An Efficient and Provably Secure Certificateless Protocol for Industrial Internet of Things

Farva Rafique, Mohammad S. Obaidat, *Life Fellow, IEEE*, Khalid Mahmood, Muhammad Faizan Ayub, Javed Ferzund, and Shehzad Ashraf Chaudhry

***Abstract*—The Internet of Things (IoT) has a wide range of applications that influence the life of people expeditiously. In recent years, IoT becomes an emerging technology in a number of fields. Different devices with divergent functionality are applied in IoT to work in several domains. These domains include smart home, smart farming, and Industrial Internet of Things (IIoT). Among these territories, the IIoT obtains more attention. In an IIoT environment, a legitimate user can control and access devices remotely. Legitimate users can access real-time data and share confidential information. The information is transmitted via public communication channel, which can be vulnerable to security attacks. In this article, we present a provably secure multifactor authenticated key agreement scheme to offer security regarding transmission of data in IIoT environment. This scheme will support the legitimate user to remotely access the sensing devices. Our presented scheme uses only symmetric cryptographic, bitwise XOR operation, and hash function to be resource-constrained. Our scheme is found to be resource efficient through communication and computation analysis. The performance analysis illustrates that the cost of computation and communication of our scheme is comparatively low as compared to other relevant schemes. The formal and informal security analysis proved that our scheme is secure and efficient as it can withstand several known adversarial attacks. We have used some cryptographic operations like XOR and hashing to provide security and privacy to legitimate entities.**

***Index Terms*—Authentication protocol, industrial Internet of Things (IIoT), key agreement, smart card.**

Manuscript received 4 January 2022; revised 8 February 2022; accepted 24 February 2022. Date of publication 7 March 2022; date of current version 9 September 2022. Paper no. TII-21-6011. *(Corresponding author: Shehzad Ashraf Chaudhry.)*

Farva Rafique, Muhammad Faizan Ayub, and Javed Ferzund are with the Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus 57000, Pakistan (e-mail: farva.rafique77@gmail.com; faizanayub9@gmail.com; jferzund@cuisahiwal.edu.pk).

Mohammad S. Obaidat is with the Indian Institute of Technology—Dhanbad, Dhanbad 826004, India, with KAIS, University of Jordan, Amman 11942, Jordan, and also with the PR of China Ministry of Education, University of Science and Technology Beijing, Beijing 100083, China (e-mail: msobaidat@gmail.com).

Khalid Mahmood is with the Future Technology Research Center, National Yunlin University of Science and Technology, Yunlin 64002, Taiwan with the Riphah School of Computing and Innovation (RSCI), Riphah International University, Lahore Campus, Lahore 55150, Pakistan, and also with the Department of Mathematics, University of Padua, 35131 Padua, Italy (e-mail: khalidm.research@gmail.com).

Shehzad Ashraf Chaudhry is with the Department of Computer Engineering, Faculty of Engineering and Architecture, Nisantasi University, Istanbul 34398, Turkey (e-mail: ashraf.shehzad.ch@gmail.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2022.3156629.

Digital Object Identifier 10.1109/TII.2022.3156629

I. Introduction

THE Internet of Things (IoT) is composed of numerous sensing devices and controllers connected physically with various functionality. Physical devices may include drones, sensors, cameras, vehicles, smart phones, and also they can be virtual objects like books, agenda, wallets, or electronic tickets. These devices are interlinked through the network to bestow copious services like data analysis, data acquisition, and real-time monitoring [1]. In IoT environment, the devices must be as smart as they are able to take decisions without intervention of human. IoT has numerous applications such as in agriculture, medical treatment, surveillance, and housing. Moreover, IoT has appreciable endowment to industrial field, which is also called Industrial Internet of Things (IIoT) [2]. To upgrade the manufacturing efficiency and acquiring intelligent industrial production, the IIoT allows us to control the industrial production, manage efficiently, and monitor automatically. The IIoT can be applied in number of industries such as in utilities, metals and mining, manufacturing, gas, oil, logistics, aviation, and transportation. IIoT is an imperitive part of the IoT environment that needs more security for the communication and data transmission [3]. Generally, the data gathered through IoT devices are transmitted through an open channel that is unprotected and susceptible to various attacks by illegitimate user. The illegitimate user can access the sensing devices for real-time data and becomes the reason for challenges to privacy and security in IIoT [4], [5]. In IIoT-based environment, numerous authentication schemes have been presented. In IIoT, there are three types of entities (user, Gateway node), and IoT devices are usually used in these types of authentication schemes. Having limited storage, energy, and computing resources, IoT devices typically become unreasonably resource-constrained to work with complex types of cryptographic primitives.

Therefore, a lightweight and secure authenticated key agreement protocol is needed to tackle security and privacy issues in the IIoT. GWN can handle more computing operations than IoT devices because it has vigorous resources, which make it more efficient [6], [7]. The legitimate user communicates to GWN using IoT devices via a public channel, which can be susceptible to security attacks. Furthermore, sensor nodes are capable of computing using limited storage space. These sensors collect

treasured information and send it through insecure channel. Many authentication schemes have been developed using ECC in order to generate session key between IoT devices and legitimate users securely [8]. Therefore, in this article, we propose lightweight authentication and key agreement scheme to reduce the computation and communication costs using fuzzy extractor algorithm in order to fulfill the requirements of resource constrained environment and to resist the known attacks.

II. Related Work

Recently, numerous authentication and key agreement schemes have been presented for IoT environments. These schemes are designed to steer the privacy and security issues. It is pivotal to protect the security and privacy of data while holding up for security traits and avoid known attacks. Various factors used in existing schemes such as smart cards, passwords, and biometrics to validate legitimate users. In industrial production monitoring, wireless sensor networks mainly act as a key factor for IIoT.

Choudhary *et al.* [9] introduced key exchange model and a lightweight remote user's mutual authentication for IIoT. Proposed scheme of Choudhary *et al.* [9] provides security features like integrity, data confidentiality, and identity anonymity. Moreover, it provides security against popular attacks (modification attack, replay attack, man in the middle attack, etc). However, this scheme is still vulnerable to internal security threats of IIoT networks. Fang *et al.* [10] go through numerous IIoT control systems and their issues as well as the security vulnerabilities of IIoT control system in details. Existing endeavor are unable to establish an uniform security mechanism for IIoT control systems due to diversity and complexity of the protocols. However, Fang *et al.* [10] has no proper framework and applicable secure authentication scheme to prevent security threats. Gu *et al.* [11] introduced authentication mechanism for an active physical layer. This mechanism is for noncoherent SIMO-based IIoT system. This is the first work to demonstrate active PLA to accomplish without using the channel estimation and pilot signal. Furthermore, the suggested authentication scheme can match the IIoT systems error rate and specific power requirements.

