IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 18 December 2023, accepted 29 December 2023, date of publication 22 January 2024, date of current version 4 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3357090

RESEARCH ARTICLE

LEAF-IIoT: Lightweight and Efficient Authentication Framework for the Industrial Internet of Things

MUHAMMAD TANVEER[1], AHMED A. ABD EL-LATIF[2,3,4], (Senior Member, IEEE), ABD ULLAH KHAN[5,6], (Member, IEEE), MUSHEER AHMAD[7], AND ABDELHAMIED A. ATEYA[3,8], (Senior Member, IEEE)

[1]School of Systems and Technology (SST), University of Management and Technology, Lahore 54770, Pakistan
[2]Center of Excellence in Quantum and Intelligent Computing, Prince Sultan University, Riyadh 11586, Saudi Arabia
[3]EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
[4]Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
[5]Department of Electrical and Electronics Engineering, Kyung Hee University, Gyeonggi-do 17104, South Korea
[6]Department of Computer Science, National University of Sciences and Technology Balochistan Campus, Islamabad 44000, Pakistan
[7]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
[8]Department of Electronics and Communications Engineering, Zagazig University, Zagazig 44519, Egypt

Corresponding author: Ahmed A. Abd El-Latif (aabdellatif@psu.edu.sa)

The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

ABSTRACT The Internet of Things (IoT) has emerged as a revolutionary communication technology, enabling the connection of resource-limited devices to the Internet. These devices are deployed in various industrial control systems to remotely monitor and control industrial applications. However, the public Internet's inherent vulnerability to malicious attacks poses a significant challenge to the secure operation of these systems. To address this challenge, a lightweight and efficient authentication framework, LEAF-IIoT, is proposed. LEAF-IIoT leverages authenticated encryption (AE) techniques to provide a multifaceted security solution encompassing confidentiality, authentication, and data integrity. It establishes a secure channel by exchanging messages between the user, gateway, and smart embedded device, culminating in the creation of a session key for secure data exchange. Rigorous security assessment confirms the robustness of LEAF-IIoT, while performance evaluation demonstrates its significantly lower computational cost and reduced communication overhead compared to existing frameworks. Despite these efficiencies, LEAF-IIoT continues to provide strong security features, ensuring the integrity and confidentiality of data exchanged in the IIoT context.

INDEX TERMS Communication security, IIoT, smart device, resource constrained.

I. INTRODUCTION

The Internet of Things (IoT), which entails linking numerous physical objects to the Internet, is a broader term encompassing the Industrial Internet of Things (IIoT) [1], [2]. A network of networked equipment and objects designated as the IIoT is equipped with sensors, software, and other cutting-edge technologies that allow them to collect and share data. In order to improve goods, services, and the overall operational effectiveness of the IIoT environment, the data gathered by these embedded devices in the IIoT environment is shared with other objects or transferred to a central location for further analysis [3]. Resources-limited and resource-capable devices are both a part of IIoT-enabled devices. For remote operating and control of various industrial operations, a significant amount of IIoT-capable equipment is installed in different industrial control systems. To guarantee the seamless functioning of the particular industrial application, these devices carry out the sensing and actuation functions [4]. The IIoT device used in the IIoT application additionally collects sensitive data from the surrounding environment and sends the sensed data to

The associate editor coordinating the review of this manuscript and approving it for publication was Stefano Scanzio.

© 2024 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

a centralized location for additional processing. In addition, the IIoT application controller delivers control commands to the IIoT devices installed in the IIoT environment to carry out a specific actuation job. The public communication channel served as the sole means of communication between the controller and IIoT devices [5]. Because the public communication channel is accessible, an attacker has the ability to intercept IIoT application operations while also capturing and altering important data. Therefore, it is crucial to safeguard confidential information sent through a public channel from unauthorized users or attackers [6], [7], [8]. Furthermore, when the remote user or controller is engaged, communication security is also required to guarantee the proper operation of the IIoT application.

