^* = DID_j^{'} \oplus h(ID_k||a^{'}||T_k)$ and $V_k^* = h(ID_k||a||T_k||RID_k)$. The $\mathcal{TA}$ checks and aborts the session if $V_k^* \neq V_k$. Otherwise, $\mathcal{TA}$ extract RID_j corresponding to ID_j, generates T_{TA} and then computes $a^{**} = a^{'} \oplus h(ID_k)$ and $V_{TA} = h(ID_k) \oplus h(RID_j||T_{TA})$. $\mathcal{TA}$ completes this step by sending the tuple $\{V_{TA}, T_{TA}, a^{**}\}$ to $\mathcal{CS}_j$.

Step MAC 3: In response to the message by $\mathcal{TA}$, $\mathcal{CS}_j$ verifies the validity of T_{TA} by comparing it with current timestamp $T_{cur} - T_{TA} \leq \Delta T$, aborts the session if it goes beyond the threshold ΔT. In case, the T_{TA} is proved as legal, $\mathcal{CS}_j$ generates T_j, selects $b \in Z_p^*$ and computes $h(ID_k) = V_{TA} \oplus h(RID_j||T_{TA})$, $a^{'} = a^{**} \oplus h(ID_k)$, $b^* = b \oplus h(h(RID_j)||T_j)$, $sk_{ij} = (a^{'}bd_j).Q_k$, $V_{CS_j} = h(sk_{ij}||ID_j||T_j||b)$ and $W_{CS_j} = h(ID_j||h(ID_k)||T_j) \oplus h(RID_j)$. $\mathcal{CS}_j$ completes this step by sending the tuple $\{V_{CS_j}, W_{CS_j}, T_j, b^*\}$ to $\mathcal{SM}_k$.

Step MAC 4: After receiving the reply message from $\mathcal{CS}_j$, $\mathcal{SM}_k$, verifies the validity of T_j by comparing it with current timestamp $T_{cur} - T_j \leq \Delta T$, aborts the session if it goes beyond the threshold ΔT. In case, the T_j is proved as legal, $\mathcal{SM}_k$ computes $h(RID_j) = W_{CS_j} \oplus h(ID_j||h(ID_k)||T_j)$, $b^{'} = b^* \oplus h(h(RID_j)||T_j)$, $sk_{ij}^{'} = (ab^{'}d_k).Q_j$ and $V_{CS_j}^* = h(sk_{ij}^{'}||ID_j||T_j||b^{'})$. The $\mathcal{SM}_k$ checks and aborts the session if $V_{CS_j}^* \neq V_{CS_j}$. Otherwise, $\mathcal{SM}_k$ consider authentication request successful and keep sk_{ij} as session key for secure communication between $\mathcal{SM}_k$ and $\mathcal{CS}_j$.

3. Weaknesses of the Scheme of Challa et al.

This section presents some weaknesses of the scheme of Challa et al. Following subsections show that the scheme proposed in [1] is having correctness issues and does not provide anonymity. Any attacker can trace a user by just listening and recording the public channel. Moreover, cloud sever do not verify the validity/legality of any request; so, every request will be processed and a key will be formed with counterpart user. Although, the Attacker will not be able to form the key because it requires the private key of the impersonated user, but this attack may force the cloud server to process the request. A large number of such requests may lead to Denial of Services.

3.1. Incorrectness

The authentication phase of Challa et al.'s scheme cannot complete normally, and the cloud server and user may not be able to share any key at all. The user in Challa et al. scheme after directing authentication message to cloud server via trusted authority, may never receive a response

and the cloud server may never generate a session key. Hence, the scheme works in total absence of authentication and key agreement. The case of incorrectness is illustrated as follows:

1. $\mathcal{U}_i$ initiates a login request by entering password, identity and biometric, the smartcard SC_i computes and sends $\{RID_i, DID_i, \alpha^*, T_i, V_i\}$ to $\mathcal{TA}$.

2. Upon receiving the request, $\mathcal{TA}$ after formal verification of timestamp freshness and legality of user, computes and sends $\{V_{TA}, T_{TA}, \alpha^{**}\}$ to $\mathcal{CS}_j$.

3. $\mathcal{CS}_j$ receives the request message and verifies the freshness of timestamp T_{TA}. $\mathcal{CS}_j$ generates/selects $T_j,\ \beta \in Z_p^*$ and computes:

$$h(R_i) = V_{TA} \oplus h(RID_j||T_{TA}) \quad (1)$$
$$\alpha^{'} = \alpha^{**} \oplus h(R_i) \quad (2)$$
$$\beta^* = \beta \oplus h(h(RID_j)||T_j) \quad (3)$$

4. After computing $h(R_i), \alpha^{'}, \beta^*$, the $\mathcal{CS}_j$ computes the session key:

$$sk_{ij} = (\alpha^{'}\beta d_j).Q_i \quad (4)$$

   The computation of session key in Eq. 4, requires the public key Q_i of $\mathcal{U}_i$. However, $\mathcal{CS}_j$ does not know identity of the requesting user. The message $(\{V_{TA}, T_{TA}, \alpha^{**}\})$ sent by $\mathcal{TA}$ does not reveal any information about the requesting user. $\mathcal{CS}_j$ process the whole request with unknown user. Moreover, $\mathcal{TA}$ does not send anyother information about the public key; so, using the public key of the user to compute session key as in Eq. 4 is out of question. Furthermore, $\mathcal{CS}_j$ sends reply message $\{V_{CS_j}, W_{CS_j}, T_j, \beta^*\}$ to $\mathcal{U}_i$. Similar to above analogy, $\mathcal{CS}_j$ does not know to whom it has to send the reply message. Moreover, $\mathcal{CS}_j$ has no established connection with $\mathcal{U}_i$. Therefore, $\mathcal{CS}_j$ cannot send any message directly to $\mathcal{U}_i$.

The scheme of Challa et al. can complete normally and can accomplish authentication as well as establishment of key between $\mathcal{U}_i$ and $\mathcal{CS}_j$ via $\mathcal{TA}$ in case if the system has one and only one registered user. Such single user systems are not desirable in real world scenarios. The same incorrectness is translated in the application of the scheme of Challa et al. to facilitate key agreement between a smart meter and cloud server. The smart meter application of Challa et al. can only work with a single meter, which is not desirable in any scenario rather the real world systems are always having a number of smart meters connected to cloud server for gaining electricity access. Therefore, Challa et al.'s scheme and it's application for facilitating smart meter authentication are incorrect and this incorrectness results into total incompatibility with real world deployments.

3.2. Lack of un-traceable Anonymity

Anonymity encompasses identity hiding as well as untraceability, the former ensures that the identity of the communicating user remains secret on public chennel and the latter implies that by just listening the communication channel, the adversary cannot ensure whether or not different sessions are initiated by a single user. The user AKA scheme and it's application in smart meter scenario, proposed by Challa et al. ensure the identity (ID_i) hiding; whereas, the same pseudo identity RID_i is sent for all subsequent sessions. Therefore, an adversary just by listening the public channel can accurately estimate by just passively recording RID_i, that the requesting user is same or not; likewise, the adversary can trace the request frequency by a particular user and so on. Therefore, Challa el al.'s scheme and it's application in smart meter scenario both lack proper anonymity.

