Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-020-02349-5

ORIGINAL RESEARCH

ILAS-IoT: An improved and lightweight authentication scheme for IoT deployment

Bander A. Alzahrani[1] · Shehzad Ashraf Chaudhry[2] · Ahmed Barnawi[1] · Wenjing Xiao[3] · Min Chen[3] · Abdullah Al-Barakati[1]

Received: 12 April 2020 / Accepted: 13 July 2020

Abstract

In 2019, Banerjee et al. (IEEE Int Things J 6(5):8739–8752, 2019; https://doi.org/10.1109/JIOT.2019.2931372) proposed an authenticated key agreement scheme to facilitate the session establishment resulting into a session key between a user and a smart device for IoT based networks. As per their claim, the scheme of Banerjee et al. provides known security features and resist all known attacks using only lightweight symmetric key primitives. The analysis in this paper; however, shows that the scheme of Banerjee et al. cannot complete normally. The user in their scheme, after sending a request message may never receive the response from smart device. This incorrectness results into total in applicability of Banerjee et al.'s scheme. Moreover, it is also shown that their scheme has weaknesses against stolen verifier attack. Then an improved lightweight authentication scheme for IoT deployments (ILAS-IoT) is proposed in this article. ILAS-IoT performs the process correctly by increasing very little computation and communication overheads. The proposed ILAS-IoT also resists stolen verifier and all known attacks, which is evident from the formal and informal security analysis.

Keywords IoT · Key establishment · Device access control · Lightweight cryptography

1 Introduction

Internet of Things (IoT) (Shakshuki et al. 2020) has become a trend from previous few years, also through studies (Gubbi et al. 2013; Lu et al. 2020; Thyagarajan and Kulanthaivelu 2020) it is probable to remain in trend in probable future. In IoT system, the data and the information are sensed through IoT devices [e.g., wearable devices, embedded systems, RFID (Radio Frequency Identification) devices] before they are send to some other IoT device, intermediary node/device (e.g., fog or edge computing node) or cloud, thorough Internet. These data are widely used in health care, pattern recognition and other fields (Chen et al. 2019b; Zhang et al. 2020). The applications of IoT comprise the Industry 4.0 also those which are at high risk situations like battlefields and disaster relief. In any prevalent deployment of the consumer technology (Atzori et al. 2010), privacy and the security are main concerns. For better understanding , let's take an application of IoT healthcare (Mukherjee et al. 2020) as an example. In this setting, quality of the health-care (Selvakanmani and Sumathi 2020) related services can be improved by permitting the medical practitioner to have direct access of data that is sensed/collected by body sensor device being

✉ Wenjing Xiao
wenjingx@hust.edu.cn

Bander A. Alzahrani
baalzahrani@kau.edu.sa

Shehzad Ashraf Chaudhry
ashraf.shehzad.ch@gmail.com

Ahmed Barnawi
ambarnawi@kau.edu.sa

Min Chen
minchen@ieee.org

Abdullah Al-Barakati
aaalbarakati@kau.edu.sa

1 Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

2 Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey

3 School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, China

deployed into the patient's body. Such kind of information could comprise recent vital readings (blood pressure, level of blood sugar etc) (Mishra et al. 2020). Important re-medical actions are decided on the basis of this recent information. Undoubtedly, this data and information are confidential and private. Both the user and accessed sensor node need mutual authentication also session key establishment. Explicitly, to facilitate the access of data or services, both the accessed sensor node and user can communicate with each other securely by using created session keys.

To accomplish this aim, very recently, Banerjee et al. (2019) presented a lightweight symmetric key based and secure user authentication protocol with the agreement of session key customized for the IoT environment. They proved the security of their scheme using ROR model (Abdalla et al. 2005) as well as showed the key agreement and authentication using (BAN) logic (Syverson and Cervesato 2000). Despite their claim, the analysis in this paper shows that their scheme has correctness issues because of the incorrectness in their scheme, the login and authentication phase of Banerjee et al. can not complete normally, the user in their scheme , after sending a request message may never receive the response. Moreover, it is also shown that their scheme is vulnerable to stolen verifier attack. Any insider after stealing the verifier can get private keys of the registered participants and can impersonate on behalf of any user of the system. To remove the design flaws, we proposed an improved scheme (ILAS-IoT). The ILAS-IoT securely and correctly completes authentication between a user and a sensing devices with the help of gateway node. The formal analysis of security of ILAS-IoT is carried out through ROR (real-or-random) (Abdalla et al. 2005). Moreover, the informal analysis of security is performed to illustrate that introduced ILAS-IoT is secure against various other communication attacks.

2 Related work

The basic requirements of security which is required in IoT network is similar as needed by other wireless sensor networks (WSNs) (Chen et al. 2018; Mathapati et al. 2020). The requirements required by any wireless networks are named as integrity, authorization, forward and backward secrecy, confidentiality, non-repudiation, authentication and availability. An IoT infrastructure-based user authentication scheme requires to be resilience to attacks such as smart card stolen, offline password guessing, replay, privileged insider, man-in-middle and replay attacks. The curtailed computation and communication cost should also be incorporated by the IoT environment-based user authentication scheme. The scheme should involve efficient password alteration phase that enables the user to locally alter the password without participation of gateway node (GWD). The addition phase of dynamic sensing device is required because an attacker can attack some IoT devices physically or the battery power drains some devices due to limited resources and after primary deployment of the nodes (Karthika and Vidhya Saraswathi 2020), the additional sensor devices are required to place in the network. Suppose a scenario where a medical practitioner (MU) is wandering in the environment of medical IoT. In such environment, the user's confidential information is essential to be secured. For example, the user is prevented for linking his messages or session to other parties by attaining the preservation of user's anonymity. Because, if the identity of user is revealed then the location history and current location of MU can be tracked by any unauthorized user. In other words, one of the numerous basic features of authentication schemes is anonymity of user (He et al. 2015). When the user communicates from one location to other then the track of user must not be followed by an attacker for the purpose of untraceability. This feature is very important in applications of IoT because it make the attacker unable to track the user (Chen et al. 2019c). In distributed systems, the literature has some other studies for remote user authentication, such as privacy, user's anonymity, trust, untraceability and liability (He et al. 2015; Li et al. 2018b; Granjal et al. 2015; Mansoor et al. 2019).

In 2018, it is identified by Makhdoom et al. (2018) that identity management of user is the privacy and security challenge (Zahra and Chishti 2020). Thus, it is compulsory for IoT system-based authentication schemes to offer the features of untraceability and user anonymity. Numerous protocols in this regard have been introduced in last decade in literature. For example, a new authentication scheme is designed by Zhang et al. (2013) for preserving the privacy of user by using only lightweight cryptographic primitives. However, user anonymity is not efficiently offered by their scheme. The two authentication schemes are introduced by Chang and Le (2015). The only hash and bitwise XOR operations are used by first scheme while elliptic curve cryptographic approach is used by the second scheme. In addition, offline password guessing attack and the flaw of breaching the session specific information (Das et al. 2016) is present in both schemes. An enhanced data encryption and authentication mechanism for IoT medical system and RFID (Hsu et al. 2011; Campioni et al. 2019) based system is designed by Li et al. (2017, 2018a).

A test-bed is introduced by Khalil et al. (2014) in which the devices are controlled by using sensors in a smart building. An authentication scheme is developed by Porambage et al. (2014), in which a secure session is established between users and sensors by mutually authenticating each other. Their scheme performs in two stages, and it is scalable with size of network and applicable for deployment on heterogenous resource constrained nodes. However, user anonymity is not preserved by their scheme as determined by Li et al. (2019). The scheme of Wazid et al. also entails correctness issues, as the server will not recognize the specific user who requested for session initiation. A computationally effective scheme is designed by Turkanović et al. (2014), but their scheme is not able to offer untraceability and not able to prevent privileged insider, offline password guessing and impersonation attack. A multilayer system for smart homes security is proposed by Jie et al. (2013). However, Song et al. noticed that large computational overhead on SD_s is present in Jie et al. (2013) due to certificate authority. The limitations are diminished by developing the two authentication schemes by them: (1) hash operation are used by first, (2) chaotic systems are used by other. A signature-based authentication scheme is designed by Chen et al. (2019c) based on elliptic curve cryptography for IoT deployment. However, the utilization of ECC cryptographic functions causes high computation overhead. A user authentication scheme is designed by Amin et al. (2018) for the environment of distributed cloud computing which consists of IoT devices. However, their scheme is vulnerable to several security threats, such as impersonation and privileged insider attack (Challa et al. 2018). Chaudhry et al. (2020), described that both the schemes of Chen et al. (2019c); Challa et al. (2018) are having correctness issues and cannot extend authentication between two entities. A multi factor remote user authentication scheme is designed by Dhillon and Kalra (2017) for IoT infrastructure but properties of user anonymity and untraceability is not offered by their scheme. The authentication schemes are classified by Chaung et al. into two types namely device to device and user to device models. Afterwards, a lightweight authentication scheme is presented by them, but their scheme is not able to offer anonymity of sensing device. A briefed survey on numerous authentication schemes, including schemes for IoT infrastructure, is applicable in Chen et al. (2020) and Ferrag et al. (2017). In literature, various security requirements are not satisfied by various authentication schemes (Hassan et al. 2020; Irshad et al. 2020) and the required functionality features are lacked by them (e.g. untraceability, anonymity, password change procedures and addition of IoT sensing device dynamically). Therefore, our goal is to design a new lightweight user authentication scheme appropriate for IoT environment, which will offer untraceability and anonymity.