For secure communication between sensors and routers in IIoT, Baruah *et al.* [12] introduced a secure authentication scheme. Using AVISPA tool and BAN logic, the security of the proposed schemes are examined. The performance of the proposed schemes is studied and compared with state-of-the-art authentication schemes to establish its viability. This scheme still has limitations regarding authentication of sensor and router in IIoT. To broadcast scalable and secure M2M communications, which is based on pub/sub paradigm, Amoretti *et al.* [13] presented a unique dynamic multibroker framework. In addition, Amoretti *et al.* [13] aimed to put the proposed architecture into a new context for challenging real world IIoT applications. The scenarios of IIoT applications are cloud manufacturing and predictive maintenance. Regardless of their work, they still need to develop their framework to provide effectiveness regarding numerous physical cyber-attacks. These attacks are specially related to communication between third party and machine's authorization and authentication process. Karati *et al.* [14] presented a certificateless signature scheme in 2018. The scheme is presented to ensure the integrity of data in IIoT. Even so, Zhang *et al.* [16] claimed that the scheme of Karati *et al.* [14] is susceptible to a signature forgery attack. Afterthat, to preserve the reliability of IIoT data, Zhang *et al.* [16] presented a robust CLS cloud-assisted scheme. The security analysis of the scheme revealed that their scheme is resistant to signature forgery and four other CLS attacks. Rezaeibagha *et al.* [15] claimed that Karati *et al.* [14] scheme is also sensitive to signature forgery. Rezaeibagha suggested a new CLS scheme that is considered safe against both types of adversaries. Zhang *et al.* [15] claimed that Karati *et al.* [14] is unable to achieve the claimed security goals. They proved their claim by presenting forgery attacks of four types on Karati *et al.* [14] CLS scheme. They presented a robust certificateless signature scheme, which is devoid of ROM and MTP to explain the challenges described in cloud-assisted IIoT. They prove that their scheme is secure from these four types of attacks and robust in nature. Peng *et al.* [17] also proposed a novel certificateless online/offline signature scheme and design an efficient authentication protocol for the wireless body area networks. Compared with related protocols, their protocol has the much less computation cost.

To come up with more services of IoT, Yu *et al.* [18] combined IoT with cloud computing. But, a number of known attacks are there that threaten cloud user and server security. They presented an enhanced scheme for cloud computing environment based on IoT, which is resistant to DoS attack and privileged insider attack. By using BAN-logic automated verification of security, they proved security of their scheme. For IoT-based WSN, Haseeb *et al.* [19] presented a stable as well as consistent sensor-cloud based architecture. It offers efficient and secure services of communication in smart cities to address the security vulnerability triggered by sensor node failure. In this article, an authenticated multifactor key agreement scheme is introduced, which is distinct from the numerous current schemes reported in the literature. First, using a simple hash function along with XOR operation significantly reduced the computing complexity of accessing single and multiple devices. Second, they proposed a scheme that enables sensing devices seamlessly enter and exit from IIoT network. It reduces communication costs to help users to access different sensing devices. On the other hand, it lacks of robust security for multihop communication, lack of trusted end-to-end routing delivery for longer regions and also have no repudiation and playback network attacks.

Table I summarizes several existing schemes with respect to their cryptographic primitives used, benefits and drawbacks/flaws.

A. Article Organization

The notations are provided in Table II. Section II presents the related work and Section III deals with the problem statement.

TABLE I
SUMMARIZING EXISTING SCHEMES IN IIoT

Protocol	Cryptographic Primitives	Benefits	Drawbacks/Flaws
Zhang *et al.* [16]	∗ RCLS without using hash function and ROM ∗ Partial private key	∗ Provide tight security ∗ Public key replacement	∗ Computational cost is high
Karati *et al.* [14]	∗ CLS ∗ Bilinear pairing ∗ Provable security	∗ Resist from both TYPE I and TYPE II ∗ Recover authenticity issue in IIoT ∗ Provide intractability ∗ Light weight	∗ Lack of data authenticity ∗ Untrustworthy for third parties ∗ Unable to provide efficiency and robustness
Haseeb *et al.* [19]	∗ Routing protocol ∗ Hash & VOR operations ∗ Multifactor authentication	∗ Secure communication ∗ Computing complexity reduced ∗ Reduce communication cost	∗ Lacks for the robust security for multi hope communication ∗ No repudiation and playback network attacks ∗ Lack of trusted end-to-end routing delivery for longer regions
Wang *et al.* [20]	∗ WSN, Smart card ∗ Two factor authentication	∗ Provide distributed lightweight sensor nodes ∗ Real time data acquisition	∗ Unable to provide user anonymity ∗ Unable to provide mutual authentication

TABLE II
NOTATIONS AND DESCRIPTIONS

Notations	Description	Notations	Description
GWN	Gateway Node	ID_{GWN}	GWN's identity
U_i	i^{th} user SD_j	j^{th}	sensing device
ID_i	U_i's identity	ID_{SD_j}	SD_J's identity
r_{GWN}	Random nonce	B_i	U_i's biometrics
PW_i	U_i's password	BK_i	U_i's biometric key
$Gen(.)$	Generation algorithm	$Rep(.)$	Reproduction algorithm
KEY_{GWN-U_i}	Symmetric key	S	Secret value sharing
ECC	Elliptic Curve Cryptography	$SIMO$	single-input multiple-output
PLA	physical layer authentication	CLS	Certificateless

Sections IV presents registration phase, login phase, authentication, and key agreement phase of proposed scheme. Section V shows the detailed security analysis of our scheme. In Section VI, the performance analysis of our scheme is explained. Section VII concludes this article.

B. Motivation and Contribution

In recent years, numerous studies regarding security as well as privacy issues in IIoT environment have been reported [1]. The communication of IIoT devices is done via public channel. So, these communications are vulnerable to numerous attacks. As a result, illegitimate users can access sensitive information regarding industrial production. So, to validate a user's identity, there is a need to establish a more secure mechanism. Furthermore, in already existing schemes, users can access a sole IoT device simultaneously [21]. Users need to validate repeatedly to get access to the numerous sensing devices. There is a need to design a multifactor key agreement protocol, so that users can access numerous sensing devices at a time to create session keys between them.