3.3. Lack of Request Verification on Cloud Server

Upon receiving the $\mathcal{U}_i$'s request message $\{V_{TA}, T_{TA}, \alpha^{**}\}$ from $\mathcal{TA}$, $\mathcal{CS}_j$ verifies the freshness of T_{TA} and on successful verification proceeds with the request. $\mathcal{CS}_j$ does not verify any other parameter. The adversary can create a fabricated message by just generating current timestamp T_A and randomly selecting $\{\overline{V}_{TA}$ and $\overline{\alpha}^{**}\}$. The fabricated message $\{\overline{V}_{TA}, T_A, \overline{\alpha}^{**}\}$ may be sent to $\mathcal{CS}_j$. Upon reception of fabricated message, $\mathcal{CS}_j$ will verify the freshness of T_A, as it is freshly generated, so will pass the verification. $\mathcal{CS}_j$ will then compute other parameters without checking the legality/validity and sends reply message to $\mathcal{U}_i$. Although, the adversary may not be able to compute session key as it requires private key (d_i) of $\mathcal{U}_i$ but against each fabricated message, $\mathcal{CS}_j$ may complete whole procedure. A large number of such requests may also lead to denial of services from cloud server. Similarly, the attacker can just replace the time stamp and replay an old message. The same problem *lack of request verification on Cloud server* side also exist in smart meter application of Challa et al.'s scheme.

4. Proposed Scheme

In this section, we explain the proposed AKA scheme for CPS. The scheme is designed after carefully analyzing the design flaws of Challa et al.'s scheme. The shifting of tradeoff between security and efficiency towards computation and communication efficiencies led to the incorrectness of the scheme. Furthermore, the lack of untraceability and lack of cloud server side verification is also a result of this shift. The proposed scheme is designed as an effort to provide a better tradeoff between the two. The proposed scheme works by modifying some step in user and smart meter authentication phases of Challa et al.'s scheme. The system setup, and registration phases are taken as it is from Challa et al.'s scheme. Following subsections explain the proposed scheme, which is also summarized in Fig. 3:

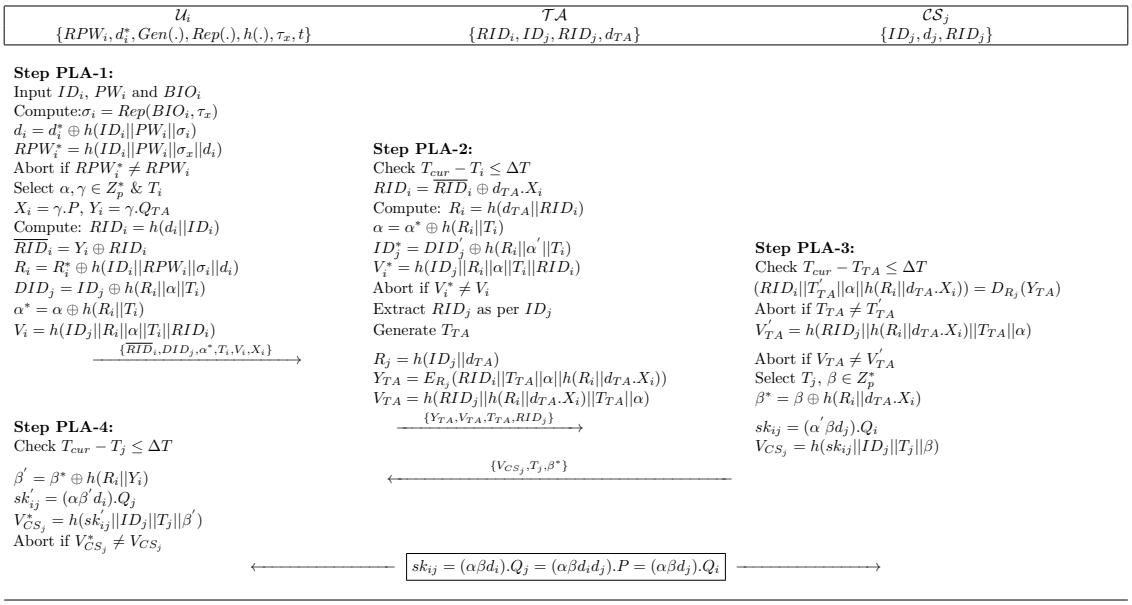

Figure 3: Proposed Scheme

4.1. Login Phase

$\mathcal{U}_i$ initiate login phase. Following steps are executed between smartcard/reader and $\mathcal{U}_i$:

Step LP 1: $\mathcal{U}_i$ insert SC_i into reader and inputs the pait $\{ID_i,\ PW_i\}$ and imprints his BIO_i.

Step LP 2: In response to login request, SC_i computes $\sigma_i = Rep(BIO_i, \tau_x)$, $d_i = d_i^* \oplus h(ID_i||PW_i||\sigma_i)$, $RPW_i^* = h(ID_i||PW_i||\sigma_x||d_i)$. SC_i aborts the session in case $RPW_i^* \neq RPW_i$. Otherwise, $\mathcal{U}_i$'s login attempt is successful and SC_i selects $\alpha, \gamma \in Z_p^*$ & T_i and computes:

$$X_i = \gamma.P$$
$$Y_i = \gamma.Q_{TA}$$
$$RID_i = h(d_i||ID_i)$$
$$\overline{RID}_i = Y_i \oplus RID_i$$
$$R_i = R_i^* \oplus h(ID_i||RPW_i||\sigma_i||d_i)$$
$$DID_j = ID_j \oplus h(R_i||\alpha||T_i)$$
$$\alpha^* = \alpha \oplus h(R_i||T_i)$$
$$V_i = h(ID_j||R_i||\alpha||T_i||RID_i)$$

Then SC_i sends the tuple $\{\overline{RID}_i, DID_j, \alpha^*, T_i, V_i, X_i\}$ to $\mathcal{TA}$.

4.2. Authenticated Key Agreement

In proposed scheme two separate AKA phases are defined for two entities (i.e User and Smart Meter), explained as follows:

4.2.1. Authenticated Key Agreement

During this phase, $\mathcal{U}_i$ gets authenticated from $\mathcal{TA}$ and shares a session key with $\mathcal{CS}_j$ with the help of $\mathcal{TA}$. Following steps are executed in this phase:

Step AP 1: In response to authentication request, $\mathcal{TA}$ verifies the validity of T_i by comparing it with current timestamp $T_{cur} - T_i \leq \Delta T$, aborts the session if it goes beyond the threshold ΔT. In case, the T_i is proved as legal, $\mathcal{TA}$ computes:

$$RID_i = \overline{RID}_i \oplus d_{TA}.X_i$$
$$R_i = h(d_{TA}||RID_i)$$
$$\alpha = \alpha^* \oplus h(R_i||T_i)$$
$$ID_j^* = DID_j^{'} \oplus h(R_i||\alpha^{'}||T_i)$$
$$V_i^* = h(ID_j||R_i||\alpha||T_i||RID_i)$$

The $\mathcal{TA}$ checks and aborts the session if $V_i^* \neq V_i$. Otherwise $\mathcal{TA}$ extract RID_j corresponding to ID_j, generates T_{TA} and then computes:

$$R_j = h(ID_j||d_{TA})$$
$$Y_{TA} = E_{R_j}(RID_i||T_{TA}||\alpha||h(R_i||d_{TA}.X_i))$$
$$V_{TA} = h(RID_j||h(R_i||d_{TA}.X_i)||T_{TA}||\alpha)$$

$\mathcal{TA}$ completes this step by sending the tuple $\{Y_{TA}, V_{TA}, T_{TA}, RID_j\}$ to $\mathcal{CS}_j$.