2.1 Adversarial model

The common and realistic adversarial model as considered in Dolev and Yao (1983); Ali et al. (2020); Ghani et al. (2019) is adopted for the security analysis purposes. As per model, the $\mathcal{A}$ posses following capabilities:

1. $\mathcal{A}$ administer the communication over public channel. Precisely, $\mathcal{U}_{\mathcal{A}}$ can intercept, modify, replay, and/or insert a new message and can stop anyone.
2. Any user $\mathcal{A}$ registered with *GWD*, can extract data stored in his own smart card issued by the trusted party/*GWD* (Messerges et al. 2002; Kocher et al. 1999).
3. Any insider say $\mathcal{A}$ can expose the verifier information stored in the database maintained by *GWD* (Hao et al. 2020; He et al. 2018; Hussain and Chaudhry 2019).

3 Review of the scheme of Banerjee et al.

Following four phases describe Banerjee et al.'s protocol; whereas, Table 1 is provided for notations used in the paper.

3.1 Setup phase

System parameters are selected in this phase. The gateway node *GN* selects hash $h(.)$, Fuzzy Probabilistic Generation $FGen(.)$, Reproduction $FRep(.)$ functions along with symmetric encryption/decryption $E[.]_k$, $D[.]_k$ algorithms. *GN* further selects the stateless CBC mode of AES algorithm. Finally, *GN* selects it's private key *PKG*.

3.2 IoT device enrollment phase

Any IoT device SD_k can be enrolled dynamically. On a enrollment request, *GN* selects an identity ID_y, a random number r_y and computes $LSK_y = h(PKG \oplus h(ID_y||r_y))$ for requesting device SD_y. The *GN* then loads ID_y and LSK_y in memory of SD_y and deploys it in the system and updates the available devices list by adding SD_y.

3.3 User registration phase

Following steps are performed for registering a user:

Table 1 Notation guide

Notations	Description
U_x, ID_x, SC_x	User, U_x's identity, smart card
PW_x, BIO_x	Password and biometrics of U_x
$\|\|$, $\oplus$	Concatenation, xor
$h(.)$, $\stackrel{?}{=}$	Hash function, checking equality
$E[.]_k/D[.]_k$	Symmetric encryption and decryption using k as key
GN, ID_{gn}	Gateway node, Identity of GN
$FGen()$ $FRep()$	Fuzzy generation and reproduction function
LSK_x	Long term shared key between GN and entity X
PKG	Private key of GN
σ_x, τ_x	Biometric key and reproduction parameter
T_x, ΔT	Time-stamp of entity X, delay tolerance
ΔT_L, $\mathcal{A}$	Life time of EID_x, adversary

$\mathcal{U}_x$	$\mathcal{GWD}$	$\mathcal{SD}_y$
$\{EID_x^*, LSK_x, DList^*, r_x^*, IPB_x, \tau_x\}$	$\{PKG\}$	$\{ID_y, LSK_y\}$

Step BLA-1:
Input ID_x and PW_x
Imprint BIO_x and Compute:
$\sigma_x = FRep(BIO_x, \tau_x)$
$IPB'_x = h(PW_x||h(ID_x||\sigma_x))$
Abort if $IPB_x \neq IPB'_x$
Compute: $r_x = r_x^* \oplus h(ID_x||h(PW_x||\sigma_x))$
$EID_x = EID_x^* \oplus h(ID_x||r_x||PW_x||\sigma_x)$
$LSK_x = LSK_x^* \oplus h(r_x||ID_x||\sigma_x||PW_x)$
$DList = DList^* \oplus h(PW_x||r_x||ID_x||\sigma_x)$
Generate fresh T_x
Compute: $EID_y = E[ID_y||T_x]_{LSK_x}$
$\xrightarrow{M_1=\{EID_x, EID_y, T_x\}}$

Step BLA-2:
Checks freshness of T_x
$(RID_x, x) = D[EID_x]_{PKG}$
Abort if $x \overset{?}{=} h(PKG||RID_x)$
Or $x - T_x > \Delta T_L$
$LSK_x = h(PKG \oplus RID_x)$
$(ID_y, T'_x) = D[EID_y]_{LSK_x}$
If U_x needs to be revoked
$x' = h(PKG||RID_x)$
else $x' = T_{g1}$
$EID'_x = E[RID_x, x']_{PKG}$
Generate x_g
$X_g = h(T_{g1}||x_g)$
$auth = h(LSK_x||X_g||RID_x)$
Set $DList$ accordingly
$D_1 = E[EID'_x, X_g, Dev']_{LSK_x}$
$D_2 = E[auth, D_1, T_{g1}]_{LSK_y}$
$\xrightarrow{M_2=\{D_2, T_{g1}\}}$

Step BLA-3:
Checks freshness of T_{g1}
$(auth, D_1, T'_{g1}) = D[D_2]_{LSK_y}$
Check $T'_{g1} \overset{?}{=} T_{g1}$
Generate y
$D_3 = E[y, T_y]_{auth}$
$SK = h(auth||y)$
$cert = h(SK||T_y||D_1)$
$\xleftarrow{M_3=\{D_1, D_3, cert, T_y\}}$

Step BLA-4:
Verify freshness of T_y
$(EID'_x, X_g, Dev') = D[D_1]_{LSK_x}$
$auth = h(LSK_x||X_g||RID_x)$
$(y, T_y) = D[D_3]_{auth}$
$EID_x^* = EID'_x \oplus h(ID_x||r_x||PW_x||\sigma_x)$
Update $DList$ with Dev', if $Dev' \neq 0$
$DList^* = DList \oplus h(PW_x||r_x||ID_x||\sigma_x)$
$SK' = h(auth||y)$
Check $cert \overset{?}{=} h(SK'||T_y||D_1)$

Fig. 1 The scheme of Banerjee et al

- BUR 1: $\mathcal{U}_x$ selects ID_x, r_x and computes $RID_x = h(ID_x||r_x)$. The $\mathcal{U}_x$ sends RID_x to GN.
- BUR 2: The GN upon reception, computes $LSK_x = h(PKG||RID_x)$ and gets current time stamp x. The GN then computes $EID_x = E[RID_x, x]_PKG$ and imprints the tuple $\{EID_x, LSK_x, DList\}$ in smart card SC_x, where $DList$ defines the available for access, devices in the network for SC_x.
- BUR 3: $\mathcal{U}_x$ upon receiving SC_x, selects PW_x, imprints BIO_x and computes σ_x, τ_x as $(\sigma_x, \tau_x) = FGen(BIO_x)$ along with a verification token $IPB_x = h(PW_x||h(ID_x||\sigma_x))$. $\mathcal{U}_x$ then computes $r_x^* = r_x \oplus h(ID_x||h(PW_x||\sigma_x))$ and inserts r_x^* and IPB_x into SC_x.
- BUR 4: Finally, SC_x replaces $EID_x^* = EID_x \oplus h(ID_x||r_x||PW_x||\sigma_x)$,$LSK_x^* = LSK_x \oplus h(r_x||ID_x||\sigma_x||PW_x)$ and $DList^* = DList \oplus h(PW_x||r_x||ID_x||\sigma_x)$ in it's memory.