The authenticated session key agreement (ASKG), among other security measures, has been established to provide dependable and secure communication in the IIoT environment. Due to the prevalence of symmetric and asymmetric encryption, many ASKG systems demand high computational overhead, making them unsuitable for IIoT devices with low resources and processing capacity. To address this issue, NIST has standardized a number of authenticated encryption (AE) algorithms that concurrently provide confidentiality and authenticity with a low overhead for processing and transmission. Our goal in this study is to design an ASKG to provide effective protection against malicious insiders, jamming, and other attacks in the IIoT context.

A. MOTIVATION AND RESEARCH CONTRIBUTION

In the existing literature, numerous ASKG schemes are found to be vulnerable to various attacks, such as impersonation, replay, jamming, and privileged insider attacks. In the context of the IIoT environment, the gateway assumes a central role, facilitating communication between IIoT devices within the environment and the external internet domain. The gateway is also responsible for storing sensitive information related to users and IIoT devices, essential for accomplishing the mutually ASKG phase. However, a significant concern arises as even legitimate but curious users may gain access to the gateway's secret key, potentially leading to the execution of various attacks. For example, the ASKG presented in [9] is susceptible to privileged insider attacks, and fails to accomplish the ASKG after performing the password update phase. Moreover, the authentication scheme proposed in [1] stores the gateway key in plaintext form in the database, creating a risk for privileged insider attacks. Additionally, many ASKG schemes involve computationally expensive asymmetric cryptography, leading to performance issues. To address these critical concerns, a robust ASKG design is essential, offering resistance against privileged insider attacks while remaining suitable for the resource-limited nature of IIoT devices. Consequently, this article introduces a lightweight and efficient authentication framework for IIoT, named (LEAF-IIoT), aiming to tackle these challenges effectively.

The article makes the following primary contributions:

1) LEAF-IIoT is constructed by incorporating the NIST lightweight cryptography-based AE scheme called "ASCON [10]" and leveraging the physical unclonable function (PUF). The primary aim behind designing LEAF-IIoT is to establish a secure channel (session key) between the user and the IIoT smart device (ISD) during the execution of the ASKG phase. Once the secure channel is established, the user gains the capability to send control commands to the ISD deployed in the IIoT environment securely. The utilization of PUF serves two key purposes: ensuring physical security and generating the secret long-term key essential for accomplishing the ASKG phase. By incorporating PUF, LEAF-IIoT enhances its resistance against privileged insiders.
2) To showcase the robustness of LEAF-IIoT against various malicious security attacks, such as replay, jamming, impersonation, and man-in-the-middle attacks, an informal security analysis is performed. Additionally, we employ BAN logic to establish the logical correctness of LEAF-IIoT. Furthermore, the Scyther tool is utilized to provide further verification of the security measures implemented in LEAF-IIoT.
3) We assess the efficiency of LEAF-IIoT in terms of its security measures and computing and communication costs, comparing it to fifteen other ASKG schemes. LEAF-IIoT demonstrates effective security measures while significantly reducing computing costs by 53.58% to 59.41% and communication costs by 42.11% to 64.14% when compared to the other schemes.

The paper's structure encompasses several key sections. Firstly, in Section II, we conduct an analysis of the strengths and weaknesses of recent ASKG designs tailored for IIoT. Following this, in Section IV, we delve into the system architecture and the roles fulfilled by various IIoT devices, along with the accompanying attack model. In Section V, we elaborate on the various Algorithms utilized at different phases of the proposed LEAF-IIoT. Subsequently, in Section VI, we perform essential security validations. The computing and communication efficiency of LEAF-IIoT is assessed in Section VII. Finally, we conclude the paper with remarks in Section VIII.

II. RELATED WORK

In [11], the authors introduced an innovative ASKG approach that enables mobile device users to perform mutual authentication in a single round. By implementing physically unclonable functionalities, their approach assures user anonymity, protects user privacy, and offers a defense against physical threats. In [12], the authors present the ASKG mechanism for wearables technology. Both the user and the wearable device, as well as the user and the cloud server, can mutually authenticate by employing their suggested technique. Additionally, it creates private session keys for every session, guaranteeing safe communication between all participating parties. The designers of [13] introduced the IIoT-specific resource-effective ASKG protocol called REAP-IIoT. REAP-IIoT makes use of the AEGIS primitive. Since AE primitives require fewer computing resources and are therefore more easily implemented, they are perfect for devices with limited resources within the IIoT. In [14], the authors propose an innovative ASKG approach that employs authentication and derivation primary keys. Through the utilization of the XOR operator and hash function, this ASKG scheme accomplishes mutual authentication, key exchange, and message integrity, offering a streamlined and efficient solution. A security framework is presented in [15], though it displays a design flaw. This flaw becomes evident when modifying the credentials, resulting in compromised scheme functionality. Conversely, a secure and reliable communication scheme is put forth in [16].