Step AP 2: In response to the message by $\mathcal{TA}$, $\mathcal{CS}_j$ verifies the validity of T_{TA} by comparing it with current timestamp $T_{cur} - T_{TA} \leq \Delta T$, aborts the session if it goes beyond the threshold ΔT. In case, the T_{TA} is proved as legal, $\mathcal{CS}_j$ computes:

$$(RID_i||T_{TA}^{'}||\alpha||h(R_i||d_{TA}.X_i)) = D_{R_j}(Y_{TA})$$
$$V_{TA}^{'} = h(RID_j||h(R_i||d_{TA}.X_i)||T_{TA}||\alpha)$$

$\mathcal{CS}_j$ abort the session if $T_{TA} \neq T_{TA}^{'}$ and/or $V_{TA} \neq V_{TA}^{'}$ and in case of success, $\mathcal{CS}_j$ selects $\beta \in Z_p^*$ and computes :

$$\beta^* = \beta \oplus h(R_i||Y_i)$$
$$sk_{ij} = (\alpha^{'}\beta d_j).Q_i$$
$$V_{CS_j} = h(sk_{ij}||ID_j||T_j||\beta)$$

$\mathcal{CS}_j$ completes this step by sending the tuple $\{V_{CS_j}, T_j, \beta^*\}$ to $\mathcal{U}_i$.

Step AP 3: After receiving the reply message from $\mathcal{CS}_j$, $\mathcal{U}_i$, verifies the validity of T_j by comparing it with current timestamp $T_{cur} - T_j \leq \Delta T$, aborts the session if it goes beyond the threshold ΔT. In case, the T_j is proved as legal, $\mathcal{U}_i$ computes:

$$\beta^{'} = \beta^* \oplus h(R_i)||d_{TA}.X_i)$$
$$sk_{ij}^{'} = (\alpha\beta^{'}d_j).Q_i$$
$$V_{CS_j} = h(sk_{ij}||ID_j||T_j||\beta^{'})$$

The $\mathcal{U}_i$ checks and aborts the session if $V_{CS_j}^* \neq V_{CS_j}$. Otherwise, $\mathcal{U}_i$ consider authentication request successful and keep sk_{ij} as session key for secure communication between $\mathcal{U}_i$ and $\mathcal{CS}_j$.

4.2.2. Smart Meter Authentication Phase

During this phase, $\mathcal{SM}_k$ gets authenticated and shares a session key with $\mathcal{CS}_j$ with the help of $\mathcal{TA}$. Following steps are executed in this phase:

Step PMA 1: $\mathcal{SM}_k$ selects $a, c \in Z_p^*$ & T_k and computes $X_k = c.P$, $Y_k = c.Q_{TA}$, $RID_k = h(d_k||ID_k)$, $\overline{RID}_k = Y_k \oplus RID_k$, $DID_j = ID_j \oplus h(ID_k||a||T_k)$, $a^* = a \oplus h(Y_k||T_k)$ and $V_k = h(ID_j||Y_k||a||T_k||RID_k)$. Then $\mathcal{SM}_k$ sends the tuple $\{\overline{RID}_i, DID_j, a^*, T_k, V_k, X_k\}$ to $\mathcal{TA}$.

Step PMA 2: In response to the received request, $\mathcal{TA}$ verifies the validity of T_k by comparing it with current timestamp $T_{cur} - T_k \leq \Delta T$, aborts the session if it goes beyond the threshold ΔT. In case, the T_k is proved as legal, $\mathcal{TA}$ computes $RID_k = \overline{RID}_k \oplus d_{TA}.X_k$, $a = a^* \oplus h(d_{TA}.X_k||T_k)$, $ID_j^* = DID_j^{'} \oplus h(ID_k||a^{'}||T_k)$ and $V_k^* = h(ID_j||d_{TA}.X_k||a||T_k||RID_k)$. The $\mathcal{TA}$ checks and aborts the session if $V_k^* \neq V_k$. Otherwise, $\mathcal{TA}$ extract RID_j corresponding to ID_j, generates T_{TA} and then computes $R_j = h(ID_j||d_{TA})$, $Y_{TA} = E_{R_j}(RID_k||T_{TA}||a||d_{TA}.X_k)$ and $V_{TA} = h(RID_j||d_{TA}.X_k||T_{TA}||a)$. $\mathcal{TA}$ completes this step by sending the tuple $\{Y_{TA}, V_{TA}, T_{TA}, RID_j\}$ to $\mathcal{CS}_j$.

Step PMA 3: In response to the message by $\mathcal{TA}$, $\mathcal{CS}_j$ verifies the validity of T_{TA} by comparing it with current timestamp $T_{cur} - T_{TA} \leq \Delta T$, aborts the session if it goes beyond the threshold ΔT. In case, the T_{TA} is proved as legal, $\mathcal{CS}_j$ computes $(RID_k||T_{TA}^{'}||a||d_{TA}.X_k) = D_{R_j}(Y_{TA})$ and $V_{TA}^{'} = h(RID_j||d_{TA}.X_k||T_{TA}||a)$. $\mathcal{CS}_j$ abort the session if $T_{TA} \neq T_{TA}^{'}$ and/or $V_{TA} \neq V_{TA}^{'}$ and in case of success, $\mathcal{CS}_j$ selects $b \in Z_p^*$ and computes $b^* = b \oplus d_{TA}.X_k$, $sk_{ij} = (a^{'}bd_j).Q_k$ and $V_{CS_j} = h(sk_{ij}||ID_j||T_j||b)$. $\mathcal{CS}_j$ completes this step by sending the tuple $\{V_{CS_j}, T_j, b^*\}$ to $\mathcal{SM}_k$.

Step PMA 4: After receiving the reply message from $\mathcal{CS}_j$, $\mathcal{SM}_k$, verifies the validity of T_j by comparing it with current timestamp $T_{cur} - T_j \leq \Delta T$, aborts the session if it goes beyond the threshold ΔT. In case, the T_j is proved as legal, $\mathcal{SM}_k$ computes $b^{'} = b^* \oplus Y_k$, $sk_{ij}^{'} = (ab^{'}d_j).Q_k$ and $V_{CS_j} = h(sk_{ij}||ID_j||T_j||b^{'})$. The $\mathcal{SM}_k$ checks and aborts the session if $V_{CS_j}^* \neq V_{CS_j}$. Otherwise, $\mathcal{SM}_k$ consider authentication request successful and keep sk_{ij} as session key for secure communication between $\mathcal{SM}_k$ and $\mathcal{CS}_j$.

5. Security Analysis

This section solicits the formal security analysis as well as a discussion on attack resilience of the proposed scheme for various attacks. Following subsections provide the detail analysis:

5.1. Formal Security

This section deals with the utilization of universally recommended Real or Random (ROR) model [41] for analysis of formal security of the proposed scheme. Several formal security models and assumptions of given proves are used to implant these analysis. The session key security (SK security) during user login and key agreement phases are proposed by theorem 3.

The instances are supplemented by the ROR model. The participants (1) a User $\mathcal{U}_i$, (2) the $\mathcal{TA}$ and (3) a cloud server $\mathcal{CS}_j$ are used during the user login, key agreement and authentication phases.

Participants Let $\Pi_{TA}^a, \Pi_{U_i}^b, \Pi_{CS_j}^c$ specify the attribute c, b, a of $\mathcal{TA}$,$\mathcal{U}_i$ and $\mathcal{CS}_j$, particularly. They are specified as oracles.

Accept state. The transit of Π^b into an accept state is dependent upon receiving the last protocol accepted message. The session identification (SID) of Π^b comprises of the ordered concentration of all communicated messages by Π^b.