III. PROBLEM STATEMENT

The problem will be stated in this section using the three features, these are threat model, network model, and security goals.

A. Threat Model

In our scheme, U_A is assumed to have the same capabilities as the attacker used: CK-adversary [22] and Dolev–Yao (DY) threat model [23]. In DY model, both users and sensing devices are deemed untrustworthy, and any entity can send and receive messages via an open channel. Any two entities message can be altered, eavesdropped, intercepted, and deleted by U_A. U_A can also counterfeit messages into a legal entity to deceive it.

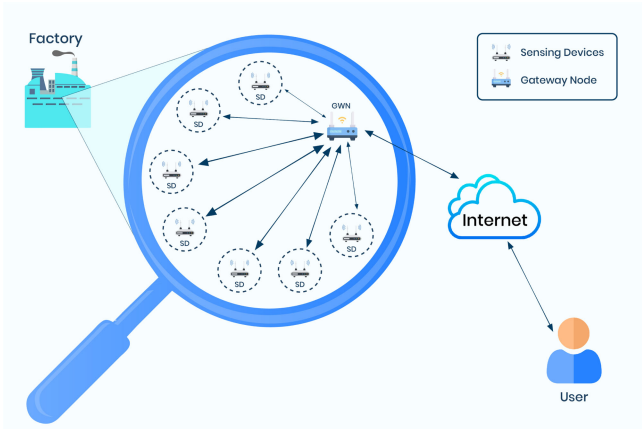

Fig. 1. IIoT environment.

U_A can also receive and transmit messages by impersonating communication between U_i and SD_j. In IIoT, the GWN is the most important factor. It is deemed completely trustworthy and can not be harmed by U_A. First, in a protected environment the GWN is physically secure. Second, the tamper-resistance mechanism ensures that in GWN any stored information is not accessible by the adversary [24]. The CK-adversary model not only shows the characteristics of an adversary in the DY model, but it also exposes some session secrets between participants who are communicating with each other [22]. As a result, if the previous temporary secrets or session keys are revealed during communication, the adversary can not violate the scheme's security.

B. System Architecture

In system architecture of IIoT, the design is depicted in Fig. 1. In this design, there are three types of entities.

1) Users: Using the smart card, the user can send request via GWN to get access from sensing devices
2) Sensing devices: These devices are used in IIoT to investigate the collection of data and manufacturing status. The information acquired by sensing devices can easily be accessed in real-time by the user.
3) GWN: GWN is a fully trusted entity in our model, it is in charge of registering between sensing devices and users.

In our presented scheme, the SD_js are registered through GWN and GWN stores some secret credentials into their memory. To gain access to sensing devices in IIoT, a user must be registered in GWN and store the credentials for authentication

into the memory of user devices. First, the U_i sends request to GWN for authentication during the login and authentication key agreement phase, after validating the authenticity of the user, GWN sends the request message to sensing devices. After that, to recreate the secret value, the sensing devices communicate their credentials with GWN. Sensing devices acquire the secret value from GWN and produce the shared session key before transmitting messages to U_i. At last, the user can access data that is gathered via sensing devices and then use these sensing devices to regulate the industrial production process.

IV. Proposed Scheme

In this section, we present the proposed protocol. Our protocol consists of two phases, registration phase, login, and authentication phase. First, registration phase is discussed and then login and authentication phase is explained.

A. Registration Phase: When users require to access sensing devices securely, U_i must first register in a GWN via a reliable channel. We explain the registration phase of U_i in steps which are given as follows:

Step URP 1: U_i chooses a unique identity as ID_i and password as PW_i. U_i then imprints his/her biometric B_i into the device. Then, using fuzzy extractor biometric key BK_i is obtained and calculated variables will be $(BK_i, \tau_i) = Gen(B_i)$, where $Gen(.)$ is a function which is called when user need to generate key from bios. U_i randomly generates a nonce of 128-bit and computes $TPW_i \leftarrow h(\{PW_i \| ID_i \| BK_i\}) \oplus a$. After that, BK_i securely sends message having values ID_i, TPW_i to GWN.

Step URP 2: When obtaining the request $\langle ID_i, TPW_i \rangle$, GWN generates randomly a secret key of 1024-bit as KEY_{GWN} and calculates $KEY_{GWN-U_i} \leftarrow h(ID_i \| KEY_{GWN-U_i})$, $A_i \leftarrow KEY_{GWN-U_i} \oplus TPW_i$, $C_i \leftarrow ID_{GWN} \oplus TPW_i$, TID_i for U_i as $TID_i \leftarrow ENC_{KEY_{GWN}(ID_i \| R_o)}$. After that, GWN generates SC_i. SC_i stores $\{TID_i, A_i, C_i, h()\}$ for each U_i and passes the SC_i to U_i.

Step URP 3: After receiving SC_i, U_i calculates $RPW_i \leftarrow h(ID_i \| PW_i \| BK_i)$, $A'_i \leftarrow A_i \oplus TPW_i \oplus RPW_i$, $D_i \leftarrow a \oplus h(ID_i \| BK_i)$, $C'_i \leftarrow C_i \oplus TPW_i \oplus h(ID_i \| BK_i)$, $V_i \leftarrow h(RPW_i \| A_i \| a \| h(ID_i \| BK_i)) \; mod \omega$. It is calculated to validate the legal user's identity, whereas, ω is a medium integer. At last, $\{TID_i, A'_i, C'_i, V_i, D_i, Rep(.), h(.), Gen(.), \omega, \tau_i\}$ is stored in U_i's memory and already stored information is discarded.

D. Login Phase: Whenever U_i wants to get the data of SD_j using his/her identity ID_i, the following authentication and key agreement steps are performed among U_i, GWN, and SD_j. The process for further communication is given as follows:

Step LP 1: The U_i inserts the SC_i and imprints the biometric B_i^* into the card reader. Then input ID_i and PW_i. The SC_i computes $BK_i^* \leftarrow Rep(B_i^* \| \tau)$, where $Rep(.)$ is also a function which is called when user needs to reproduce the secret key from helping data and bios. Using the U_i credentials as well as the information stored in the SC_i, SC_i calculates $RPW_i^* \leftarrow h(PW_i \| ID_i \| BK_i^*)$, $a^* \leftarrow D_i \oplus h(ID_i \| BK_i^*)$ and $A_i^* \leftarrow A'_i \oplus a^*$. SC_i, $V_i^* \leftarrow h(RPW_i^* \| A_i^* \| a^* \| h(ID_i \| BK_i^*)) mod \omega$. It checks whether $V_i \leftarrow V_i^*$ to authenticate the identity of U_i.