3.4 Login & authentication

The login and authentication procedure in Banerjee et al.'s scheme (*BLA*), as illustrated in Fig. 1, can be invoked by a registered user $\mathcal{U}_x$ of the system, when $\mathcal{U}_x$ decides to establish a connection with some IoT device SD_y. Following steps are performed between $\mathcal{U}_x$ and SD_y, for successful completion of this phase:

- BLA 1: $\mathcal{U}_x$ insert SC_x in reader and supplies ID_x, PW_x and BIO_x. $\mathcal{U}_x$ then computes $\sigma_x = FRep(BIO_x, \tau_x)$, $IPB'_x = h(PW_x||h(ID_x||\sigma_x))$. Aborts the session if IPB'_x computed is not equal to IPB_x stored in SC_x; otherwise, SC_x computes $r_x = r_x^* \oplus h(ID_x||h(PW_x||\sigma_x))$ and extracts $EID_x = EID_x^* \oplus h(ID_x||r_x||PW_x||\sigma_x)$, $LSK_x = LSK_x^* \oplus h(r_x||ID_x||\sigma_x||PW_x)$ and $DList = DList^* \oplus h(PW_x||r_x||ID_x||\sigma_x)$. The T_x is generated next and SC_x further computes $EID_y = E[ID_y||T_x]_{LSK_x}$. At end, SC_x sends the request message $M_1 = \{EID_x, EID_y, T_x\}$ to GN.
- BLA 2: Upon reception of M_1, the GN checks the freshness of T_x with a maximum delay tolerance Δt, session is aborted by GN if T_x is not fresh. Otherwise, GN computes $(RID_x, x) = D[EID_x]_{PKG}$. The session is aborted if $x \overset{?}{=} h(PKG||RID_x)$ holds or $x - T_x > \Delta T_L$, both these implies that the access of $\mathcal{U}_x$ has been revoked. GN then computes $LSK_x = h(PKG \oplus RID_x)$ and $(ID_y, T'_x) = D[EID_y]_{LSK_x}$. Now, GN decides about access rights of user, if user needs to be revoked GN set

$x' = h(PKG||RID_x)$ and in normal scenario GN sets $x' = T_{g1}$. The GN then computes $EID'_x = E[RID_x, x']_{PKG}$. Subsequently, GN extracts LSK_y corresponding to ID_y, generates random x_g and computes $X_g = h(T_{g1}||x_g)$, $auth = h(LSK_x||X_g||RID_x)$. Then GN checks if the device access list $DList$ of $\mathcal{U}_x$ has changed in case of dynamic device addition, GN adds the change and in unchanged scenario, GN sets $Dev' = \phi$. Now, GN computes $D_1 = E[EID'_x, X_g, Dev']_{LSK_x}$, $D_2 = E[auth, D_1, T_{g1}]_{LSK_y}$ and sends $M_2 = \{D_2, T_{g1}\}$ to IoT device SD_y.

BLA 3: Once SD_y receives $M_2 = \{D_2, T_{g1}\}$, verifies the freshness of T_{g1} using the delay lag Δt. Upon successful freshness verification, the procedure continues and SD_y computes $(auth, D_1, T'_{g1}) = D[D_2]_{LSK_y}$. Then SD_y checks the equality of received T_{g1} and extracted T'_{g1} from D_2 ($T'_{g1} \stackrel{?}{=} T_{g1}$). Aborts the session in failure scenario. Otherwise, SD_y generates y and computes $D_3 = E[y, T_y]_{auth}$, $SK = h(auth||y)$, $cert = h(SK||T_y||D_1)$ and sends reply $M_3 = \{D_1, D_3, cert, T_y\}$ directly to $\mathcal{U}_x$.

BLA 4: Upon receiving M_3, the user $\mathcal{U}_x$ verifies the freshness of T_y and in case of success, computes $(EID'_x, X_g, Dev') = D[D_1]_{LSK_x}$, $auth = h(LSK_x||X_g||RID_x)$ and $(y, T'_y) = D[D_3]_{auth}$. Then $\mathcal{U}_x$ verifies the equality of received T_y and extracted T'_y from D_3. In success scenario, $\mathcal{U}_x$ computes $EID^*_x = EID'_x \oplus h(ID_x||r_x||PW_x||\sigma_x)$ and updates device list accordingly if $Dev \neq \phi$ and replaces $DList^*$ with $DList^* = DList \oplus h(PW_x||r_x||ID_x||\sigma_x)$. $\mathcal{U}_x$ further computes $SK' = h(auth||y)$ and checks $cert \stackrel{?}{=} h(SK'||T_y||D_1)$, the session key SK is accepted only if the $cert$ equality holds. The $SK' = h(auth||y)$ is the now used to establish the secure session between $\mathcal{U}_x$ and SD_y.

4 Weaknesses of Banerjee et al.'s scheme

The discussion in this section shows that the authentication scheme for IoT by Banerjee et al. is incorrect. Moreover, their scheme is also vulnerable to stolen verifier attack. Following subsections present the weaknesses of Banerjee et al.'s scheme:

4.1 Incorrectness

The login and authentication phase of the scheme of Banerjee et al. can not complete normally, the user in their scheme, after sending a request message may never receive the response. Hence, there may be no authentication at all. The scenario can be depicted as follows:

1. The user say $\mathcal{U}_x$ initiates login request message by computing and sending $M_1 = \{EID_x, EID_y, T_x\}$ to GN.
2. For processing the received request, The gateway device GN computes and sends $M_2 = \{D_2, T_{g1}\}$ to an IoT device say SD_y.
3. SD_y upon reception of $M_2 = \{D_2, T_{g1}\}$ from GN, verifies the validity and then computes response message $M_3 = \{D_1, D_3, cert, T_y\}$ intended for $\mathcal{U}_x$. However, SD_y does not know the identity of $\mathcal{U}_x$ nor it has any established connection with $\mathcal{U}_x$. The situation here is SD_y is sending a message to an unknown entity even without the receiver's address. Moreover, SD_y does not have any established connection with $\mathcal{U}_x$. Therefore, SD_y cannot send any message to $\mathcal{U}_x$ directly.

Hence, Banerjee et al.'s scheme can work when there is one and only user of the system. Such situation is not desirable in any scenario. Specifically, the IoT scenario pre-requisites multiple devices connecting with multiple users on demand. The incorrectness of Banerjee et al.'s scheme leads to its' in-applicability in multiple scenario specially in IoT based deployments.

4.2 Stolen verifier attack

In Banerjee et al.'s scheme, GN stores private key ($LSK_i : \{i = 1 \ldots n\}$) of each device ($ID_i : \{i = 1 \ldots n\}$) in its database/verifier table. These private keys are looked-up during processing of some user request in Step **BLA-2** completed by GN. Such verifiers are subject to stolen verifier attack as mentioned in realistic adversarial model in Sect. 2.1. Any adversary after stealing the verifier can impersonate as any device of the system using the private key of the real device. Therefore, Banerjee et al.'s scheme is susceptible to stolen verifier attack.

5 Proposed ILAS-IoT

We have slightly modified IoT device enrollment phase and some changes are made in login and authentication phases of Banerjee et al.'s proposal; whereas, the user registration, password and biometric update, card revocation and dynamic device addition phases are taken as it is from Banerjee et al.'s scheme. Moreover, in this article an explanation regarding the post authentication, access control phase is also given. The proposed ILAS-IoT as depicted in Fig. 2 is explained in following subsections:

5.1 Setup phase

System parameters are selected in this phase. The gateway node GN selects hash $h(.)$, Fuzzy Probabilistic Generation $FGen(.)$, Reproduction $FRep(.)$ functions along with symmetric encryption/decryption $E[.]_k$, $D[.]_k$ algorithms. GN

$\mathcal{U}_x$	$\mathcal{GWD}$	$\mathcal{SD}_y$
$\{EID^*_x, LSK_x, DList^*, r^*_x, IPB_x, \tau_x\}$	$\{PKG\}$	$\{ID_y, LSK_y\}$

Step PLA-1:
Input ID_x and PW_x
Imprint BIO_x and Compute:
$\sigma_x = FRep(BIO_x, \tau_x)$
$IPB'_x = h(PW_x||h(ID_x||\sigma_x))$
Abort if $IPB_x \neq IPB'_x$
Compute: $r_x = r^*_x \oplus h(ID_x||h(PW_x||\sigma_x))$
$EID_x = EID^*_x \oplus h(ID_x||r_x||PW_x||\sigma_x)$
$LSK_x = LSK^*_x \oplus h(r_x||ID_x||\sigma_x||PW_x)$
$DList = DList^* \oplus h(PW_x||r_x||ID_x||\sigma_x)$
Generate fresh T_x
Compute: $EID_y = E[ID_y||T_x]_{LSK_x}$
$\xrightarrow{M_1=\{EID_x, EID_y, T_x\}}$

Step PLA-2:
Checks freshness of T_x
$(RID_x, x) = D[EID_x]_{PKG}$
Abort if $x \stackrel{?}{=} h(PKG||RID_x)$
Or $x - T_x > \Delta T_L$
$LSK_x = h(PKG \oplus RID_x)$
$(ID_y, T'_x) = D[EID_y]_{LSK_x}$
If U_x needs to be revoked
$x' = h(PKG||RID_x)$
else $x' = T_{g1}$
Generate x_g, $X_g = h(T_{g1}||x_g)$
$auth = h(LSK_x||X_g||RID_x)$
Set $DList$ accordingly
$LSK_y = h(PKG \oplus ID_y)$
$D_1 = E[auth, X_g, T_{g1}, RID_x]_{LSK_y}$
$\xrightarrow{M_2=\{D_1, T_{g1}\}}$

Step PLA-3:
Checks freshness of T_{g1}
$(auth, X_g, T'_{g1}, RID_x) = D[D_1]_{LSK_y}$
Check $T'_{g1} \stackrel{?}{=} T_{g1}$
Generate y
$D_2 = E[y, T_y]_{auth}$
$SK = h(auth||y||RID_x||ID_y)$
$cert = h(SK||T_y||X_g||RID_x)$
$\xleftarrow{M_3=\{D_2, cert, T_y\}}$

Step PLA-4:
$EID'_x = E[RID_x, x']_{PKG}$
Verify freshness of T_y
$EID_{xy} = E[RID_x, T_{g1}, T_{val}]_{LSK_y}$
$D_3 = E[EID'_x, EID_{xy}, X_g, Dev', T_{g2}]_{LSK_x}$
$\xleftarrow{M_4=\{D_2, D_3, cert, T_{g2}\}}$

Step PLA-5:
Verify freshness of T_{g2}
$(EID'_x, EID_{xy}, X_g, Dev', T'_{g2}) = D[D_3]_{LSK_x}$
Check $T'_{g2} \stackrel{?}{=} T_{g2}$
$EID^*_x = EID'_x \oplus h(ID_x||r_x||PW_x||\sigma_x)$
$auth = h(LSK_x||X_g||RID_x)$
$(y, T_y) = D[D_2]_{auth}$
Update $DList$ with Dev', if $Dev' \neq 0$
$DList^* = DList \oplus h(PW_x||r_x||ID_x||\sigma_x)$
$SK' = h(auth||y||RID_x||ID_y)$
Check $cert \stackrel{?}{=} h(SK'||T_y||X_g||RID_x)$

Fig. 2 Proposed ILAS-IoT

further selects the stateless CBC mode of AES algorithm. Finally, *GN* selects it's private key *PKG*.