Partnering. Two instances U_i^b and CS_j^c if the consecutive three condition are fulfilled contemporary then it is said to be partnered:(1) both U_i^b and CS_j^c are in accepted state; (2) both U_i^b and CS_j^c mutually valid each other and communicate the same sid; and (3) U_i^b and CS_j^c are the

corresponds partners.

Freshness. An attribute Π^b is in good state, if the session key sk_{ij} is not leaked to an opponent $\mathcal{A}$ through the show (Π^b) problems.

Adversary. Under the ROR model, All the communication in this network than $\mathcal{A}$ will have the full the full controlled. So that, $\mathcal{A}$ can read, change and fabricate or injected the transferred messages. although, $\mathcal{A}$ will have the following problems:

• **Execute** (Π^b, Π^a): $\mathcal{A}$ execute this hypothesis so as to get the message traded between two number. If display a listing stealthily attacks.

• **Send** ($\Pi^b, mesg$): $\mathcal{A}$ makes this hypothesis for communicating something specific express MSG to a member case, say Π^b and furthermore for accepting a reaction message. It demonstrate a functioning assault

• **Reveal** (Π^b): This hypothesis uncovers the present session key sk_{ij} produced by Π^b (and its accomplice) to and misfortune $\mathcal{A}$.

• **Corruptsmartcard**($\Pi^b_{U_j}$): It demonstrate the keen card lost assault, and it separates all the data away in SC_i of legal user U_i.

• **CorruptsmartMeter**(Π^b_{SMK}): The condition of long term secret key revel to $\mathcal{A}$ is modeled by this query. CorruptSmartMeter and CorruptSmartCard queries both are linked to a weak-corruption model where ephermal secrets and internal data of the participants is never corrupted.

• **Test**(Π^b): The semantic security of the session key sk_{ij} is modeled by this query between $\mathcal{U}_i$ and $\mathcal{CS}j$. The value of coin C is first flipped towards the beginning of the investigation and its worth is just known to $\mathcal{A}$. The bit worth is just known to $\mathcal{A}$. The bit worth c (either 0 or 1) known to $\mathcal{A}$. The bit worth c (either 0 or 1) further used to choose the yeild of the test question in the wake of executing the inquiry by $\mathcal{A}$. In the event that the setup sk_{ij} is new, and return sk_{ij} when c=1 or an irregular number in a similar area when c=0 else it restores an invalid worth.

• **Semantic security of the session key**

In ROR model it is essential that $\mathcal{A}$ requirements to recognize a attribute's genuine session key and an random number. $\mathcal{A}$ few test question can be questioned by $\mathcal{A}$ to either $\Pi^b_{U_i}$ or $\Pi^c_{CS_j}$ towards the end, $\mathcal{A}$ profits a speculated bit $c^{'}$ and can be denominated, he match when the condition $c^{'} == c$ is met. Let succ mean an occasion that $\mathcal{A}$ can dominate the match. In our Authenticated Key Exchange (AKE) scheme the breaking of SK and advantage of Adv_p^{AKE}, where P is defined by

$$Adv_p^{AKE} = |2.P_r[Succ] - 1| \tag{5}$$

6. Random Oracle

The access to collision resistant one way cryptographic hash $h(.)$ is allowed to all participants and A. The modeling of $h(.)$ is done as random oracle H.

Theorem 3: Here $\mathcal{A}$ is letted to be an adversary that is run in an polynomial state of time b against a proposed scheme P in ROR model, D is taken as the uniformly distributed password dictionary and l is considered to be the number of bits in bio-metrics key sigmai. At that point thee upside of breaking the sk_{ij} security of the proposed plot during client login, and confirmation and key understanding stages is given by:

$$Adv_P^{AKE} \leq \frac{q_h^2}{|Hash|} + \frac{q_{Send}}{2^{l-1}.|D|} + 2Adv^{ECDDHP}(b) \tag{6}$$

Where $q_h, q_{sends}, |Hash|, |D|$ and $Adv^{ECDDHP}(b)$ are the number of H queries, sends queries, the range space of $h(.)$, size of D and advantage of $ECDDHP$ respectively.

Proof: Five different games $Game_{in}(in = 0, 1, 2, 3, 4)$ are considered in our security proof. For example we consider a situation where Succi is an event that is open to $\mathcal{A}$ and it can guess the bit c in $Game_{in}$ and win it. Game0 reflects the real attack on P and game end with Game4 leaving $\mathcal{A}$ with minor advantage of breaking SK security of proposed scheme.

$Game_0$: By launching a real attack on p at the start of this game at start time. First of all we select the bit c

$$Adv_P^{AKE} = |2.P_r[Succ_0] - 1| \tag{7}$$

$Game_1$: For simulating eavesdropping attack $Game_0$ is modified to $Game_1$". $Game_1$ begins with querying the function Execute(Π^t, Π^u) query by $\mathcal{A}$. A session key sk_{ij} is received by Test query from $\mathcal{A}$ to check if it is a random value or actual value. The CS_j computes the session sk_{ij}. As $sk_{ij} = (\alpha\beta d_j).Q_i$. sk_{ij} also evaluates the same session key $sk_{ij} = (\alpha\beta d_i).Q_j$. The secrets α, β , the private key d_j of U_i and the private key d_j of CS_j are necessary to evaluate the session key. Therefore, the probability of $\mathcal{A}$ winning $Game_1$ is not improved by eavesdropping. Resultant $Game_0$ and $Game_1$ are essentially equivalent, therefore

$$Pr[Succ1] = Pr[Succ0] \tag{8}$$

$Game_2$: $Game_1$ helped in the transformation of $Game_2$. H and Send are sent by $\mathcal{A}$ in this game. By submitting a forged message, $\mathcal{A}$ will deliberately target a participant. The secrets ID_j, RID_j, d_i and d_j are required by $\mathcal{A}$, to generate a authentic message $\{RID_i, DID_j, \alpha^*, T_i, V_i, X_i\}$, $\{Y_{TA}, V_{TA}, T_{TA}, RID_j$ and $\{VCS_j, T_j, \beta^*\}$. These values are embedded in the values of hash. Additionally, no collision will occur in message digests(hash outputs) due to random numbers α and β, and current timestamps T_i, T_{TA} and T_j. Birthday paradox results ensure that:

$$Pr[Succ1] - Pr[Succ2] | \leq \frac{q^2 h}{2.|Hash|} \tag{9}$$

$Game_3$: $\mathcal{A}$ makes the CorruptSamrtCard query in this game. $\mathcal{A}$ may conjecture the correct smartcard SC_i password PW_i of U_i from extracted details, using the password dictionary attack. The proposed scheme uses a fuzzy extractor which allows almost l nearly random bits for the biometric key σ_i. The probability of guessing the biometric key $\sigma_i \in 0, 1$ by $\mathcal{A}$ is approximately $1/2^l$. As, the number of permitted incorrect password entries is limited. We have,

$$|Pr[Succ2] - Pr[Succ3]| \leq \frac{q_{send}}{2^l.|D|} \tag{10}$$

$Game_4$: The real session key $SK_{ij} (= SK_{ij}^{'})$ is retrieved by $\mathcal{A}$, by eavesdropping in the final game. It is necessary to have secret information α, β , the private key d_i of $\mathcal{U}_i$ and the private key d_j of CS_j to evaluate the session key. In order to get $(d_i d_j).P$, it is hard to compute $\mathcal{A}$, given equations $Q_i = d_i.P$ and $Q_j = d_j.P$ because of the difficulty in solving ECDDHP. Due to that, to derive the session key $SK_{ij} = (\alpha\beta d_i).Q_j = (\alpha\beta d_i d_j).P = (\alpha\beta d_j).Q_i$. it is a hard task for $\mathcal{A}$. Therefore we have

$$|Pr[Succ3] - Pr[Succ4]| \leq Adv^{ECDDHP}(b) \tag{11}$$

Eventually, $\mathcal{A}$ does not know the bit c as both U_i and CS_J generate the session keys independent and randomly.