Step LP 2: As the authentication of U_i is successful, SC_i creates a random nonce r_i and a timestamps TS_1. Then, SC_i computes $ID_{GWN}^* \leftarrow C'_i \oplus h(ID_i \| BK_i)$, $M_1 \leftarrow h(KEY_{GWN-U_i} \oplus r_i)$, $M_2 \leftarrow h(TID_i \| M_1 \| ID_{GWN}^*) \| r_i \| TS_1$ and transfers the message $\{TID_i, M_1, M_2, TS_1\}$ to GWN.

C. Authentication and Key Agreement Phase

The complete process of authentication and key agreement is described in Fig. 2.

V. Security Analysis

We will discuss the security analysis of the proposed authentication scheme. As security analysis is done to check the robustness, invincibility, validity, and level of provided security of our scheme. It has been cleared that the security of presented scheme remains in diverse circumstances. We used the approach of security analysis followed in [25]. There are basically two sections of security analysis, which are formal and informal. The formal security analysis is described as follows.

A. Formal Security Analysis Using Real or Random Model

In this section, the formal security analysis of our scheme with the help of a widely used ROR model is introduced. The main motive is to assure the security of session key in this scheme under the ROR model. This model is given in theorem 1. This theorem uses one way cryptographic hash function with the IND-CPA. The description of ROR model is as follows:

ROR Model: In this network, there are three participants named as user U_i, gateway node GWN, and sensing device SD_j. Moreover, there are different components of ROR model described as follows.

Participants: $\Pi_{\mathrm{SD}_j}^t$, $\Pi_{U_i}^u$, Π_{GWN}^v denote the instances *t*, *u*, *v* of the participants SD_j, U_i, and GWN, which are shown as oracles.

Partnering: Π_{U_i} of U_i is a partner of $\pi_{\mathrm{SD}_j}^t$ of SD_j and vice-versa. The current session identity is unique as $\Pi_{U_i}^u$ participates in it. It is also known as the partial transcription of all transmitted messages among U_i and SD_j.

Freshness: $\Pi_{U_i}^u$ or $\Pi_{SD_j}^t$ is called fresh if the $\{SK = SK^*\}$ between U_i and SD_j can not be disclosed by U_A seeking the help of given reveal query $(\Pi^t)U_A$. In this model, U_A can control all the communication in which reading and modifications of all transmitted messages are included. These queries can easily be accessed by U_A.

Execute: This is useful for retrieving messages sent between two legitimate participants. It is represented as the eavesdropping attack.

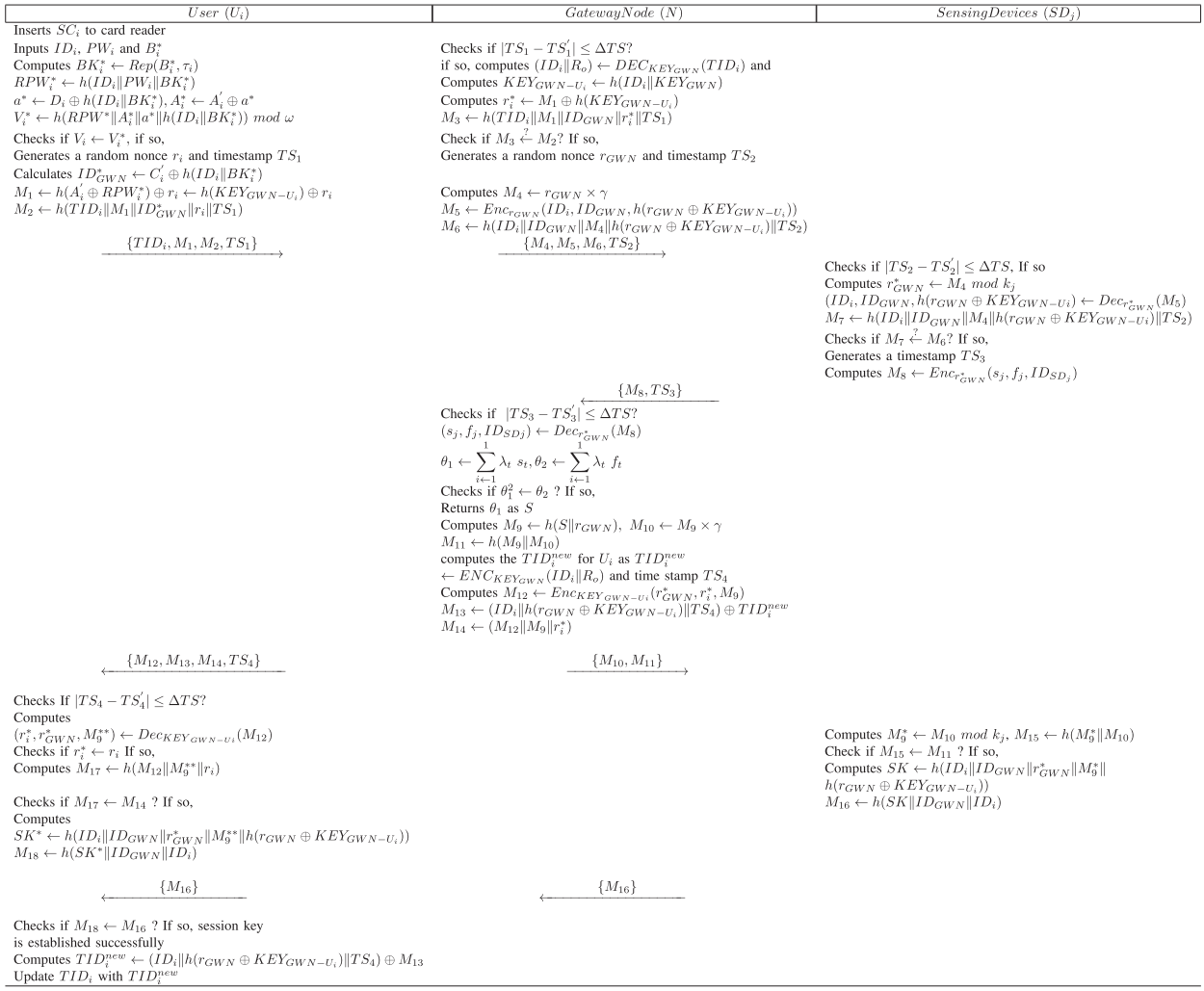

Fig. 2. Authentication and key agreement phase of proposed scheme.