5.2 IoT device enrollment phase

Any IoT device SD_k can be enrolled dynamically. On a enrollment request, *GN* selects an identity ID_y, a random number r_y and computes $LSK_y = h(PKG \oplus ID_y)$ for requesting device SD_y. The *GN* then loads ID_y and LSK_y in memory of SD_y and deploys it in the system and updates the available devices list by adding SD_y.

Note: In proposed ILAS-IoT, *GN* only stores identities of IoT devices. *GN* does not store private key of any user or IoT device. To avoid stolen verifier attack, we have amended the formation of private key of each device.

5.3 Login & authentication

The login and authentication procedure in proposed ILAS-IoT (*PLA*) can be invoked by a registered user $\mathcal{U}_x$ of the system, when $\mathcal{U}_x$ decides to establish a connection with some IoT device SD_y. Following steps are performed between $\mathcal{U}_x$ and SD_y, for successful completion of this phase:

PLA 1: $\mathcal{U}_x$ insert SC_x in reader and supplies ID_x, PW_x and BIO_x. $\mathcal{U}_x$ then computes $\sigma_x = FRep(BIO_x, \tau_x)$, $IPB'_x = h(PW_x||h(ID_x||\sigma_x))$. Aborts the session if IPB'_x computed is not equal to IPB_x stored in SC_x; otherwise, SC_x computes $r_x = r^*_x \oplus h(ID_x||h(PW_x||\sigma_x))$ and extracts $EID_x = EID^*_x \oplus h(ID_x||r_x||PW_x||\sigma_x)$, $LSK_x = LSK^*_x \oplus h(r_x||ID_x||\sigma_x||PW_x)$ and $DList = DList^* \oplus h(PW_x||r_x||ID_x||\sigma_x)$. The T_x is generated next and SC_x further computes $EID_y = E[ID_y||T_x]_{LSK_x}$. At end, SC_x sends the request message $M_1 = \{EID_x, EID_y, T_x\}$ to *GN*.

PLA 2: Upon reception of M_1, the *GN* checks the freshness of T_x with a maximum delay tolerance Δt, session is aborted by *GN* if T_x is not fresh. Otherwise, *GN* computes $(RID_x, x) = D[EID_x]_{PKG}$. The session is aborted if $x \stackrel{?}{=} h(PKG||RID_x)$ holds or $x - T_x > \Delta T_L$, both these implies that the access of $\mathcal{U}_x$ has been revoked. *GN* then computes $LSK_x = h(PKG \oplus RID_x)$ and $(ID_y, T'_x) = D[EID_y]_{LSK_x}$. Now, *GN* decides about access rights of user, if user needs to be revoked *GN* set $x' = h(PKG||RID_x)$ and in normal scenario *GN* sets $x' = T_{g1}$. The *GN* then computes $EID'_x = E[RID_x, x']_{PKG}$. Subsequently, *GN* computes $LSK_y = h(PKG||ID_y)$ corresponding to ID_y, generates random x_g and computes

$X_g = h(T_{g1}||x_g)$, $auth = h(LSK_x||X_g||RID_x)$. Then GN checks if the device access list $DList$ of $\mathcal{U}_x$ has changed in case of dynamic device addition, GN adds the change and in unchanged scenario, GN sets $Dev' = \phi$. Now, GN computes $D_1 = E[auth, X_g, T_{g1}, RID_x]_{LSK_y}$ and sends $M_2 = \{D_1, T_{g1}\}$ to IoT device SD_y.

PLA 3: Once SD_y receives $M_2 = \{D_1, T_{g1}\}$, verifies the freshness of T_{g1} using the delay lag Δt. Upon successful freshness verification, the procedure continues and SD_y computes $(auth, X_g, T'_{g1}, RID_x) = D[D_1]_{LSK_y}$. Then SD_y checks the equality of received T_{g1} and extracted T'_{g1} from D_1 $T'_{g1} \stackrel{?}{=} T_{g1}$. Aborts the session in failure scenario. Otherwise, SD_y generates y and computes $D_2 = E[y, T_y]_{auth}$, $SK = h(auth||y||RID_x||ID_y)$ $cert = h(SK||T_y||X_g||RID_x)$ and sends reply $M_3 = \{D_2, cert, T_y\}$ directly to $\mathcal{U}_x$.

PLA 4: Upon receiving M_3, the GN verifies the freshness of T_y and in case of success, computes $EID_{xy} = E[RID_x, T_{g1}, T_{val}]_{LSK_y}$ and generates new time stamp T_{g2}. The GN then computes $D_3 = E[EID'_x, EID_{xy}, X_g, Dev', T_{g2}]_{LSK_x}$ and sends $M_4 = \{D_2, D_3, cert, T_{g2}\}$ to $\mathcal{U}_x$.

PLA 5: Upon receiving M_4, $\mathcal{U}_x$ verifies the freshness of T_{g2} and in case of success, computes $(EID'_x, EID_{xy}, X_g, Dev', T'_{g2}) = D[D_3]_{LSK_x}$ and replaces $EID^*_x = EID'_x \oplus h(ID_x||r_x||PW_x||\sigma_x)$. $\mathcal{U}_x$ now computes $auth = h(LSK_x||X_g||RID_x)$, $(y, T_y) = D[D_2]_{auth}$ and updates device list accordingly if $Dev \neq \phi$ and replaces $DList^*$ with $DList^* = DList \oplus h(PW_x||r_x||ID_x||\sigma_x)$. The $\mathcal{U}_x$ further computes $SK' = h(auth||y||RID_x||ID_y)$ and checks $cert \stackrel{?}{=} h(SK'||T_y||X_g||RID_x)$, the session key SK is accepted only if the $cert$ equality holds. $\mathcal{U}_x$ stores dynamic pseudo identity EID_{xy} for subsequent time based access control of SD_y. The $SK' = h(auth||y||RID_x||ID_y)$ is the now used to establish the secure session between $\mathcal{U}_x$ and SD_y.

5.4 Access control phase

This phase as illustrated in Fig. 3, concerns with access control/data collection by an IoT device. The phase is initiated after a successful round of login and authentication (Zhou et al. 2019; Wu et al. 2018) with key agreement between a user $\mathcal{U}_x$ and IoT device SD_y with the help of gateway node GN. $\mathcal{U}_x$ gets access rights for a limited time and a secure session key SK is exchanged between $\mathcal{U}_x$ and SD_y. For access control purposes, $\mathcal{U}_x$ generates fresh time stamp T_{xf} and computes $C_1 = E[m_x, T_{xf}]_{SK}$ and sends $U_m = \{EID_{xy}, C_1, T_{xf}\}$ to SD_y. Upon reception, SD_y verifies the freshness of T_{xf} and on successful verification (Alamer 2020), computes $(RID_x, T_{g1}, T_{val}) = D[EID_{xy}]_{LSK_y}$. SD_y checks the validity of EID_{xy} by verifying the lag between the gateway's time stamp $T_{current} >= T_{val} - T_{g1}$. Upon successful validation SD_y decrypts $(m_x, T'_{xf}) = D[C_1]_{SK}$ and checks $T'_{xf} \stackrel{?}{=} T_{xf}$. On success and as per the required information m_x, the sensor node generates fresh time stamp T_{yf}, encrypts the response data m_y as $C_2 = E[m_y, T_{yf}]_{SK}$ and sends $S_m = \{C_2, T_{yf}\}$ to $\mathcal{U}_x$. The $\mathcal{U}_x$ on receiving S_m verifies the freshness of T_{yf} and on success, computes $(m_y, T'_{yf}) = D[S_m]_{SK}$ and verifies the equality $T'_{yf} \stackrel{?}{=} T_{yf}$. The data m_y is accepted by $\mathcal{U}_x$ on successful verification.