$$Pr[Succ4] = \frac{1}{2} \tag{12}$$

By solving equation 1, 2 and 6 we get

$$\frac{1}{2}.Adv_P^{AKE} = Pr[Succ0] - \frac{1}{2}|Pr[Succ1] - \frac{1}{2}| \tag{13}$$

Using triangular equality solve equations 3 and 7 we btain

$$\begin{aligned} |Pr[Succ1] - Pr[Succ4]| &\leq |Pr[Succ1] - Pr[Succ2]| + \\ |Pr[Succ2] - Pr[Succ4]| &\leq |Pr[Succ1] - Pr[Succ2]| + \\ |Pr[Succ2] - Pr[Succ3]| &+ |Pr[Succ3] - Pr[Succ4]| \leq \\ &\frac{q^2 h}{2.|Hash|} + \frac{q_{sends}}{2^l.|D|} + Adv^{ECDDHP}(b) \end{aligned} \tag{14}$$

Now, equation 6 and 7 proceeded and find the results:

$$|Pr[Succ1] - \frac{1}{2}| \leq \frac{q^2 h}{2.|Hash|} + \frac{q_{sends}}{2^l.|D|} + Adv^{ECDDHP}(b) \tag{15}$$

After that, equation 7 and 9 produces results as follows

$$Adv_P^{AKE} \leq \frac{q^2 h}{2.|Hash|} + \frac{q_{sends}}{2^{l_1}.|D|} + 2Adv^{ECDDHP}(b) \tag{16}$$

Remark1: According to the similarity of theorem 3, It is cleared that in the stolen of the SK-security of the proposed protocol their is an advantage of an adversary amid the key agreement phase and authentication of the smart meter is

$$Adv_P^{AKE} \leq \frac{q^2 h}{+} 2.|Hash| + 2Adv^{ECDDHP}(b) \tag{17}$$

6.1. Security Discussion

6.1.1. Anonymity & Privacy

Our scheme, in contrary to Challa's scheme, complies with the notion of maintaining anonymity or user's privacy which is one of the critical security requirement of smart grid-based AKA schemes. In Challa's scheme, the user submits RID_i in each session towards $\mathcal{TA}$. In our scheme, we computed $\overline{RID}_i = Y_i \oplus RID_i$ and submitted $\overline{RID}_i$ to $\mathcal{TA}$ instead of submitting RID_i directly over a public channel. In this manner, the adversary may not be able to distinguish a user among different sessions of the protocol.

6.1.2. Privileged insider attack

An adversary, being an insider, having privileged access to the resources of $\mathcal{TA}$ may access registration request parameters such as RID_i during registration phase. At the same time if the former is also assumed to steal the contents of smart card using power analysis attack. Even then, it may not initiate any kind of privileged insider attack such as password guessing or identity tracing. For this guessing, the adversary will need access to private key d_i as well as biometric key σ_i. Hence, our scheme is resistant to privileged insider attack.

6.1.3. User impersonation attack

An attacker may attempt to impersonate as a user by constructing an authentication request by eavesdropping the original login request $\{\overline{RID}_i, DID_j, \alpha^*, T_i, V_i, X_i\}$ as submitted towards $\mathcal{TA}$. However, after generating a new random integer $\alpha^{'}$ and current time stamp $T_i^{'}$, the parameters $V_i^* = h(ID_j||R_i||\alpha||T_i||RID_i)$, $DID_j^* = ID_j \oplus h(R_i||\alpha||T_i)$ cannot be constructed by the adversary until it has access to R_i. Likewise, to compute $R_i = h(d_{TA}||RID_i)$, it requires d_{TA}, the private key of $\mathcal{TA}$. Similarly, the adversary needs biometric key factor σ_i to compute R_i from R_i^*. Hence, it

is computational infeasible to recover or compute all these required parameters in polynomial amount of time. Thus our scheme is resistant to user impersonation attack.

6.1.4. Cloud server impersonation attack

An adversary may attempt to impersonate as a $\mathcal{CS}_j$ to user by making attempts to reconstruct the message $\{V_{CS_j}, T_j, \beta^*\}$. However, it may not be able to compute this message since it does not have d_j (private key) which is only possessed by $\mathcal{CS}_j$. Hence, even after eavesdropping the contents on open channel, it will be a hard computational problem to reconstruct the same message $\{V_{CS_j}, T_j, \beta^*\}$ with an up-to-date random integer β. Hence, the proposed scheme is free from $\mathcal{CS}_j$ impersonation attack.

6.1.5. Smart meter impersonation attack

Upon eavesdropping previous SM_k requests, an attacker may attempt to impersonate as a smart meter by constructing a valid authentication request $\{\overline{RID}_k, DID_j, a^*, T_k, V_k, X_k\}$ and submitting towards $\mathcal{TA}$. However, to compute a genuine authentication request the attacker needs both identities ID_k as well as ID_j, as well as private key d_k of the smart meter and without $\{ID_k, d_k\}$, SM_k cannot construct a valid request due to hardness problem. Moreover, the adversary has to compute V_{CS_j} and sk_{ij} on reception of reply message and both these also require the values of pair $\{ID_k, d_k\}$ for their computation. Hence, proposed scheme provides immunity to smart meter for any possible smart meter impersonation attack.

6.1.6. $\mathcal{TA}$ impersonation attack

An adversary may attempt impersonating as a $\mathcal{TA}$ after intercepting the messages available on public channel, by constructing a message $\{Y_{TA}, V_{TA}, T_{TA}, RID_j\}$. However, constructing a valid message, an adversary needs to access R_j parameter, i.e. $R_j = h(ID_j||d_{TA})$, which is only known to either $\mathcal{TA}$ or $\mathcal{CS}_j$. If an adversary attempts to replay or reconstruct the message $\{Y_{TA}, V_{TA}, T_{TA}, RID_j\}$, the $\mathcal{CS}_j$ confirms the legitimacy of the source by first decrypting the message using R_j, and afterward checking the equality for $V_{TA} \neq V_{TA}^{'}$. Hence, our scheme is protected from $\mathcal{TA}$ impersonation attack.

6.1.7. Offline password guessing attack

In our scheme, the adversary may not initiate offline password guessing attack even if the former recovers all of the smart card's contents $\{d_i^*, RPW_i, \tau_i, t\}$ using power analysis attack [30, 31] or intercepts the message on public channel. Since, the attacker may not recover password PW_i from either $RPW_i = h(PW_i||ID_i||\sigma_i||d_i)$ or $d_i^* = d_i \oplus h(ID_i||PW_i||\sigma_i)$ or $R_i^* = h(ID_i||RPW_i||\sigma_i||d_i)$ parameters for lacking σ_i, ID_i, d_i. The recovery of ID_i, PW_i and d_i parameters is largely dependent on the availability of biometric factor σ_i, while it is hard to compute it in polynomial amount of time. Hence, our scheme is resistant of offline password guessing attack.