Exchange (Π^t, Msg): The exchange model is used to represent an active attack. In this model, participant π^t can receive, send, and respond to the messages.

Reveal (Π^t) : In this query, U_A gets session key, which is computed by Π^t (and its partner).

Corrupt ($\Pi_{U_i}^t$)*:* In this query, U_A steals the U_i's smart card SC_i to extract secret credentials stored in it.

Corrupt ($\Pi_{\text{SD}_j}, MAKA$)*:* In this mode, secret credentials $(ID_{\text{SD}_j}, s_j, k_j, f_j)$ of SD_j are revealed to U_A.

Test ($\Pi_{U_i}^t$)*:* The SK follows the uniformity in ROR model. In the beginning of the experiment, a coin is flipped and only U_A knows the result. The output of test query is decided by U_A.

Semantic Security of the SK: In the ROR model, it is necessary for U_A to discriminate the real SK from the random key instances. U_A can create a number of test queries for $\Pi_{\text{SD}_j}^t$ or $\Pi_{U_i}^u$. Before termination of the game, U_A guesses a bit a'. We use ROR model to demonstrate the security aspects of our scheme.

Theorem 1: It is supposed that in random oracle, U_A is the adversary against our scheme Prb running in probabilistic polynomial time. According to Zipf's law [26], let $|Dic_p|, Dic_p, |Hsh|, len$, q_{hsh}, q_{exe}, and q_{snd} show the password range space along with its frequency distribution, the number of sent oracles, size of Dic_p, hash function with the range space, the bit length of BK_i, the number of executed oracles and the number of hash oracle, respectively. Moreover in PPT, the advantage of U_A breaking the symbolic security of Prb can be defined as follows:

$$\text{Advt}_{R,U_A}^{\text{MAKA}}(K) \leq \frac{q_{hsh}^2}{|Hsh|} + 2\text{max}\left(B'.q_{\text{snd}}^{s'}\frac{q_{\text{snd}}}{2^{\text{len}}}\right) + \frac{2}{q}.\text{Advt}_{R,U_A}^{\text{IND-CPA}}(K). \quad (1)$$

Proof: The security proof of our scheme is in a way similar to the one shown in [24]. In the scheme, there are five games $Game_n$, $n \leftarrow 0, 1, 2, 3, 4$. If U_A guesses successfully a bit b before the game, then it is known as $Succ_n$. The complete definition of each $Game_n$ is described as follows.

$Game_0$*:* The real attacks to our proposed authenticated scheme Prb are modeled in this game. At the start of $Game_0$,

the U_A guesses the bit b. From the theorem

$$\text{Advt}^{\text{MAKA}}_{R,U_A}(K_i) \leftarrow |2P_r[\text{Succ}_0] - 1|. \quad (2)$$

$Game_1$: In this game, the man-in-the-middle attack is launched by U_A during the phase of login and authentication of scheme. At the end of $Game_1$, U_A tests oracles running as $(\pi_1^t, \pi_2^t, \pi_3^t)$. U_A requires to differentiate either output of the test oracles is a random string or a real SK. In our scheme, U_i and SD_j calculate the session key as $SK^* \leftarrow h(ID_i \| r^*_{\text{GWN}} \| ID_{\text{GWN}} \| M_9^* \| h(r_{\text{GWN}} \oplus KEY_{\text{GWN}-U_i}))$. And this session key includes $\{r^*_{\text{GWN}}, KEY_{\text{GWN}-U_i}$, and $h(r_{\text{GWN}} \oplus KEY_{GWN-U_i})\}$. U_A can not compute the session key without knowing these secret credentials so, it is clear that U_A has no access to these secret credentials. As a result, U_A has no access for all transmitted messages in PPT. The game winning advantage for U_A is not increased. However, the probability of winning the $Game_0$ and $Game_1$ is same for U_A. So, it is clear from $Game_1$ that

$$P_r[\text{Succ}_0] \leftarrow P_r[\text{Succ}_1]. \quad (3)$$

$Game_2$: In $Game_2$, an active attack is launched in $Game_1$ by adding Hash and oracle. In $Game_2$, U_A diverts the users so as to convince them of the forged message sent from U_A. To detect the collision of the secret key, U_A can make a number of hash oracles. The use of timestamp, identity, long-term secrets, and the existing transmitted messages assure the randomness of the message. After neglecting the running of sent oracles, collision probability is guaranteed. However, it is clear from the birthday paradox that

$$|P_r[\text{Succ}_1] - P_r[\text{Succ}_2]| \leq \frac{q^2_{hsh}}{2.|Hsh|}. \quad (4)$$

$Game_3$: This game models $Corrupt_{\text{SD}}$ oracles. Using side channel attack, U_A can get the sensitive information $\{V_i, C'_i, A'_i, D_i\}$, which is stored in the smart card. U_A requires random nonce a and bit length of biometric key BK_i to get secret credentials $\{V_i, C'_i, A'_i, D_i\}$. In $BK_i = 0, 1^{\text{len}}$, the len shows the bit length of biometric key BK_i. Here, $\frac{1}{2^{\text{len}}}$ is the probability of guessing the BK_i successfully. The benefit will be over $\frac{1}{2}$ for U_A to get the low entropy password through Zipf's law when $q_{\text{snd}} \leftarrow 10^7$ or 10^8. For guessing the low entropy password, U_A can use personal information of users. Furthermore, the advantage of guessing the password successfully will be over $\frac{1}{2}$, when $q_{\text{snd}} < 10^6$. There are limited attempts to input BK_i and PW_i. The guessing attacks are excluded, so the $Game_3$ can be acknowledged as ideal game. It is shown as

$$|P_r[\text{Succ}_2] - P_r[\text{Succ}_3]| \leq \max\left(B' \,.\, q^{s'}_{\text{snd}} \, \frac{q_{\text{snd}}}{2^{\text{len}}}\right) \quad (5)$$

where the parameters (B', s') are defined in [26].