In [17], an inexpensive ASKG method known as RAMP-IoD is introduced. This approach makes use of an AE primitive and a hash function. Because of their low processing requirements, AE primitives are ideal for resource-constrained drones. RAMP-IoD also ensures privacy-preserving user authentication capabilities and creates an SK between the drones deployed in the IoD environment and the users. This established SK is used for encrypted communication by both the user and the drones. In [18], an effective and reliable ASKG is developed for use in the setting of smart devices with constrained computational processing capability. The goal of ASKG is to create a secure communication channel. The security validation tool AVISPA is used to assure the stability of the proposed framework. AVISPA tests the proposed ASKG's robustness, adding another level of assurance to the security measures. The authors within [19], introduced an ASKG scheme tailored for 5G-enabled WSNs using SHA and ECC. To bolster the security of this proposed ASKG approach, the authors used the AVISPA and ROR models. Notably, it's essential to highlight that the security of the ASKG proposed in [19] hinges on a solitary parameter, namely $h(ID_{gw} \parallel X_{GWN})$, which is shared among all system users. An inquisitive but legitimate system user could potentially expose the value of $h(ID_{gw} \parallel X_{GWN})$, thereby compromising the security of the entire system. The ASKG scheme introduced in [20] leveraged cryptographic primitives, including SHA, EC, and XOR. Furthermore, to reinforce the security of the proposed approach, verification was conducted through the AVISPA and ROR models. This scheme stands resilient against man-in-the-middle, identity guessing, and impersonation attacks. In [21], the authors introduced an anonymous ASKG scheme targeting WSN environments. Nonetheless, evaluation in [22] reveals that their protocol is insufficient in countering insider, stolen verifier, and ephemeral secret leakage attacks. A security scheme in [23] is designed using the chaotic map and hash function and its security capabilities are ensured using the Scyther and ROR model. The security scheme outlined in [24] exhibits vulnerabilities to privileged insider attacks, user impersonation, and denial-of-service incidents, and does not possess perfect forward secrecy. The security scheme proposed in [25] is based on the hash function and XOR. In addition, the scheme proposed in [25] is unable to ensure the anonymity feature.

Many security schemes [20], [26], [27], [28] adopt the approach of storing the long-term secret key in the database of the gateway/server, operating under the assumption that the secret key is beyond the reach of potential attackers. Nonetheless, the existence of an insider adversary introduces the potential vulnerability of extracting the secret key from the gateway/server, thereby endangering the overall system's security. To confront this formidable challenge, we have devised an authentication framework tailored for the IIoT. This framework is engineered to counter device capture, privileged insider, and impersonation attacks, ensuring robust resistance against such threats. An innovative user authentication and key agreement scheme with provable security has been crafted in [29], incorporating physically unclonable functions and elliptic curve cryptography. This system is designed to withstand diverse security attacks.

III. PRELIMINARIES

This section provides an explanation of the background knowledge required to understand LEAF-IIoT.

A. ASCON: AN AE SCHEME

Known for its remarkable performance and security, "ASCON" is a very effective and efficient (in terms of computing and communication overheads) AE Algorithm. It was acknowledged as one of the winners of the NIST competition for lightweight cryptography. As opposed to AES, which just provides confidentiality, "ASCON" goes further offering other security components, such as data authenticity. As an encryption Algorithm, "ASCON" generates the "ciphertext" (Ct) and authentication parameter (MAC) from the "plaintext" (Pt), respectively.