6.1.8. Denial of service attack

Our scheme is resistant of denial of service attack, in case of any wrong input such as ID_i or PW_i into the smart card by user during login phase. This scheme does not permit the smart card to initiate a login request towards $\mathcal{CS}_j$ until the user's input parameters are authenticated with the equality check, i.e. $RPW_i^* \neq RPW_i$. Thus, our scheme is immune to denial of service attack.

6.1.9. Replay attack

In case, the adversary intercepts the messages on public channel and replays towards the intended participants with malicious intent, the former will not be able to initiate this kind of replay attacks due to the time stamp verification at every member's end. It is ensured that the time threshold for timestamps verification should be sufficiently small to legitimately foil this attack. Hence, our scheme is free of replay attack.

6.1.10. Man in the middle attack

In case, an adversary intercepts the login request $\{\overline{RID}_i, DID_j, \alpha^*, T_i, V_i, X_i\}$, it may attempt to modify this message to act as a middle man for attaining its malicious objectives. If it generates a fresh timestamp T_a^*, and attempts to reconstruct $V_i^* = h(ID_j||R_i||\alpha||T_i||RID_i)$, $DID_j^* = ID_j \oplus h(R_i||\alpha||T_i)$ and $\alpha^{**} = \alpha \oplus h(R_i||T_i)$ parameters, it will not be able to construct above mentioned parameters V_i^*, DID_j^*, and α^{**}, since it has no access to R_i parameter. Hence, the attacker can never act as an intermediary into this protocol, and for this our scheme can resist well against this man in the middle attack.

6.1.11. Resilience against smart meter capture attack

If an adversary happens to steal a smart meter $\mathcal{SM}_k$ and recovers information $\{ID_k, d_k, Q_k\}$ from the smart meter's memory, it may compute the session key only for the current smart meter $\mathcal{SM}_k$. It may not compute or extract any session key of other smart meters in the system which are not compromised as the values $\{ID_k, d_k, RID_k\}$ are unique for each smart card. Alternatively, the compromise of any $\mathcal{SM}_k$ does not lead to the revelation of session keys for non-compromised smart meters. In this scenario, the proposed scheme is resilient against this attack.

6.1.12. Session specific temporary information attack

Our scheme is secure against session specific temporary information attack. In this scheme a session key is established between $\mathcal{U}_i$ and $\mathcal{CS}_j$ by computing $sk_{ij} = (\alpha\beta^{'} d_i).Q_j$ and $sk_{ij} = (\alpha^{'} \beta d_j).Q_i$, respectively. The session key security for the proposed scheme is resilient due to its dependency on two factors for establishing the agreed session key, i.e. 1) the ephemeral secrets such as α or β, i.e. In accordance with our proposed model, if temporary short term secrets α or β or both are revealed to the adversary, the latter will not be able to compute the session key between $\mathcal{U}_i$ and $\mathcal{CS}_j$ due to absence of long term secrets as

well. 2) The long term secrets of user such as d_i or d_j, i.e. According to our scheme, if the long term secrets are revealed to the adversary, the attacker may not compute the session key between $\mathcal{U}_i$ and $\mathcal{CS}_j$ due to lacking ephemeral secrets maintained during the session. Both of these parameters are required to construct a session key, while to compute a legitimate session key sk_{ij} by employing any one of the above mentioned factors will be a hard problem in computational terms. Likewise, we may draw an analogous outcome regarding security of session key between $\mathcal{U}_i$ and $\mathcal{CS}_j$ of login and authentication phase. The adversary without the knowledge of ephemeral secrets α or β, and $\mathcal{CS}_j$ or $\mathcal{U}_i$'s private key d_j or d_i may not compute a valid session key, i.e., $sk_{ij} = (\alpha\beta^{'} d_i).Q_j$ or $sk_{ij} = (\alpha^{'} \beta d_j).Q_i$.

6.1.13. TA independent password and biometric update phase

In our scheme, a user may modify its password as well as biometric parameters locally without engaging $\mathcal{TA}$ or $\mathcal{CS}_j$, contributing to low communication overhead.

7. Security and Performance Comparisons

This section elaborates the security and performance contrast of various analogous protocols of [1], [2], [3] and [4]. The Table 3 reveals that our introduced protocol offers invincibility against several familiar attacks. The security comparisons are illustrated in Table 3.

The notation and the corresponding approximate running time as mentioned in [5] is given below

- $T_{pb} \approx 5.811\ ms$: Time to carry out a bilinear-pair mapping
- $T_{mp} \approx 2.226\ ms$: Time to carry out a point multiplication
- $T_{ap} \approx 0.0288\ ms$: Time to carry out a point addition
- $T_{sc} \approx 0.0046\ ms$: Time to carry out symmetric encryption/decryption
- $T_{sh} \approx 0.0023\ ms$: Time to carry out one-way hash function
- $T_{ef} \approx 2.226\ ms$: Time to compute Fuzzy Extractor

Since the time incurred during point addition and XOR operations is insignificant as compared to the rest of the operations defined above. Therefore, these operations and their corresponding time is not considered. Moreover, as per [1] $T_{ef} \approx T_{mp}$. In our protocol smart meter carry out its execution in $2T_{pm} + T_{bp} + T_e + 3T_h$ to authenticate the concerned utility control. Whereas, utility control carry out its execution in $2T_{pm} + 2T_{bp} + T_e + 4T_h$ to perform authentication of corresponding smart meter. The communication costs of proposed and related schemes proposed in [1, 2, 3, 4]is solicited in Table 4. For anaylysis purposes, we have considered the size of identities (actual and pseudo) as 160 *bit*, time stamps are taken as standard 32 *bit* long, random numbers are selected with 160 *bit* length. $SHA-1$ with 160 *bit* length is considered as the used hash function in proposed protocol. The size of elliptic curve cryptosystem is fixed at 160 *bit*. We have considered $AES-128$ as symmetric key algorithms with 128 *bit* block size. The proposed scheme completes the AKA process by transmitting $\{\overline{RID}_i, DID_j, \alpha^*, T_i, V_i, X_i\}$, $\{Y_{TA}, V_{TA}, T_{TA}, RID_j\}$ and $\{V_{CS_j}, T_j, \beta^*\}$ with sizes $\{160 + 160 + 160 + 32 + 160 + 160\} = 832\ bits$, $\{512 + 160 + 32 + 160\} = 864\ bits$ and $\{160 + 32 + 160\} = 35\ bits2$ and the total communication cost in case of proposed scheme is 2048 *bits*. Please note that using a block length of 128 *bits* the $Y_{TA} = E_{R_j}(RID_i||T_{TA}||\alpha||h(R_i||d_{TA}.X_i))$ parameters costs $\{160 + 32 + 128 + 160\} = 480\ bits$ to accommodate 480 *bits*, we need 4 blocks each of 128 bits long totaling it to $128 * 4 = 512\ bits$. The communication cost of the scheme of Challa et al.[1] is 1536 whereas, schemes [2, 3, 4] are having 2528, 2272 and 2560 *bits* communication costs respectively.

8. Conclusion

This article analyzed a recent key agreement scheme involving user and cloud server by Challa et al. as well as its' application in smart meter infrastructure. It is shown that the scheme of Challa et al. is is unable to facilitate the agreement between user/smart meter and cloud server in the presence of more than one registered users/smart meters. Moreover, their scheme lacks untraceable anonymity and lacking the request verification on cloud server side which can led to replay and/or denial of services attack. This article then introduced an improved and secure scheme for facilitating key agreement between user/smart card and cloud server. The security of the proposed scheme is solicited using formal analysis backed by a security features discussion. The proposed scheme provides resistance to the known attacks on the charge of slight increase in computation and communication costs.