$Game_4$: By appending $Corrupt_{\text{SD}}$ oracle, the $Game_3$ is converted to the final $Game_4$. In this game, U_A can not get the session key directly from devices. Therefore, to get secret credentials, U_A can abduct numerous sensing devices through special attacks. U_A needs secret credentials as $\{r_{\text{GWN}}, KEY_{\text{GWN}-U_i}\}$ to get the session key $SK^* = h(ID_i \| ID_{\text{GWN}} \| r^*_{\text{GWN}} \| M_9^* \| h(r_{\text{GWN}} \oplus KEY_{\text{GWN}-U_i}))$. As in SD_j, secret credentials are not stored directly. So, U_A will not be able to get these secret credentials. U_A can get any sensing device to get secret share pair (f_j, s_j) from its memory, but he cannot get $(r_{\text{GWN}})$to compute the secret values. The secret shared pair has forging probability $\frac{1}{2}$. So, it is shown as

$$|P_r[\text{Succ}_3] - P_r[\text{Succ}_4]| \leq \frac{1}{q}.\,\text{Advt}^{\text{IND-CPA}}_{R,U_A}(K). \quad (6)$$

In the last game, all the oracles have been modeled. If U_A guesses the bit b successfully, then U_A will win the game. So, it is clear that

$$P_r[\text{Succ}_4] \leftarrow \frac{1}{2}.$$

However, from (2) to (6) formula, we have

$$\begin{aligned}
&\text{Advt}^{\text{MAKA}}_{R,U_A}(K) \leftarrow 2\,.\,|P_r[\text{Succ}_0] - \frac{1}{2} \\
&= 2.\,|P_r[\text{Succ}_1] \\
&- P_r[\text{Succ}_4]|. \leq 2.\,(|P_r[\text{Succ}_1] - \\
&P_r[\text{Succ}_2]|) + |P_r[\text{Succ}_2] - P_r[\text{Succ}_4]| \\
&\leq 2.\,(|P_r[\text{Succ}_1] - P_r[\text{Succ}_2]|) \\
&+ |P_r[\text{Succ}_2] - P_r[\text{Succ}_3]| \\
&+ |P_r[\text{Succ}_3] - P_r[\text{Succ}_4]| + \\
&\frac{1}{q}.\,\text{Advt}^{\text{IND-CPA}}_{R,U_A}(K)). \leq \frac{q^2_{hsh}}{2.\,|Hsh|} + \\
&2\max\left(B' \,.\, q^{s'}_{\text{snd}} \, \frac{q_{\text{snd}}}{2^{\text{len}}}\right) + \\
&\frac{2}{q}.\,\text{Advt}^{\text{IND-CPA}}_{R,U_A}(K)).
\end{aligned} \quad (7)$$

B. Informal Security Analysis

In security analysis, informal analysis is the way to check the validity of any scheme considering the threat model. Here, the security of the presented scheme is analyzed properly. The informal analysis demonstrates that the presented scheme can easily resist well-known adversarial attacks, which are described as follows:

1) Stolen Verifier Attack: Assume that the trusted insider user of GWN acts as privilage attacker or U_A. U_A has the registration information of U_i and GWN. Without knowing both ID_i and $KEY_{\text{GWN}-U_i}$ of U_i, it is challenging for U_A to guess either ID_i or $KEY_{\text{GWN}-U_i}$ accurately form TID_i. This proves that our scheme is resistant to stolen verifier attack.

2) Impersonation Attacks: If U_A wants to impersonate on behalf of legal entity and calculates its messages to get authenticated; this is known as impersonation. Let us assume that U_A wants to impersonate the U_i. U_A intercepts the message on user's behalf and calculates the values. Correspondingly, U_A can also impersonate GWN or smart sensing device SD_j. However, in our proposed scheme, U_A is not able to calculate the valid message because our messages contain secret credentials. So, our scheme provides resilience against different impersonation attacks, which are described in following sections.

3) User Impersonation Attack: If U_A wants to impersonate U_i, it needs to generate the message $\{TID_i, M_1, M_2, TS_1\}$ tuple. However, U_A cannot generate the valid $\{TID_i, M_1, M_2, TS_1\}$. The reason is that, M_1 and M_1 contain secret credentials such as, $KEY_{\text{GWN}-U_i}$. Even, U_A generates random nonce r_i or current timestamp TS_1. U_A will not be able to compute M_1 as $M_1 \leftarrow h(A_i' \oplus RPW_i^*) \oplus r_i \leftarrow h(KEY_{\text{GWN}-U_i}) \oplus r_i$ and $M_2 \leftarrow h(TID_i \| M_1 \| ID_{\text{GWN}}^* \| r_i \| TS_1)$ and also $TID_i \leftarrow ENC_{\text{KEY}_{\text{GWN}}}(ID_i \| R_o)$. The reason is that these values need secret credentials for computation such as $KEY_{\text{GWN}-U_i}$, ID_i, TID_i, and R_o. So, we can say that, U_A will not be able to impersonate U_i in our scheme.

4) GWN Impersonation Attack: If U_A can generate valid $\{M_4, M_5, M_6, TS_2\}$, then it can impersonate GWN. Nevertheless, in our scheme, U_A is unable to calculate $M_4 \leftarrow r_{\text{GWN}} \times \gamma$, $M_5 \leftarrow Enc_{r_{\text{GWN}}}(ID_i, ID_{\text{GWN}}, h(r_{\text{GWN}} \oplus KEY_{\text{GWN}-U_i}))$, and $M_6 \leftarrow h(ID_i \| ID_{\text{GWN}} \| M_4 \| h(r_{\text{GWN}} \oplus KEY_{\text{GWN}-U_i}) \| TS_2)$. To calculate these values, the following secret credentials $\{ID_i, r_{\text{GWN}}, KEY_{\text{GWN}-U_i}\}$ are needed. These credentials are secret and U_A will not be able to get them. So, our scheme is resilient against impersonation attack of GWN.