The operating mechanism of "ASCON" may be represented symbolically as "$(Ct, MAC) = E_K\{(N, Ad), Pt\}$ and $(Pt, MAC) = D_K\{(N, Ad), Ct\}$", where K stands for the secret key, N stands for the "nonce," and Ad stands for the "Associative Data." Since MAC is present, the veracity and integrity of both Ad and Ct are assured. In the proposed LEAF-IIoT, the chosen "encryption/decryption" Algorithm is "ASCON".

B. PHYSICAL UNCLONEABLE FUNCTION

PUFs rely on a device's intrinsic physical properties, such as changes in delay or impedance brought on by manufacturing inconsistencies. PUFs come in a variety of forms, such as ring PUFs, delay-based PUFs, and arbiter PUFs, as a result of these differences. The PUF is useful for activities like key creation and identity authentication in the IoT sector since it acts as a hardware "fingerprint" and retains a distinct identity in response. PUF technology has several uses in situations where strong security measures are necessary.

TABLE 1. Analysis of vulnerabilities in the current ASKG for IIoT environments.

Reference/ASKG	Cryptographic Algorithms Utilized	Security Vulnerabilities/Attack Analysis
[9]	SHA + AES + XOR	Exhibits a design flaw as the scheme becomes nonfunctional after a password change. it is vulnerable to privileged insider attacks.
[15]	SHA + AE + XOR	Demonstrates a design deficiency wherein the system becomes inoperative following a password alteration. It is exposed to potential privileged insider attacks.
[19]	SHA + EC + AES + XOR	The overall system's security might be compromised if an authorized yet curious user exposes the parameter $h(ID_{gw} \parallel X_{GWN})$.
[20]	SHA + EC + XOR	The security of the entire system could be jeopardized if an authorized yet inquisitive user reveals the parameters G_2 and G_3. Moreover, the system is susceptible to man-in-the-middle, identity guessing, and impersonation attacks.
[30]	SHA + EC + XOR	This scheme fails to provide protection against three major attacks: drone impersonation, privilege insider threat and drone capture.
[24]	SHA + AES + XOR	This scheme fails to provide protection against three major attacks: privileged insider, user impersonation, and denial-of-service (DoS) attacks and does not possess perfect forward secrecy.
[31]	SHA + XOR	This scheme fails to provide protection against impersonation and session key disclosure attacks.
LEAF-IIoT	SHA + AE + XOR	A constraint of the proposed LEAF-IIoT is its dependency on specialized hardware, specifically for the operation of PUFs.

Note: SHA: "Secure hash Algorithm"; AES: "Advanced encryption standard".

When *Ch* stands for the challenge and *Re* is the appropriate response, the functionality of a PUF may be written as $Re = PUF(Ch)$. We use a fuzzy extractor (FE) to stabilize the output to guarantee a constant output from the PUF regardless of temperature variations.

C. FUZZY EXTRACTOR

In general, the concept of "FE" refers to a cryptographic approach that pertains to the extraction of secure and trustworthy cryptographic keys from noisy or error-prone sources, such as biometric data or other sensitive information. A FE's fundamental objective is to produce a stable key that is resistant to changes in the input data and can be utilized in cryptographic processes.

The process of extracting a stable key from noisy data involves two main steps:

Key Generation (input): The FE transforms a noisy input (such as biometric information like fingerprints) into an accurate output in this stage of the process. This reliable representation functions as a cryptographic key in essence. To provide a reliable and consistent key, the enrollment process attempts to remove the noise and variances found in the input data. The user's biometric data, the biometric key, and the helper data are represented as Bio, B_k, and hd and $(B_k, hd) = Gen(Bio)$ is the logical operation of the key generation function utilizing FE.

Key Reconstruction (input): The second stage is the key generation step done in reverse. The FE receives the same noisy input data again during the key reconstruction process. The original key is then recreated by the extractor using the previously generated hd. For the reconstruction process, the user's biometric data, the biometric key, and the helper data are represented by Bio^*, B_k^*, and hd, respectively, in the logical operation of the key generation function utilizing FE, which is represented as $(B_k^*) = Gen(Bio^*, hd)$. If the criteria are met, $HD(Bio^*, Bio) \leq et$, where et and HD denote the error tolerance and hamming distance.