Note: The access rights delegated to $\mathcal{U}_x$ are valid for a certain time and $\mathcal{U}_x$ has to renew its lease once validity expires. This is true depiction of real world IoT objects, where user pays to acquire services for limited time and renews his lease after expiration, like: PayTV system, telecare medical services etc.

6 Security analysis

The formal and informal analysis of ILAS-IoT is presented in this section. To prove the session key security we have used ROR model (Abdalla et al. 2005). Furthermore, informal security analysis shows that the resilience of proposed scheme against realistic attacks.

6.1 Informal security analysis

Here, the security features extended by ILAS-IoT are discussed. The security analysis demonstrates the correctness of ILAS-IoT and highlights that it is secured against various attacks.

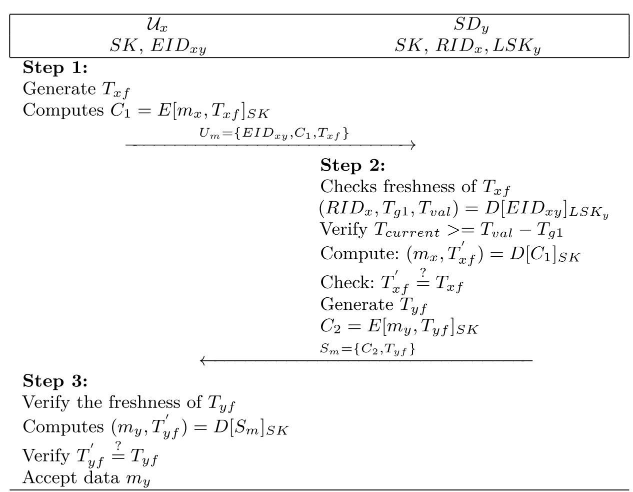

Fig. 3 ILAS-IoT access control phase

6.1.1 Stolen verifier attack

The introduced scheme in this paper is free from storing any database containing verifier. Similarly, there is no database maintained by server. Moreover, the $\mathcal{U}_x$ does not send the password in plain text so insider is not able to exploit and misapply $\mathcal{U}_x$ Password.

6.1.2 User impersonation attack

An attacker $\mathcal{A}$ may attempt to launch user impersonation attack (UIA) to feign as another user say $\mathcal{U}_x$ and for faking purposes, $\mathcal{A}$ may send M_1 (request message) to $\mathcal{GWD}$ by pretending as $\mathcal{U}_x$. The legitimate request $M_1 = \{EID_x, EID_y, T_x\}$ contains timestamp T_x, which can be constructed easily; whereas, to compute $EID_y = E[ID_y \| T_x]_{LSK_x}$, $\mathcal{A}$ needs ID_y and LSK_x, which are secret. Therefore, it may be a failed attempt. Thus, forging M_1 is computationally infeasible and ILAS-IoT provides resilience against UIA.

6.1.3 $\mathcal{GWD}$ impersonation attack

$\mathcal{A}$ may attempt to feign as $\mathcal{GWD}$ by faking the message $M_2 = D_1, T_{g1}$ and may send forged M_2 to some device $\mathcal{SD}_\dagger$. $\mathcal{A}$ can produce T_{g1} freshly on the fly. However, the legitimate $D_1 = E[auth, X_g, T_{g1}, RID_x]LSK_y$ can only be generated if $\mathcal{A}$ has access to shared key LSK_y between $\mathcal{GWD}$ as well as X_g and RID_x which are secret and finding these are computationally infeasible. Thus, forging M_2 is computationally infeasible and ILAS-IoT provides resilience against $\mathcal{GWD}$ impersonation attack.

6.1.4 Smart device impersonation attack (SDIA)

$\mathcal{A}$ may attempt to feign as smart device $\mathcal{SD}_y$ by faking the message $M_3 = D_2, cert, T_y$ and may send forged M_3 to some device $\mathcal{GWD}$. $\mathcal{A}$ can produce T_y freshly on the fly. However, the legitimate $D_2 = E[y, T_y]_a uth$ and $SK = h(auth \| y \| RID_x \| ID_y)$ as well as $cert = h(SK \| T_y \| X_g \| RID_x)$ can only be generated if $\mathcal{A}$ has access to shared key $auth$ as well as LSK_y between $\mathcal{GWD}$ as well as X_g and RID_x which are secret and finding these are computationally infeasible. Thus, forging M_3 is computationally infeasible and ILAS-IoT provides resilience against $\mathcal{SD}_y$ impersonation attack.

6.1.5 Replay attack

For each session timestamps are generated T_x, T_{g1}, T_y if the adversary as a malicious $\mathcal{A}$ intercepts the request message he cant replay it later, because for each session challenge message against request message contain different values.

6.1.6 Smart card stolen attack

The smartcard in proposed ILAS-IoT consists of $\{EID_x^*, LSK_x^*, DList^*, r_x^*, IPB_x\}$. Let $\mathcal{A}$ attempts to verify a guessed PW_x, $\mathcal{A}$ has $r_x^* = r_x \oplus h(ID_x || h(PW_x || \sigma_x))$, inserts r_x^* and IPB_x into SC_x, $EID_x^* = EID_x \oplus h(ID_x || r_x || PW_x || \sigma_x)$, $LSK_x^* = LSK_x \oplus h(r_x || ID_x || \sigma_x || PW_x)$ and $DList^* = DList \oplus h(PW_x || r_x || ID_x || \sigma_x)$ parameters to perform the said task. However, without having the secrets r_x, σ_x and ID_x, $\mathcal{A}$ will have to solve a computationally hard problem to verify the guessed password PW_x. Likewise, $\mathcal{A}$ needs r_x, PW_x , and ID_x to compute σ_x. Hence, even if the smart card is stolen, the attacker will have no benefit to locate the password and/or biometrics.

6.1.7 Provision of user anonymity

In our introduced protocol, ID_x (identity) of $\mathcal{U}_x$ is not being sent in plain text. In-fact $EID_x = EID_x^* \oplus (ID_x, r_x, PW_x, \sigma_x)$ is computed and forwarded over secure channel to $\mathcal{GWD}$. Moreover, only the legitimate $\mathcal{GWD}$ can extract ID_x after having the private key of server $\mathcal{GWD}$. Therefore, our introduced protocol offers user anonymity.

6.1.8 Man-in-the-middle attack

Suppose $\mathcal{U}_A$ intercepts the login message $\{EID_x, EID_y, T_x\}$, still he can not change the login message because the value of EID_x and EID_y is encrypted by private key PKG. So, the ILAS-IoT protocol is secured against Man-in-the-middle attack.

6.1.9 Sensing-device physical capture

$\mathcal{A}$ can capture one or more sensing devices deployed in some hostile environment and the parameters $\{ID_y, LSK_y\}$ stored in each device are subject to expose by power analysis. The $\mathcal{A}$ after accessing $\{ID_y, LSK_y\}$ can only compromise those devices, as this pair of values are unique for each device, Therefore, capturing of one or more devices may not effect the secure communication of non-captured devices with user and gateway.

6.1.10 $\mathcal{GWD}$ bypassing

Through $\mathcal{GWD}$ bypassing, $\mathcal{A}$ by creating some legal message and send it directly to some device or user and the $\mathcal{GWD}$ is bypassed in this scenario. In ILAS-IoT any attacker may attempt to bypass $\mathcal{GWD}$ and send message $M_2 = D_1, T_{g1}$ to some device $\mathcal{SD}_y$. However, as described in Sect. 6.1.3, it has been discussed that forging M_3 is computationally hard problem. Hence, proposed ILAS-IoT resists bypassing $\mathcal{GWD}$.

6.2 Formal security analysis

Before providing the formal security proof, we define the ROR model (Abdalla et al. 2005), which has been used in many schemes (Irshad et al. 2020; Chaudhry et al. 2020; Li et al. 2019; Chen et al. 2019c; Banerjee et al. 2019; Mahmood et al. 2019) for security proofs.

6.2.1 ROR model

The proposed ILAS-IoT involves three entities (1) User $\mathcal{U}_x$, (2) Gateway device $\mathcal{GWD}$ and (3) IoT device $\mathcal{SD}_y$. Following are attached with ROR model, related to the scheme:

A: Participants: Www indicate π^x_{ux}, π^y_{GWD} and $\pi_{SD^z_y}$, where x, y, z are instances that are corresponding to the $\mathcal{U}_x$, $\mathcal{GWD}$ and $\mathcal{SD}_y$. These instances are also offers as oracles.

B: Accepted state: Lets assume that π^z is an instance and π^z represents an accepted state, after disposition of the final message of expected protocol. If all the messages of π^z are managed into series, then it develops current session's identifier *sid* of π^z.

C: Partnering: Two instances, π^{z_1} and π^{z_2} are consider partner if following indicators are fulfilled: i) π^z_1 and π^z_2 will be in accept state. ii) π^{z_1} and π^{z_2} will authenticate each other while having same std; and iii) π^{z_1} and π^{z_2} will be partners.