5) Sensing Device Impersonation Attack: Suppose U_A tries to computes $\{M_8, TS_3\}$. Although, it can generate TS_3, U_A can compute the message only when it is able to calculate $M_8 \leftarrow Enc_{r_{\text{GWN}}^*}(s_j, f_j, ID_{\text{SD}_j})$. But, U_A will not be able to compute M_8, as it needs secret parameters $\{s_j, f_j, r_{\text{GWN}} ID_{\text{SD}_j}\}$ of the smart sensing device. U_A cannot get these values in our scheme.

6) Sensing Device Capture Attack: Let U_A intercepts the message $\{M_4, M_5, M_6, TS_2\}$ and then U_A tries to impersonate SD_j using parameters $\{ID_{\text{SD}_j}, s_j, f_j, k_j\}$. These parameters are stored in SD_j. It is clear that the ID_{SD_j} of SD_j is anonymous. To guess ID_i and ID_{SD_j} of user and sensing device or the corresponding shared secret key $KEY_{\text{GWN}-U_i}$, it is computationally hard to find for U_A, which is protected by hash. Thus our scheme is also secured against sensing device capture attack.

7) Desynchronization of Pesudoidentities: As U_A is a capable to block a message or there may be some packet loss. In these situations user does not get new identity TID_i^{new}. However, in our proposed scheme U_i is a legal user, whose identity is already stored in GWN; so legal user can continue the session with GWN using previously stored identity ID_i of the user. Thus, the problem of desynchronization of pseudoidentity is not possible.

VI. Performance Analysis

We discussed the detailed comparison of the performance as well as security features of the our scheme, with the following related competing schemes: Das *et al.* [1], Shuai *et al.* [27], Yang *et al.* [28], Abdi Nasib *et al.* [29], and Vinoth *et al.* [30].

A. Communication Cost

The cost of communication for our scheme and related existing competing schemes is calculated. In this section, parameter's bit length is defined uniformly. We have considered the random nonce, identity, timestamp, ECC, XOR, password of 160 bits each, hash value of 256 bits and the Encryption/Decryption of 128 bits. The costs of communication for $msg1, msg2 \ldots msg6$ are 736, 704, 288, 512, 800, and 256 bits, respectively. The communication cost between user, gateway node, and sensing devices for [1], [27]–[30] schemes are 2688, 2592, 960, 3456, and 3456 bits, respectively.

TABLE III
Computation Comparison

Protocols	U_i/MT_i (ms)	WD_{dj} (ms)	Total Computation Cost (ms)	Cost
Das et al. [1]	$18T_{\text{H}} \approx 0.0175$	$12T_{\text{H}} \approx 0.0242$	$9T_{\text{H}} \approx 1.199$	10.8309
Shuai et al. [27]	$8T_{\text{H}} + 1T_{\text{ED}} \approx 0.0081$	$7T_{\text{H}} + 1T_{\text{ED}} \approx 0.0146$	$5T_{\text{H}} \approx 1.9256$	6.0177
Yang et al. [28]	$8T_{\text{H}} \approx 0.0175$	$12T_{\text{H}} \approx 0.00187$	$9T_{\text{H}} \approx 1.199$	10.8309
Abdi Nasib et al. [29]	$9T_{\text{H}} \approx 0.0087$	$10T_{\text{H}} \approx 0.0187$	$5T_{\text{H}} \approx 5.9950$	6.0224
Vinoth et al. [30]	$9T_{\text{H}} + 1T_{\text{E/D}} \approx 0.00906$	$6T_{\text{H}} + 3T_{\text{E/D}} \approx 0.01527$	$4T_{\text{H}} + 2T_{\text{E/D}} \approx 6.522$	6.54633
Proposed	$10T_{\text{H}} + 2T_{\text{ED}} \approx 0.01038$	$8T_{\text{H}} + 4T_{\text{ED}} \approx 0.02036$	$7T_{\text{H}} + 2T_{\text{ED}} \approx 10.119$	10.14974

B. Computational Cost

The computational cost of an authentication protocol counts the total execution time for each cryptographic operations. While calculating the computational cost of the proposed and related schemes, we examine cryptographic functions such as T_h one-way hash function, T_{ED} symmetric Encryption/Decryption. The computational cost is computed at each end, i.e ., U_i, GWN, SD. The registration step of an authentication protocol is a one-time activity, hence it is omitted in correlation. As a result, the login, authentication and key agreement phases are the leading apprehensions for determining the computing costs. In the devised protocol, the execution of hash function is ten times and encryption/decryption is executed two times by U_i. Furthermore, the computational cost for U_i is $(10 \times 0.00097) + (2 \times 0.00033) \approx 0.01038$ ms. Similarly, the encryption/decryption and hash function is executed four times and eight times at GWN. While encryption/decryption and hash function are executed two times and seven times for SD. The computational cost of GWN and SD are $(8 \times 0.0.00187) + (4 \times 0.00135) \approx 0.02036$ ms and $(7 \times 0.1.199) + (2 \times 0.0.863) \approx 10.119$ ms, respectively. The overall cost of computation of our scheme is compared with the related competing schemes. Now consider that the T_h, and T_{ED} represents the computational time needed for one-way hash function and encryption/decryption, respectively. The computational costs of T_h and T_{ED} for U_i, GWN, and SD are 0.00097, 0.00187, 1.199, and 0.00033, 0.00138, 0.863 in ms, respectively. Furthermore, the total computational cost of our scheme is 10.14974 ms. The computational costs of all related competing protocols [1], [27]–[30] are measured similarly and shown in Table III.

C. Security Features

To calculate the features and functionality of our authenticated key agreement scheme related to other competing schemes, we design evaluation metrics. In Table IV, comparison of the security features and functionality of our scheme among previously reported competing schemes is represented. According to this table, almost all the schemes are multifactor. Moreover, these schemes are insecure against different adversarial attacks. Although some of these schemes claim that they can prevent numerous adverse alert acts like privilege-insider, man-in-the-middle attack, and the replay attack. They are unable to support

TABLE IV
COMPARISON ON SECURITY FEATURES

Protocols:	$S[1]$	$S[2]$	$S[3]$	$S[4]$	$S[5]$	$S[6]$	$S[7]$
Das et al. [1]	✗	✗	✗	✗	✗	✓	✗
Shuai et al. [27]	✗	✗	✓	✗	✗	✓	✗
Yang et al. [28]	✗	✗	✗	✗	✗	✓	✗
Abdi Nasib et al. [29]	✗	✗	✗	✗	✗	✓	✗
Vinoth et al. [30]	✗	✗	✗	✗	✗	✓	✗
Proposed Protocol	✓	✓	✓	✓	✓	✓	✓
✓: Offers; ✗: Does not offer							

the smart devices in terms of security. In short, our proposed scheme is more robust and secure than previously reported competing schemes.