References

[1] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, E. Yoon, A. V. Vasilakos, Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems, Future Generation Computer Systems (2018). doi:https://doi.org/10.1016/j.future.2018.04.019.

[2] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. Goutham Reddy, E. Yoon, K. Yoo, Secure signature-based authenticated key establishment scheme for future iot applications, IEEE Access 5 (2017) 3028–3043 (2017). doi:10.1109/ACCESS.2017.2676119.

[3] C. Chang, H. Le, A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks, IEEE Transactions on Wireless Communications 15 (1) (2016) 357–366 (Jan 2016).

[4] X. Jia, D. He, N. Kumar, K.-K. R. Choo, Authenticated key agreement scheme for fog-driven iot healthcare system, Wireless Networks 25 (8) (2019) 4737–4750 (Nov 2019). doi:10.1007/s11276-018-1759-3.

Table 2: Computation Overhead Analysis

Scheme	Smart device/Meter	$\mathcal{TA}$	Cloud-Server	Total	Running Time
Proposed	$3T_{mp} + T_{ef} + 8T_{sh}$	$T_{mp} + 7T_{sh} + Tsc$	$T_{mp} + Tsc + 3T_{sh}$	$5T_{mp} + T_{ef} + 18T_{sh} + +2Tsc$	13.4066 ms
[1]	$T_{mp} + T_{ef} + 10T_{sh}$	$5T_{sh}$	$T_{mp} + 5T_{sh}$	$2T_{mp} + T_{ef} + 20T_{sh}$	6.724 ms
[2]	$5T_{mp} + 5T_{sh} + T_{ef}$	$5T_{mp} + 4T_{sh}$	$4T_{mp} + 4T_{sh}$	$14T_{mp} + T_{ef} + 12T_{sh}$	33.4176 ms
[3]	$4T_{mp} + 12T_{sh}$	–	$9T_{sh}$	$4T_{mp} + 21T_{sh}$	8.9523 ms
[4]	$2T_{mp} + 5T_{sh} + 1Tpb$	$2T_{mp} + 4T_{sh} + 1Tpb$	$3T_{mp} + 9T_{sh} + 1Tpb$	$7T_{mp} + 14T_{sh} + 3Tpb$	33.0472 ms

Table 3: Security Analysis

Scheme→ Security Properties↓	Our	[1]	[2]	[3]	[4]
Scheme Correctness	✓	✗	✗	✓	✓
Prevents Replay Attack	✓	✗	✓	✓	✓
Prevents User Impersonation	✓	✓	✓	✓	✓
Prevents Server Impersonation	✓	✓	✓	✓	✓
Prevents Man-in-the-middle	✓	✓	✓	✓	✓
User Anonymity	✓	✓	✓	✓	✓
User Untraceability	✓	✗	✓	✓	✓
Perfect Forward Secrecy	✓	✓	✓	✓	✓
Provides Biometric verification	✓	✓	✓	✗	✗
Resists Offline Password Guessing	✓	✓	✓	✗	✓
Prevents Stolen Smart Card	✓	✓	✓	✗	✓
Smart Card Revocation	✓	✓	✓	✗	✓
Easy Password Update	✓	✓	✓	✗	✓
Dynamic Node Addition	✓	✓	✓	✗	✓
Provable Security	✓	✓	✓	✓	✓

Table 4: Communication Cost Analysis

Scheme	Messages Exchanged	Bits Exchanged
Proposed	3	2080
[1]	3	1536
[2]	3	2528
[3]	4	2272
[4]	4	2560

[5] H.H. Kilinc , T. Yanik A survey of sip authentication and key agreement schemes. IEEE Commun Surv Tutorials. 16(2):1005-1023, 2014

[6] K. Carruthers, Internet of Things and Beyond: Cyber-Physical Systems, 2016. h ttp://iot.ieee.org/newsletter/may-2016/internet-of-things-and-beyond-cyber physical-systems.html (Accessed on December 4, 2019).

[7] J. Baek, Q.H. Vu, J.K. Liu, X. Huang, Y. Xiang, A secure cloud computing based framework for big data information management of smart grid, IEEE Trans. Cloud Comput. 3 (2) (2015) 233–244.

[8] A. Humayed, J. Lin, F. Li, B. Luo, Cyber-physical systems security–a survey, IEEE Internet Things J. 4 (6) (2017) 1802–1831.

[9] J. Giraldo, E. Sarkar, A.A. Cardenas, M. Maniatakos, M. Kantarcioglu, Security and privacy in cyber-physical systems: A survey of surveys, IEEE Design Test 34 (4) (2017) 7–17.

[10] Y. Ashibani, Q.H. Mahmoud, Cyber physical systems security: Analysis, challenges and solutions, Comput. Secur. 68 (2017) 81–97.

[11] S. Lee, S. Lee, H. Yoo, S. Kwon, T. Shon, Design and implementation of cybersecurity testbed for industrial IoT systems, J. Supercomput. (2017). http://dx.doi.org/10.1007/s11227-017-2219-z.

[12] L. Vegh, L. Miclea, Enhancing security in cyber-physical systems through cryptographic and steganographic techniques, in: IEEE International Conference on Automation, Quality and Testing, Robotics, Cluj-Napoca, Romania, 2014, pp. 1–6.

[13] L. Vegh, L. Miclea, Securing communication in cyber-physical systems using steganography and cryptography, in: 10th International Conference on Communications, COMM'14, Bucharest, Romania, 2014, pp. 1–4.

[14] K.K.R. Choo, M.M. Kermani, R. Azarderakhsh, M. Govindarasu, Emerging embedded and cyber physical system security challenges and innovations, IEEE Trans. Dependable Secure Comput. 14 (3) (2017) 235–236.

[15] F. Hu, Y. Lu, A.V. Vasilakos, Q. Hao, R. Ma, Y. Patil, T. Zhang, J. Lu, X. Li, N.N. Xiong,Robust cyber–physical systems: Concept, models, and implementation, FutureGener. Comput. Syst. 56 (2016) 449–475.

[16] S. Rho, A.V. Vasilakos, W. Chen, Cyber–physical systems technologies and application–Part II, Future Gener. Comput. Syst. 61 (2016) 83–84.

[17] A. Socievole, A. Ziviani, F. De Rango, A.V. Vasilakos, E. Yoneki, Cyber-physical systems for mobile opportunistic networking in proximity (MNP), Comput. Netw. 111 (2016) 1–5.

[18] S. Mehar, S. Zeadally, G. Remy, S.M. Senouci, Sustainable transportation management system for a fleet of electric vehicles, IEEE Trans. Intell. Transp. Syst. 16 (3) (2015) 1401–1414.

[19] A. Mondal, S. Misra, Game-theoretic energy trading network topology control for electric vehicles in mobile smart grid, IET Netw. 4 (4) (2015) 220–228.

[20] S. Misra, S. Bera, T. Ojha, D2P: Distributed dynamic pricing policy in smart grid for PHEVs management, IEEE Trans. Parallel Distrib. Syst. 26 (3) (2015) 702–712.

[21] X. Fang, S. Misra, G. Xue, D. Yang, Managing smart grid information in the cloud: opportunities, model, and applications, IEEE Netw. 26 (4) (2012) 32–38.

[22] N. Kumar, S. Zeadally, S.C. Misra, Mobile cloud networking for efficient energy management in smart grid cyber-physical systems, IEEE Wirel. Commun. 23 (5) (2016) 100–108.