D: Freshness: We consider the instance either $\pi^x_{U_x}$ and $\pi^y_{SD_y}$ as fresh when SK between $\mathcal{U}_x$ and $\mathcal{SD}_y$ is not exposed to $\mathcal{A}$ with defined Reveal (π^z) query (Chaudhry et al. 2020).

E: Adversary: According to the adversarial model 2.1, $\mathcal{A}$ have full control over all the messages that are being communicated because ROR model is constructed over *DY* threat model (Dolev and Yao 1983). It means that $\mathcal{A}$ can breach, delete and effect integrity of the transmitted messages. Furthermore, following queries are also accessible of $\mathcal{A}$ (Chang and Le 2015).

F: Execute(π^x, π^y, π^z): $\mathcal{A}$ can intercept all the messages among $\mathcal{U}_a$, $\mathcal{GWD}$ and $\mathcal{SD}_y$ by executing this query.

G: Send$(\pi^z$, msg): An active attack can be performed by executing this query. Using Send query can initiate as message as well as receive a response by participating instance π^z.

H: Reveal (π^z): This query helps to reveal the SK computed by π^z to $\mathcal{A}$.

I: CorruptSC $(\pi^x_{U_x})$: With the execution of query, the credentials $\{EID^*_x, LSK_s, DList^*, r^*_x, IPB_x, \pi_x\}$ stored in $\mathcal{U}'s_x$ lost smart card are known to $\mathcal{A}$

J: CorruptSD $(\pi^z_{SD_y})$: This query helps $\mathcal{A}$ to extract credentials $\{ID_y, LSK_y, \}$ from the stolen or captured IOT device $\mathcal{SD}_y$. Both queries *CorruptSD* and *CorruptSC* are assumed to provide weak Corrupt model in which internal data short term key are not Corrupted (Chang and Le 2015).

K: Test(π^z): SK established between $\mathcal{U}_x$ and $\mathcal{SD}_y$ following the in-distinguishabilty of ROR model (Abdalla et al. 2005) can be determine using *Test* (π^z) query. First of all, a coin Cn is needed to be tossed up and then its resultant is available to $\mathcal{A}$. This resultant decides the *Test* query's result. Let suppose $\mathcal{A}$ executes the query. If session key $SK$is fresh than π^z generates SK after the satisfaction off condition $Cn = 1$ or a randomly generated number for the holding of the condition $Cn = 0$ else, it returns null.

According to Chaudhry et al. (2020), $\mathcal{A}$ can access only limited number of *CorruptSD* $(\pi^z_{SD_y})$ and *CorruptSC*$(\pi^z_{SD_y})$ queries. $\mathcal{A}$ cannot make make any corrupt query corresponding to $\mathcal{GWD}$ until the $\mathcal{GWD}$ is trusted. All entities of the scheme including adversary can access hash function h(.). Hash function is modeled as random oracle, termed as $\mathcal{H}$

6.2.2 Security proof

Under the ROR model, proposed ILAS-IoT system's security $\mathcal{P}_s$, is described in Theorem T. It is observed in Wang et al. (2017) that Zipf's law does not represent the passwords in uniform distribution space. Particularly, the size of user's password is much more restricted because user's normally use small space of the allowed character for password (Wang et al. 2017). So, we have applied zipf's law to prove the security of session key in Theorem T.

Theorem T *If $\mathcal{A}$ is an adversary running against P_s, l indicates the total bits in biometric secret key and x and $Advt^{AKE}_{P_s}, A$ is $\mathcal{A}$'s advantage in breaking P_s then $Advt^{AKE}_{P_s,\mathcal{A}} \le \frac{q^2_{hs}}{|Hash|} + 2(\{C', q^{s'}_{sn}, \frac{q_{sn}}{2^l}\} + Advt^{IND-CPA}_{\Omega}(K))$ where q_{hs}, q_{sn} and $|Hash|$ are the $\mathcal{H}$ queries, Send queries and the range of hash function h(.) while the advantage of $\mathcal{A}$ in cracking the $IND-CPA$ symmetric cipher Ω in $Advt^{IND-CPA}_{\Omega}(K) = Advt^{IND-CPA}_{\Omega,SE}(K)$. C' and s' are the zipf's parameter (Wang et al. 2017).*

Proof We use the similar proof of theorem as defined in Wang et al. (2017), with five games $G_x(x = 0, 1, 2, 3, 4)$. Let $Succ^{G_x}_{\mathcal{A}}$ indicates an event where $\mathcal{A}$ can easily guess the random bit b in Game G_x, while the corresponding advantage of $\mathcal{A}$ is $Advt^{G_x}_{P_s,\mathcal{A}} = P_r[Succ^{G_x}_{\mathcal{A}}]$.

Game G_0: This is the first game, which is corresponding to the attack executed by $\mathcal{A}$ in ROR model against ILAS-IoT scheme $\mathcal{P}_s$. Until bit b is chosen from the start of $GameG_0$, it follows the semantic security's definition that

$$Advt^{AKE}_{P_s,\mathcal{A}} = |2Advt^{G_0}_{P_s,\mathcal{A}} - 1| \tag{1}$$

Game G_1: An execute query can made by $\mathcal{A}$, and breaches all the messages $M_1 = \{EID_x, EID_y, T_x\}$, $M_2 = \{D_1, T_{g1}\}$, $M_3 = \{D_2, cret, T_y\}$ and $M_4 = \{D_2, D_3, cret, T_{g2}\}$ transmitted in different phases of the ILAS-IoT scheme. *Test* query is made by $\mathcal{A}$ after finishing of this game. This originality of session key $SK = \{auth\|y\|RID_x\|ID_y\}$ is decided on the basic test query's outcome. In $SK = \{auth\|y\|RID_x\|ID_y\}$ and $Y_g = (T_{g1}\|x_g)T_{g1}$ and x_g are the secret keys chosen by $\mathcal{GWD}$ and $\mathcal{SD}_y$ respectively. So, $\mathcal{A}$ needs the T_{g1}, x_g, X_g, LTK_x and RID_x to calculate the session key SK. All these credentials cannot be derived by $\mathcal{A}$, the probabilities of winning the game is not enhanced. Therefore,

$$Advt^{G_1}_{P_s,\mathcal{A}} = Advt^{G_0}_{P_s,\mathcal{A}} \tag{2}$$

Game G_2: Except *Send* and *H* queries included in G_2, it is distinguishable with respect to G_1 are almost same. The main task of $\mathcal{A}$ in G_2 is to convince the participant that the message is not changed but legitimate. In ILAS-IoT scheme, it is important to note that all the messages M_1, M_2, M_3 and M_4 are made in a way that all are dynamic and no collision occurs in them. As per the work of birthday paradox, it follows

$$|Advt^{G_1}_{P_s,\mathcal{A}} - Advt^{G_2}_{P_s,\mathcal{A}}| \le q^2_{ns}\left(\frac{2}{|Hash|}\right) \tag{3}$$

Game G_3: The simulation of *CorruptSD* and *CorruptSC* are introduced in G_3. $\mathcal{A}$ can got the information $\{EID^*_x, LSK_x, DList^*, r^*_x, IPB_x, T_x\}$ stored in $\mathcal{U}_x$ smart card and $\{ID_y, LSK_y\}$ of captured deice $\mathcal{SD}'_y$. But ID_y and LTK_y are different for non-captured device $\mathcal{SD}_y$. The user $\mathcal{U}_x$ uses biometric and password. The chances of guessing the secret key of biometric σ_x of l bits is almost $\frac{1}{2_l}$[49]. Adversary can also use zipf's law to guess the low entropy password (Wang et al. 2017). While considering the trawling guessing attacks then the advantage of $\mathcal{A}$ will be over 0.5 when $V_{sn} = 10^7$ or 10^8 (Wang et al. 2017). As G_3 and G_4 are similar in the case of guessing attack's absence, so the resultant is as follow:

$$|[Advt^{G_2}_{P_s,\mathcal{A}} - Advt^{G_2}_{P_s,\mathcal{A}}]| \le max\left\{C', q^{s'}_{sn}, \frac{q_{sn}}{2^l}\right\} \tag{4}$$

GAME G_4: The last game of this gaming sequence is G_4 in which $\mathcal{A}$ tries to know the *SK* by breaching the message M_1, M_2, M_3 and M_4 using the decryption of information, EID_x, D_1, D_2 and D_3. In order to obtain the $auth = h(LSK_x\|X_g\|RID_x)$, the decryption of EID_x to get RID_x, the *LTS*, LTS_x and $X_g = h(T_g, x_g)$ is also needed. While the secret key is required to decrypt D_2 and D_3. This task is so expensive due to the usage of CBC version of $AES - 128$ enc/dec. The *IV* value is set as random value, for each encryption and decryption. Due to $IND - CPA$, we get

$$|Advt^{G_3}_{P_s,\mathcal{A}} - Advt^{G_4}_{P_s,\mathcal{A}}| \le Advt^{IND-CDA}_{\Omega}(K) \tag{5}$$