TABLE 2. List of notations.

Notation	Description
GW_j	Gateway node
ID_{uk}	Identity of user
PW_{uk}	Password of user
ID_j	Gateway's identity
T_{di}	Allowed maximum delay
T_1	Timestamps
T_{re}	Message receiving time
$E_{key}\{Ad, P\}$	ASCON's encryption process
$D_{key}\{Ad, C\}$	ASCON's decryption process
(C, MAC)	Ciphertext and authentication parameters
(P, MAC')	Plaintext and authentication parameters
$\mathcal{A}$	Attacker/adversary
$H(.)$	Hash-function operation
$\oplus, \parallel$	XOR and Concatenation, respectively

IV. SYSTEM ARCHITECTURE

The authentication model employed for the proposed LEAF-IIoT consists of the following components, as illustrated in Figure 1:

Gateway: Within the IIoT context, the deployment of gateway nodes (GW_j) is the task of the registration authority (RA). The IIoT-capable devices installed in the setting are connected to the internet through these gateway nodes. The important parameters related to the remote user and smart embedded devices are also stored in GW_j. It is equipped to link IIoT-capable devices to the Internet utilizing cellular or other types of Internet access. Additionally, any IIoT-capable devices installed in the environment are connected to GW_j via WiFi, 6LoWPAN, or Zigbee communication protocols.

IIoT Smart Device: Resources-constrained devices used in the IIoT environment are referred to as ISD. Each ISD is provided with communication, storage, and computing resources and is designated as ISD_i. Through the use of

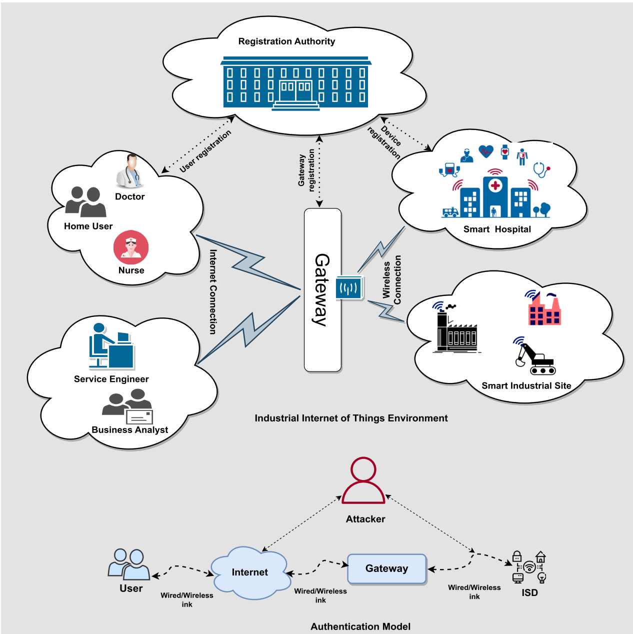

FIGURE 1. IIoT environment and authentication model.

communication protocols like WiFi, 6LoWPAN, or Zigbee, these devices can connect to GW_j. ISDs also come with sensing modules, which give them the ability to gather sensitive information from their surroundings. It is possible to send the gathered data to a central place for additional analysis.

User: The user owns smart devices with biometric sensors (SD_k). The gateway node (GW_j) is the conduit for interaction between U_k and ISD_i. Additionally, U_k and GW_j are able to interact via cellular or internet technology. It is essential to make sure that only authorized U_k can access real-time information from the deployed ISD_i in the IIoT environment. To aid in comprehending the proposed scheme, Table 2 provides an elucidation of the various symbols employed.

A. ADVERSARIAL MODEL AND ASSUMPTIONS

We will make use of the renowned DY adversarial model, to simulate an IoT application environment and assess the protocol's trustworthiness. In this model, we presume that all entities, excluding RA, interact over unencrypted channels and have trust in RA. RA is responsible for managing the establishment of the system, user registration, and cancellation. According to the DY approach, when messages are transferred using a shared channel, a third party or adversary has an opportunity to get them and manipulate them. Due to the highly complicated application architecture of the IIoT, attackers can access physical devices to obtain secret configurations and information, or they can carry out replay and MITM attacks using the retrieved information. Additionally, if the user's registered device becomes unavailable or stolen, attackers will have access to the user's privacy via the mobile device. The most up-to-date adversary attack approach from CK is additionally included, which enhances the positive aspects of the DY model by taking a wider range of circumstances into consideration. With the application of this framework, the adversary, designated as $\mathcal{A}$, acquires access to temporary partial keys by acquiring public secret credentials while the session is underway.