[23] H. Sun, Q. Wen, H. Zhang, Z. Jin, A novel remote user authentication and key agreement scheme for mobile client–server environment, Appl. Math. Inf. Sci. 7 (4) (2013) 1365–1374.

[24] M. Wazid, A.K. Das, S. Kumari, X. Li, F. Wu, Provably secure biometric-based user authentication and key agreement scheme in cloud computing, Secur. Commun. Netw. 9 (17) (2016) 4103–4119.

[25] H. Li, F. Li, C. Song, Y. Yan, Towards smart card based mutual authenticationschemes in cloud computing, KSII Trans. Internet Inf. Syst. 9 (7) (2015) 2719–2735.

[26] H. Zhu, T. Liu, A robust and efficient password-authenticated key agreement scheme without verification table based on elliptic curve cryptosystem, in: International Conference on Computational Aspects of Social Networks, CASoN'10, Taiyuan, China, 2010, pp. 74–77.

[27] C.C. Chang, H.D. Le, A provably secure, efficient, and flexible authentication scheme for Ad hoc wireless sensor networks, IEEE Trans. Wireless Commun. 15 (1) (2016) 357–366

[28] A.K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, X. Huang, Provably secure user authentication and key agreement scheme for wireless sensor networks, Secur. Commun. Netw. 9 (16) (2016) 3670–3687.

[29] R. Amin, N. Kumar, G.P. Biswas, R. Iqbal, V. Chang, A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment, Future Gener. Comput. Syst. 78 (2018) 1005–1019.

[30] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Proceedings of Nine teenth Annual IACR Crypto Conference (Advances in Cryptology) - CRYPTO'99, in: Lecture Notes in Computer Science, vol. 1666, Santa Barbara, California, USA, 1999, pp. 388–397.

[31] T.S. Messerges, E.A. Dabbish, R.H. Sloan, Examining smart-card security under the threat of power analysis attacks, IEEE Trans. Comput. 51 (5) (2002) 541–552.
[32] F. Al-Turjman, Impact of user's habits on smartphones' sensors: An overview, in: HONET-ICT International IEEE Symposium, Nicosia, Cyprus, 2016, pp. 70–74.
[33] F. Al-Turjman, 5G-enabled devices and smart-spaces in social-IoT: an overview, Future Gener. Comput. Syst. (2017). http://dx.doi.org/10.1016/j.future.2017.11.035.
[34] F. Al-Turjman, Y. Kirsal Ever, E. Ever, H.X. Nguyen, D.B. David, Seamless key agreement framework for mobile-sink in IoT based cloud-centric secured public safety sensor networks, IEEE Access 5 (2017) 24617–24631.
[35] I. Elgedawy, F. Al-Turjman, IdProF: Identity provisioning framework for smart environments, in: HONET-ICT International IEEE Symposium, Nicosia, Cyprus, 2016, pp. 12–16.
[36] Z. Chu, H.X. Nguyen, T.A. Le, M. Karamanoglu, D. To, E. Ever, F. Al-Turjman, A. Yazici, Game theory based secure wireless powered D2D communications with cooperative jamming, in: IEEE Wireless Days Conference, Porto, Portugal, 2017, pp. 95–98.
[37] D. Dolev, A. Yao, On the security of public key protocols, IEEE Trans. Inform. Theory 29 (2) (1983) 198–208.
[38] S. Rusitschka, K. Eger, C. Gerdes, Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain, in: First IEEE International Conference on Smart Grid Communications, Gaithersburg, USA, 2010, pp. 483–488.
[39] M. Abdalla, P.A. Fouque, D. Pointcheval, Password-based authenticated key exchange in the three-party setting, in: 8th International Workshop on Theory and Practice in Public Key Cryptography, PKC'05, in: Lecture Notes in Computer Science, vol. 3386, Les Diablerets, Switzerland, 2005, pp. 65–84.
[40] M. Burrows, M. Abadi, R. Needham, A logic of authentication, ACM Trans. Comput. Syst. 8 (1) (1990) 18–36.
[41] Abdalla, Michel, Pierre-Alain Fouque, and David Pointcheval. "Password-based authenticated key exchange in the three-party setting." International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, 2005.

Shehzad Ashraf Chaudhry received the master's and Ph.D. degrees (with Distinction) from International Islamic University Islamabad, Pakistan, in 2009 and 2016, respectively. He is currently working as an Associate Professor with the Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey. He has authored over 75 scientific publications appeared in different international journals and proceedings, including 60 in SCI/E journals. With an H-index of 22 and an I-10 index 39, his work has been cited over 1400 times. He has also supervised over 35 graduate students in their research. His current research interests include lightweight cryptography, elliptic/hyper elliptic curve cryptography, multimedia security, E-payment systems, MANETs, SIP authentication, smart grid security, IP multimedia subsystem, and next generation networks. He occasionally writes on issues of higher education in Pakistan.

Dr. Chaudhry was a recipient of the Gold Medal for achieving 4.0/4.0 CGPA in his Masters. Considering his research, Pakistan Council for Science and Technology granted him the Prestigious Research Productivity Award, while affirming him among Top Productive Computer Scientist in Pakistan. He has served as a TPC member of various international conferences and is an Active Reviewer of many ISI indexed journals.

Taeshik Shon (M'10) received his Ph.D. degree in Information Security from Korea University, Seoul, Korea and his M.S. and B.S. degree in computer engineering from Ajou University, Suwon, Korea. While he was working toward his Ph.D. degree, he was awarded a KOSEF scholarship to be a research scholar in the Digital Technology Center, University of Minnesota, Minneapolis, USA, from February 2004 to February 2005. From Aug. 2005 to Feb. 2011, Dr. Shon had been a senior engineer in the Convergence S/W Lab, DMC R&D Center of Samsung Electronics Co., Ltd. He is currently a professor at the Division of Information and Computer Engineering, College of Information Technology, Ajou University, Suwon, Korea. His research interests include Mobile/Wireless Network Security, WPAN/WSN Network Security, network intrusion detection systems, and machine learning

Prof. Dr. Fadi Al-Turjman received his Ph.D. in computer science from Queen's University, Kingston, Ontario, Canada, in 2011. He is a professor at Near East University, Nicosia, Cyprus. Prof. Al-Turjman is a leading authority in the areas of smart/cognitive, wireless, and mobile networks' architectures, protocols, deployments, and performance evaluation. His publication history spans over 250 publications in journals, conferences, patents, books, and book chapters, in addition to numerous keynotes and plenary talks at flagship venues. He has written and edited more than 25 books about cognition, security, and wireless sensor networks' deployments in smart environments, published by Taylor & Francis, Elsevier, and Springer. He has received several recognitions and best papers' awards at top international conferences. He also received the prestigious Best Research Paper Award from Elsevier Computer Communications Journal for the period 2015-2018, in addition to the Top Researcher Award for 2018 at Antalya Bilim University, Turkey. Prof. Al-Turjman has led a number of international symposia and workshops in flagship communication society conferences. Currently, he serves as the lead guest editor for several well reputed journals, including the Elsevier Computer Communications, Springer MONET, and the IET Wireless Sensor Systems journals.

Mohammed H. Alsharif is currently an Assistant Professor with Department of Electrical Engineering, College of Electronics and Information Engineering, Sejong University, 209 Neungdong-ro, Gwangjin-gu, Seoul 05006, Korea. He received Ph.D. degree in Electrical and Electronic Engineering at the Universiti Kebangsaan Malaysia. His research interests are in information security, wireless communications and networking, including wireless transmission technique such as Orthogonal FrequencyDivision Multiple Access (OFDMA), and energy-efficient wireless communications networks.