After the execution of all oracles, the only thing remain to guess is bit b for winning the game after querying the *Test* query. So, $Advt^{G_4}_{P_s\mathcal{A}} = \frac{1}{2}$. From equation 1 and 2 we get $(\frac{1}{2})$. $Advt^AKE_{P_s\mathcal{A}} = |Advt^{G_0}_{P_s\mathcal{A}} - \frac{1}{2}| = |Advt^{G_1}_{P_s\mathcal{A}} - |Advt^{G_4}_{P_s\mathcal{A}}|$. The inequality of triangular gives $|Advt^{G_1}_{P_s\mathcal{A}} - Advt^{G_0}_{P_s\mathcal{A}}| \le |Advt^{G_1}_{P_s\mathcal{A}} - Advt^{G_2}_{P_s\mathcal{A}}| + |Advt^{G_2}_{P_s\mathcal{A}} - Advt^{G_4}_{P_s\mathcal{A}}| \le |Advt^{G_1}_{P_s\mathcal{A}} - Advt^{G_2}_{P_s\mathcal{A}}| + |Advt^{G_2}_{P_s\mathcal{A}} - Advt^{G_3}_{P_s\mathcal{A}}| + |Advt^{G_3}_{P_s\mathcal{A}} - Advt^{G_4}_{P_s\mathcal{A}}| \le (\frac{q^2_{ns}}{2}|Hash|) + max\{C'.q^{s'}_{sn}, (\frac{q_{sn}}{2^l})\} + Advt^{IND-CPA}_{\Omega}(k)$. By solving and rearranging Eqs. 3, 4 and 5 we have:

$$Advt^{AKE}_{P_s,\mathcal{A}} \le q^2_{ns}|Hash| + 2\left(max\left\{C'.q^{s'}_{sn}, \left(\frac{q_2}{2^l}\right)\right\} + adv^{IND-CPA}_{\Omega}(K)\right) \tag{6}$$

7 Comparative study

This section presents a comparative study of the introduced scheme with related IoT based schemes in terms of computation and communication complexities and security features/attack resilience provided by these schemes.

7.1 Computation complexity

For computation complexity, T_{oh} donate the time required for one way hash function, $T_{Ec/Dc}$ donate the time required for encryption decryption and T_m donate the time required for point of multiplication. The approximate time required (in milli seconds) to perform the cryptographic operations that

Table 2 Comparison of computation and communication overheads

↓ Protocols/cost →	Computation	Comm.
ILAS-IoT	$20T_{oh}$+ $10T_{Ec/Dc}$= 97ms	4224
Banerjee et al. (2019)	$19T_{oh}$+ $10T_{Ec/Dc}$= 96.5 ms	3296
Li et al. (2019)	$26T_{oh}$+ $8T_{Ec/Dc}$= 82.5 ms	4800
Chen et al. (2019c)	$19T_{oh}$+ $16T_m$= 891.5 ms	3488
Chang and Le (2015)	$20T_{oh}$+ $4T_m$= 263.3 ms	4704

Table 3 Comparison of security features

Protocols→ Features↓	Our	Banerjee et al. (2019)	Li et al. (2019)	Chen et al. (2019c)	Chang and Le (2015)
$\mathcal{SFC}_1$	✓	✗	✗	✓	✓
$\mathcal{SFC}_2$	✓	✓	✓	✗	✓
$\mathcal{SFC}_3$	✓	✓	✓	✓	✗
$\mathcal{SFC}_4$	✓	✓	✓	✓	✓
$\mathcal{SFC}_5$	✓	✓	✓	✓	✓
$\mathcal{SFC}_6$	✓	✓	✓	✗	✗
$\mathcal{SFC}_7$	✓	✓	✓	✓	✓
$\mathcal{SFC}_8$	✓	✓	✓	✓	✓
$\mathcal{SFC}_9$	✓	✓	✓	✓	✓
$\mathcal{SFC}_{10}$	✓	✗	✓	✓	✓
$\mathcal{SFC}_{11}$	✓	✗	✗	–	–

$\mathcal{SFC}_1$ Correctness, $\mathcal{SFC}_2$ user impersonation attack, $\mathcal{SFC}_3$ gateway impersonation attack, $\mathcal{SFC}_4$ IOT smart device impersonation attack, $\mathcal{SFC}_5$ replay attack, $\mathcal{SFC}_6$ smart card stolen attack, $\mathcal{SFC}_7$ user anonymity, $\mathcal{SFC}_8$ man in the middle attack, $\mathcal{SFC}_9$ resilience against sensing device physical capture attack, $\mathcal{SFC}_{10}$ stolen verifier attack, $\mathcal{SFC}_{11}$ access control phase

are used in scheme are taken from the experimental results performed in He et al. (2013) and Jiang et al. (2014) where T_{oh}, $T_{Ec/DC}$ and T_m takes 0.5 ms, 8.7 ms and 63.075 ms, respectively. The Table 2 demonstrates that the proposed ILAS-IoT takes less overall computation complexity then the existing protocols.

7.2 Communication overhead

For communication overhead, it is assumed that arbitrary number, password, P the point multiplication, username and time stamp are 160-bit long, server's public and private key are 256-bits, hash function is 256-bits, Encryption and decryption are 512 bits, the Table 2 summarizes the communication overhead. Although, proposed ILAS-IoT scheme increased some computation and communication costs as compared with Banerjee et al.'s scheme, but in the Table 2 it can be clearly seen that the ILAS-IoT takes less communication cost than most of the existing protocols.

7.3 Security features

Table 3 demonstrates the comparative summary of functionality and security features of our scheme and other related schemes. Proposed ILAS-IoT provides known security features and thwarts all known attacks, the scheme of Banerjee et al. lacks correctness and is vulnerable to stolen verifier attack as mentioned in Sects. 4.1, 4.2. The same incorrectness issue is persistent in Wazid et al.'s scheme, where the gateway generates the user specific credentials without specifying a user. It's important to understand the information (Chen et al. 2019a). The user in Wazid et al.'s scheme sends alias identity and the gateway is having no information to extract his credentials and the scheme (if it is) can work with only a single user. Moreover schemes of Wazid et al. and Banerjee et al. do not provide the access control method. The scheme of Challa et al. is helpless against user impersonation and Chang and Le's scheme is vulnerable to gateway impersonation attack, whereas, both the mentioned schemes are unable to detect replay attack.

8 Conclusion

In this paper, we analyzed a recent lightweight authenticated key agreement scheme presented by Banerjee et al. We have shown that their scheme is not correct and is vulnerable to stolen verifier attack. Moreover, their scheme lacks the description regarding the access control phase. We than proposed an improved and light weight scheme for IoT based deployments (ILAS-IoT). The security of ILAS-IoT is carried out using formal and informal methods. Although, the ILAS-IoT increased some computation and communication overheads as compared with Banerjee et al.'s scheme, but ILAS-IoT provides resistance to all known attacks including stolen verifier attacks and completes the process correctly. Moreover, ILAS-IoT also provides access control mechanism and is more desirable in IoT based access control scenarios.

Acknowledgements This Project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, under grant no. RG-7-611-40. The authors, therefore, acknowledge with thanks DSR for technical and financial support.

References

Abdalla M, Fouque PA, Pointcheval D (2005) Password-based authenticated key exchange in the three-party setting. In: International Workshop on Public Key Cryptography. Springer, Berlin, pp 65–84

Alamer A (2020) An efficient group signcryption scheme supporting batch verification for securing transmitted data in the internet of things. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-02076-x

Ali Z, Chaudhry SA, Ramzan MS, Al-Turjman F (2020) Securing smart city surveillance: a lightweight authentication mechanism for unmanned vehicles. IEEE Access. https://doi.org/10.1109/ACCESS.2020.2977817

Amin R, Kumar N, Biswas G, Iqbal R, Chang V (2018) A light weight authentication protocol for iot-enabled devices in distributed cloud computing environment. Future Gener Comput Syst 78:1005–1019

Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. Comput Netw 54(15):2787–2805
Banerjee S, Odelu V, Kumar DA (2019) A provably secure and lightweight anonymous user authenticated session key exchange scheme for internet of things deployment. IEEE Int Things J 6(5):8739–8752
Campioni F, Choudhury S, Al-Turjman F (2019) Scheduling rfid networks in the iot and smart health era. J Ambient Intell Human Comput 10(10):4043–4057
Challa S, Das AK, Gope EA (2018) Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems. Future Gener Comput Syst 108:1267–1286
Chang CC, Le HD (2015) A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. IEEE Trans Wirel Commun 15(1):357–366
Chaudhry SA, Shon T, Al-Turjman F, Alsharif MH (2020) Correcting design flaws: an improved and cloud assisted key agreement scheme in cyber physical systems. Comput Commun 153:527–537. https://doi.org/10.1016/j.comcom.2020.02.025
Chen M, Miao Y, Jian X, Wang X, Humar I (2018) Cognitive-lpwan: towards intelligent wireless services in hybrid low power wide area networks. IEEE Trans Green Commun Netw 3(2):409–417
Chen M, Hao Y, Gharavi H, Leung V (2019a) Cognitive information measurements: a new perspective. Inf Sci 505:487–497
Chen M, Hao Y, Gharavi H, Leung V (2019b) Label-less learning for emotion cognition. IEEE Trans Neural Netw Learn Syst 31(7):2430–2440
Chen M, Jiang Y, Cao Y, Zomaya AY (2019c) CreativeBioMan: a brain- and body-wearable, computing-based, creative gaming system. IEEE Syst Man Cybernetics Magazine 6(1):14–22. https://doi.org/10.1109/MSMC.2019.2929312
Chen M, Jiang Y, Guizani N, Zhou J, Tao G, Yin J, Hwang K (2020) Living with i-fabric: smart living powered by intelligent fabric and deep analytics. IEEE Netw 1–8
Das AK, Kumari S, Odelu V, Li X, Wu F, Huang X (2016) Provably secure user authentication and key agreement scheme for wireless sensor networks. Secur Commun Netw 9(16):3670–3687
Dhillon PK, Kalra S (2017) Secure multi-factor remote user authentication scheme for internet of things environments. Int J Commun Syst 30(16):e3323
Dolev D, Yao A (1983) On the security of public key protocols. IEEE Trans Inf Theory 29(2):198–208
Ferrag MA, Maglaras LA, Janicke H, Jiang J, Shu L (2017) Authentication protocols for internet of things: a comprehensive survey. Secur Commun Netw 2017, Article ID 6562953
Ghani A, Mansoor K, Mehmood S et al (2019) Security and key management in iot based wireless sensor networks: an authentication protocol using symmetric key. Int J Commun Syst 32:16. https://doi.org/10.1002/dac.4139
Granjal J, Monteiro E, Silva JS (2015) Security for the internet of things: a survey of existing protocols and open research issues. IEEE Commun Surv Tutorials 17(3):1294–1312
Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of things (iot): a vision, architectural elements, and future directions. Future Gener Comput Syst 29(7):1645–1660
Hao Y, Chen M, Cao D, Zhao W, Smeliansky R (2020) Cognitive-caching: cognitive wireless mobile caching by learning fine-grained caching-aware indicators. IEEE Wirel Commun 27(1):100–106
Hassan MU, Chaudhry SA, Irshad A et al (2020) An improved sip authenticated key agreement based on dongqing. Wirel Pers Commun 110(4):2087–2107
He D, Kumar N, Khan MK, Lee JH (2013) Anonymous two-factor authentication for consumer roaming service in global mobility networks. IEEE Trans Consum Electron 59(4):811–817
He D, Kumar N, Chen J, Lee CC, Chilamkurti N, Yeo SS (2015) Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimedia Syst 21(1):49–60
He D, Kumar N, Wang H, Wang L, Choo KR, Vinel A (2018) A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network. IEEE Trans Dependable Secure Comput 15(4):633–645
Hsu HH, Chen BK, Lin CY, Barolli L, Takizawa M (2011) Danger warning via fuzzy inference in an rfid-deployed environment. J Ambient Intell Human Comput 2(4):285–292
Hussain S, Chaudhry SA (2019) Comments on "biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment". IEEE Internet Things J 6(6):10936–10940. https://doi.org/10.1109/JIOT.2019.2934947
Irshad A, Usman M, Ashraf Chaudhry S, Naqvi H, Shafiq M (2020) A provably secure and efficient authenticated key agreement scheme for energy internet based vehicle-to-grid technology framework. IEEE Trans Indust Appl. https://doi.org/10.1109/TIA.2020.2966160
Jiang Q, Ma J, Li G, Yang L (2014) An efficient ticket based authentication protocol with unlinkability for wireless access networks. Wirel Pers Commun 77(2):1489–1506
Jie Y, Pei JY, Jun L, Yun G, Wei X (2013) Smart home system based on iot technologies. In: 2013 International Conference on Computational and Information Sciences, IEEE, pp 1789–1791
Karthika P, Vidhya Saraswathi P (2020) Iot using machine learning security enhancement in video steganography allocation for raspberry pi. J Ambient Intell Humaniz Comput
Khalil N, Abid MR, Benhaddou D, Gerndt M (2014) Wireless sensors networks for internet of things. In: 2014 IEEE ninth international conference on Intelligent sensors, sensor networks and information processing (ISSNIP), IEEE, pp 1–6
Kocher P, Jaffe J, Jun B (1999) Differential power analysis. In: Wiener M (ed) Advances in cryptology – CRYPTO' 99. Springer, Heidelberg, pp 388–397
Li CT, Wu TY, Chen CL, Lee CC, Chen CM (2017) An efficient user authentication and user anonymity scheme with provably security for iot-based medical care system. Sensors 17(7):1482
Li CT, Lee CC, Weng CY, Chen CM (2018a) Towards secure authenticating of cache in the reader for rfid-based iot systems. Peer-to-Peer Netw Appl 11(1):198–208
Li X, Niu J, Kumari S, Wu F, Sangaiah AK, Choo KKR (2018b) A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. J Netw Comput Appl 103:194–204
Li W, Xuelian L, Gao J, Wang HY (2019) Design of secure authenticated key management protocol for cloud computing environments. IEEE Trans Depend Secure Comput. https://doi.org/10.1109/TDSC.2019.2909890
Lu H, Zhang Y, Li Y, Jiang C, Abbas H (2020) User-oriented virtual mobile network resource management for vehicle communications. IEEE Trans Intell Trans Syst. https://doi.org/10.1109/TITS.2020.2991766
Mahmood K, Arshad J, Chaudhry SA, Kumari S (2019) An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure. Int J Commun Syst 32:16
Makhdoom I, Abolhasan M, Lipman J (2018) Anatomy of threats to the internet of things. IEEE Commun Surv Tutorials 21(2):1636–1675
Mansoor K, Ghani A, Chaudhry SA, Shamshirband S, Ghayyur SAK (2019) Securing iot based rfid systems: a robust authentication protocol using symmetric cryptography. Sensors 19:21. https://doi.org/10.3390/s19214752
Mathapati M, Kumaran TS et al (2020) Secure routing scheme with multi-dimensional trust evaluation for wireless sensor network.

J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-02169-7

Messerges TS, Dabbish EA, Sloan RH (2002) Examining smart-card security under the threat of power analysis attacks. IEEE Trans Comput 51(5):541–552

Mishra M, Choudhury P, Pati B (2020) Modified ride-nn optimizer for the iot based plant disease detection. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-02051-6

Mukherjee A, Ghosh S, Behere A, Ghosh SK, Buyya R (2020) Internet of health things (ioht) for personalized health care using integrated edge-fog-cloud network. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-02113-9

Porambage P, Schmitt C, Kumar Pea (2014) Two-phase authentication protocol for wireless sensor networks in distributed iot applications. In: 2014 IEEE Wireless Communications and Networking Conference (WCNC), IEEE, pp 2728–2733

Selvakanmani S, Sumathi M (2020) Fuzzy assisted fog and cloud computing with miot system for performance analysis of health surveillance system. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-02156-y

Shakshuki EM, Malik H, Yasar AUH (2020) Special issue on ubiquitous computing in the iot revolution. J Ambient Intell Human Comput 11(6):2203–2204

Syverson P, Cervesato I (2000) The logic of authentication protocols. In: International school on foundations of security analysis and design. Springer, Berlin, pp 63–137

Thyagarajan J, Kulanthaivelu S (2020) A joint hybrid corona based opportunistic routing design with quasi mobile sink for iot based wireless sensor network. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-02116-6

Turkanović M, Brumen B, Hölbl M (2014) A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. Ad Hoc Netw 20:96–112

Wang D, Cheng H, Wang P, Huang X, Jian G (2017) Zipf's law in passwords. IEEE Trans Inf Forensics Secur 12(11):2776–2791

Wu F, Xu L, Kumari S, Li X, Das AK, Shen J (2018) A lightweight and anonymous rfid tag authentication protocol with cloud assistance for e-healthcare applications. J Ambient Intell Human Comput 9(4):919–930

Zahra SR, Chishti MA (2020) Fuzzy logic and fog based secure architecture for internet of things (flfsiot). J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-02128-2

Zhang P, Lin C, Jiang Y, Fan Y, Shen X (2013) A lightweight encryption scheme for network-coded mobile ad hoc networks. IEEE Trans Parallel Distrib Syst 25(9):2211–2221

Zhang Y, Li Y, Wang R, Hossain MS, Lu H (2020) Multi-aspect aware session-based recommendation for intelligent transportation services. IEEE Trans Intell Transp Syst. https://doi.org/10.1109/TITS.2020.2990214

Zhou Z, Wang P, Li Z (2019) A quadratic residue-based rfid authentication protocol with enhanced security for tmis. J Ambient Intell Human Comput 10(9):3603–3615