For our study, we have taken into account a number of assumptions. First, we assume that PUF capability is present on the gateway nodes. Analogously, we consider that both ISD and smart cards have PUF capabilities.

V. THE PROPOSED LEAF-IIOT FRAMEWORK

The development of LEAF-IIoT is organized into several sequential phases: registration, ASKG, and the update of secret credentials. Each of these phases is thoroughly explained in the subsequent subsections.

A. REGISTRATION PHASE

Within this section, the process of registering the gateway node, ISD_i, and user (U_k) is elaborated. During the registration phase, it is assumed that all communications will occur through a secure channel. The Registration Authority (RA) holds the responsibility for registering the gateway node, ISD_i, and user U_k before their deployment in the IIoT environment.

1) GATEWAY NODE REGISTRATION

RA undertakes the task of selecting a distinct identity for the gateway node (ID_j), generating a challenge (Ch_j), and securely transmitting these credentials to the gateway (GW_j). In this scenario, it is assumed that the gateway (GW_j) is equipped with a PUF, which computes $PUF(Ch_j) = Res_j$. To mitigate the effects of variations in PUF's output due to temperature fluctuations, a FE mechanism is employed. This mechanism derives a consistent key (denoted as K_{GW}) from Res_j by executing the operation $(K_{GW}, hd) = Gen\ (Res_j)$. Ultimately, the gateway (GW_j) retains the credentials (ID_j, hd, and Ch_j) within its own database.

2) ISD_I REGISTRATION

The RA chooses an exclusive identity, SID_i, as well as Ch_i, for the ISD_i. These credentials are then securely transmitted to ISD_i. Upon receipt of the credentials, ISD_i calculates $PUF(Ch_i) = Res_i$. An FE mechanism is employed to counteract the potential impact of PUF output fluctuations caused by temperature variations. This mechanism extracts a consistent key (B_{kd}) from Res_i using the operation $(B_{kd}, hdi) = Gen(Res_i)$. Eventually, ISD_i keeps the credentials (SID_i, hdi, and Ch_i) within its internal database and sends B_{kd} securely to RA. Finally, RA computes $(C_a, Tag_a) = E_{K_{GW}}\{B_{kd}\}$ using the ASCON encryption Algorithm and computes $SID_j = H(ID_j)$, $Z = (SID_j \oplus H(B_{kd}))$ and stores the credentials $\{SID_i, C_a, Tag_a\}$ in the database of GW_j. In addition, RA stores Z in the memory of ISD_i before its deployment in the IIoT environment.

3) U_K REGISTRATION

The trusted entity referred to as RA initiates this process by selecting a challenge denoted as Ch_{uk} and SID_j and transmitting them to U_k. Upon receiving Ch_{uk}, U_k computes two values: Res_a using a PUF denoted as $PUF(Ch_{uk})$, and $(B_{k1}, hdk1)$ by utilizing a process denoted as $Gen(Res_a)$. U_k transmits the data B_{k1} along with its unique identifier ID_{uk} to the designated recipient. Subsequently, GW_j selects a temporary identifier PID_t, and generate the pair (C_u, Tag_u) using the encryption key K_{GW}. The resulting encrypted data (C_u, Tag_u) is then stored in GW_j's database. This storage is linked to two distinct associations: one with the temporary identifier $PID_t^r = PID_t$ and another with $PID_t^p = null$. Additionally, GW_j records the temporary identifier PID_t and compiles a list of devices denoted as SID_i that can provide real-time information to the user and sends PID_t and SID_i to GW_j.