VII. CONCLUSION

In this article, we presented a provable secure and robust multifactor authenticated key agreement scheme for the IIoT environment. This scheme is proposed to improve the production efficiency in industries. It also helps to tackle the production issues rapidly. Our scheme only uses XOR operation, symmetric cryptography, and hash function. Furthermore, to calculate the features and functionality of our authenticated and key agreement scheme related to competing schemes, we design evaluation metrics. Our presented scheme can resist numerous known attacks easily. It works comparatively at a low cost when compared to the previously reported competing schemes as it resists several adversarial attacks. The proposed scheme is designed as resource efficient regarding communication and computation cost. It supports the joining and revocation of sensing devices dynamically. Furthermore, we plan to explore our scheme of authentication and key agreement to improve security issues present in diffierent IoT-based environments.

REFERENCES

[1] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4900–4913, Dec. 2018.

[2] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for Big Data in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3628–3636, Aug. 2018.

[3] W. Ali, I. U. Din, A. Almogren, M. Guizani, and M. Zuair, "A lightweight privacy-aware IoT-based metering scheme for smart industrial ecosystems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 9, pp. 6134–6143, Sep. 2021.

[4] S. A. Chaudhry, "Correcting "palk: Password-based anonymous lightweight key agreement framework for smart grid,"" *Int. J. Elect. Power Energy Syst.*, vol. 125, 2021, Art. no. 106529.

[5] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, "Efficient and secure anonymous authentication with location privacy for IoT-based WBANs," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2603–2611, Apr. 2020.

[6] Z. Ali, S. A. Chaudhry, K. Mahmood, S. Garg, Z. Lv, and Y. B. Zikria, "A clogging resistant secure authentication scheme for fog computing services," *Comput. Netw.*, vol. 185, 2021, Art. no. 107731.

[7] S. A. Chaudhry *et al.*, "A lightweight authentication scheme for 6G-IoT enabled maritime transport system," *IEEE Trans. Intell. Transp. Syst.*, to be published, doi: 10.1109/TITS.2021.3134643..

[8] B. Liang, M. Obaidat, X. Liu, H. Zhou, and M. Dong, "Resource scheduling based on priority ladders for multiple performance requirements in wireless body area networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 7027–7036, Jul. 2021.

[9] K. Choudhary, G. S. Gaba, I. Butun, and P. Kumar, "Make-it-a lightweight mutual authentication and key exchange protocol for industrial Internet of Things," *Sensors*, vol. 20, no. 18, 2020, Art. no. 5166.

[10] L. Fang, H. Zhang, M. Li, C. Ge, L. Liu, and Z. Liu, "A secure and fine-grained scheme for data security in industrial IoT platforms for smart city," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 7982–7990, Sep. 2020.

[11] Z. Gu, H. Chen, P. Xu, Y. Li, and B. Vucetic, "Physical layer authentication for non-coherent massive SIMO-based industrial IoI communications," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2020, pp. 1–6.

[12] B. Baruah and S. Dhal, "An efficient authentication scheme for secure communication between industrial IoT devices," in *Proc. 11th Int. Conf. Comput., Commun. Netw. Technol.*, 2020, pp. 1–7.

[13] M. Amoretti, R. Pecori, Y. Protskaya, L. Veltri, and F. Zanichelli, "A scalable and secure publish/subscribe-based framework for industrial IoI," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 3815–3825, Jun. 2021.

[14] A. Karati, S. H. Islam, and M. Karuppiah, "Provably secure and lightweight certificateless signature scheme for IIoT environments," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3701–3711, Aug. 2018.

[15] F. Rezaeibagha, Y. Mu, X. Huang, W. Yang, and K. Huang, "Fully secure lightweight certificateless signature scheme for IIoT," *IEEE Access*, vol. 7, pp. 144 433–144 443, 2019.

[16] Y. Zhang, R. H. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, "Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 15, no. 9, pp. 5099–5108, Sep. 2019.

[17] C. Peng, M. Luo, L. Li, K.-K. R. Choo, and D. He, "Efficient certificateless online/offline signature scheme for wireless body area networks," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 14 287–14 298, Sep. 2021.

[18] Y. Yu, L. Hu, and J. Chu, "A secure authentication and key agreement scheme for IoT-based cloud computing environment," *Symmetry*, vol. 12, no. 1, 2020, Art. no. 150.

[19] K. Haseeb, A. Almogren, I. Ud Din, N. Islam, and A. Altameem, "SASC: Secure and authentication-based sensor cloud architecture for intelligent Internet of Things," *Sensors*, vol. 20, no. 9, 2020, Art. no. 2468.

[20] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4081–4092, Sep. 2018.

[21] J. Seto, Y. Wang, and X. Lin, "User-habit-oriented authentication model: Toward secure, user-friendly authentication for mobile devices," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 1, pp. 107–118, Mar. 2015.

[22] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proc. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2001, pp. 453–474.

[23] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[24] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 2, pp. 391–406, Mar./Apr. 2020.

[25] F. Wen and X. Li, "An improved dynamic id-based remote user authentication with key agreement scheme," *Comput. Elect. Eng.*, vol. 38, no. 2, pp. 381–387, 2012.

[26] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 11, pp. 2776–2791, Nov. 2017.

[27] M. Shuai, L. Xiong, C. Wang, and N. Yu, "A secure authentication scheme with forward secrecy for industrial Internet of Things using rabin cryptosystem," *Comput. Commun.*, vol. 160, pp. 215–227, 2020.

[28] Z. Yang, J. He, Y. Tian, and J. Zhou, "Faster authenticated key agreement with perfect forward secrecy for industrial internet-of-things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6584–6596, Oct. 2020.

[29] H. A. N. Far, M. Bayat, A. K. Das, M. Fotouhi, S. M. Pournaghi, and M.-A. Doostari, "LAPTAS: Lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT," *Wireless Netw.*, vol. 27, no. 2, pp. 1389–1412, 2021.

[30] R. Vinoth, L. J. Deborah, P. Vijayakumar, and N. Kumar, "Secure multifactor authenticated key agreement scheme for industrial IoT," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3801–3811, Mar. 2021.