U_k selects PW_{uk} and imprints Bio_{uk} and computes the biometric key $B_k = Rep(Bio_{uk}, hdk)$ and the encryption key $A_1 = H(ID_{uk} \parallel PW_{uk} \parallel B_k^*)$. In addition, U_k computes $(C_a, MAC_1) = E_{A_1}\{P_a\}$ using the ASCON encryption Algorithm, where $P_a = \{Ch_{uk}, SID_i, SID_j, PID_t\}$. Finally, U_k stores $\{C_a, MAC_1, hdk, hdk1\}$ in its own memory.

B. ASKG PHASE

The execution of the ASKG phase in the proposed LEAF-IIoT is achieved by implementing the subsequent Algorithm 1, Algorithm 2, Algorithm 3, and Algorithm 4.

1) USER LOGIN AND AUTHENTICATION MESSAGE GENERATION

In order to attain local authentication and produce authentication messages, U_k employs its own SD_k to execute Algorithm 1. Furthermore, the SD_k facilitates the fuzzy extractor-based key generation and reproduction functionality. When Algorithm 1 is executed, the SD_k receives the parameters $\{ID_{uk}, PW_{uk}, Bio_{uk}, C_a, hdk, hdk1\}$ as input and produces the parameters $\{T_1, C_b, C_c, MAC_2\}$ as output. Upon receiving biometric information from U_k, SD_k calculates the biometric key B_k^* using the fuzzy extractor's reproduction function. Notably, the biometric key's size amounts to 256 bits. Subsequently, the secret key A_1^* is computed for decryption, also consisting of 256 bits. This secret key can further be divided into a 128-bit secret key and a 128-bit nonce. Decryption is carried out through the application of the ASCON decryption Algorithm. This Algorithm utilizes the ciphertext C_a along with the secret parameter $A_1^* = (\text{key} \parallel \text{nonce})$ to produce the plaintext $P_a = \{Ch_{uk}, SID_i, SID_j, PID_t\}$ as well as MAC_1^*.Local authentication and verification of all the secret credentials associated with U_k are accomplished by evaluating the condition $MAC_1 = MAC_1^*$. If this condition holds true, SD_k proceeds to generate a random number R_2 and a timestamp T_1, following which it computes the plaintext P_2 and associative data Ad_2. For encryption, SD_k undertakes

Algorithm 1 User Login and Authentication Message Generation

Input: $\{ID_{uk}, PW_{uk}, Bio_{uk}, C_a, MAC_1, hdk, hdk1\}$
Output: $\{T_1, C_b, C_c, MAC_2\}$

procedure ALG-1($\{ID_{uk}, PW_{uk}, Bio_{uk}, C_a, MAC_1, hdk, hdk1\}$)
  $B_k^* \leftarrow Rep(Bio_{uk}, hdk)$
  $A_1^* \leftarrow H(ID_{uk} \parallel PW_{uk} \parallel B_k^*)$
  $(P_a, MAC_1^*) \leftarrow D_{A_1^*}\{C_a\}$
  if $MAC_1 == MAC_1^*$ **then**
    $P_a \leftarrow \{Ch_{uk}, SID_i, SID_j, PID_t\}$
    $Res_a \leftarrow PUF(Ch_{uk})$
    $B_{k1} \leftarrow Rep(Res_a, hdk1)$
    generate R_2 and T_1
    $P_2 \leftarrow \{R_2, SID_i \oplus R_2\}$
    $Ad_2 \leftarrow (PID_t \oplus T_1)$
    $((C_b, C_c), MAC_2) \leftarrow E_{B_{k1}}\{(Ad_2), (P_2)\}$
  else
    Stop the execution
  end if
end procedure

the process of deriving the encryption key using both PUF and FE. Subsequently, SD_k generates C_b, C_c, and MAC_2, combining them to construct the message M_1: $\{T_1, C_b, C_c, MAC_2\}$. This constructed message is then transmitted to GW_j via the public communication channel.

2) VERIFICATION OF M_1 AND GENERATION OF M_2

The timeliness of the received message M_1 is determined by evaluating the condition $T_{di} \leq |T_{re} - T_1|$, where T_{re}, T_1, and T_{di} represent the message reception time, generation time, and acceptable delay threshold, respectively. If this condition is not met, GW_j discards the message and halts the ASKG process. Upon successful validation of the condition, GW_j employs PUF and FE to compute the decryption key, which is then utilized to decrypt the data stored within its database. Subsequent to calculating the decryption key, GW_j extracts PID_t from the received message and searches for it within its internal database. In the event that PID_t is located, GW_j retrieves the corresponding ciphertext and authentication code associated with that specific PID_t.

Following the decryption process in the ASCON encryption Algorithm, the decryption itself is executed using the key K_{GW}, resulting in the acquisition of B_{k1} and MAC_u^*. The integrity of the stored data is verified by assessing the condition $MAC_u == MAC_u^*$. When $MAC_u == MAC_u^*$ is satisfied, GW_j confirms the authenticity of the received message and subsequently obtains $P_2 = (R_2, SIDi \oplus R_2)$ through a decryption operation involving the key B_{k1}. Furthermore, GW_j acquires SID_i and conducts a search within its internal database. Here, SID_i signifies the specific accessed device. In the event that SID_i is discovered within the database, GW_j proceeds to retrieve the ciphertext and authentication parameters associated with the corresponding SID_i from the database. Consequently, GW_j derives B_{kd} and MAC_d^*. To guarantee the integrity of B_{kd}, the condition $MAC_d == MAC_d^*$ is employed for validation. Moreover, GW_j computes P_3 and Ad_4. Additionally, it employs the encryption Algorithm to calculate C_d, C_e, and MAC_3. Furthermore, GW_j substitutes PID_t^n with PID_t^r and replaces PID_t^r

with PID_t^p. Subsequent to these operations, GW_j assembles a message named M_2, incorporating the parameters $\{T_2, C_d, C_e, C_f, MAC_3\}$. This assembled message is then transmitted to ISD_i via the public communication channel.

Algorithm 2 Verification of M_1 and Generation of M_2

Input: $\{T_1, PID_t, C_b, C_c, MAC_2, Ch_j\}$
Output: $\{T_2, C_d, C_e, C_f, MAC_3\}$
procedure ALG-2($\{T_1, PID_t, C_b, C_c, MAC_2, Ch_j\}$)
  if $T_{di} \leq |T_{re} - T_1|$ **then**
    $Res_j \leftarrow PUF(Ch_j)$
    $K_{GW} \leftarrow Rep(Res_j, hd)$
    Searches the PID_t database
    if $PID_t == PID_t^r$ or $PID_t == PID_t^p$ **then**
      gets (C_u, MAC_u)
      $(B_{k1}, MAC_u^*) \leftarrow D_{K_{GW}}\{C_u\}$
      if $MAC_u == MAC_u^*$ **then**
        $Ad_3 \leftarrow (PID_t \oplus T_1)$
        $(P_2, MAC_2^*) \leftarrow D_{B_{k1}}\{(Ad_3), C_b, C_c\}$
        if $MAC_2 == MAC_2^*$ **then**
          $P_2 \leftarrow (R_2, SID_i \oplus R_2)$
          $SID_i \leftarrow (R_2 \oplus P_2)$
          if SID_i is found in database **then**
            gets (C_d, MAC_d)
            $(B_{kd}, MAC_d^*) \leftarrow D_{K_{GW}}\{C_d\}$
            if $MAC_d == MAC_d^*$ **then**
              generate R_3, PID_t^n and T_2
              $P_3 \leftarrow \{R_3, R_2 \oplus PID_t \oplus SID_i, PID_t^n\}$
              $Ad_4 \leftarrow (SID_i \oplus T_2)$
              $((C_d, C_e), MAC_3) \leftarrow E_{B_{kd}}\{(Ad_4), (P_3)\}$
              replace PID_t^n with PID_t^r
              replace PID_t^r with PID_t^p
            else
              Stop the execution
            end if
          else
            Stop the execution
          end if
        else
          Stop the execution
        end if
      else
        Stop the execution
      end if
    else
      Stop the execution
    end if
  else
    Stop the execution
  end if
end procedure

3) VALIDATION OF M_2 AND CREATION OF M_3

Once confirming the freshness of the received message M_2, ISD_i proceeds to calculate B_{kd} utilizing the PUF and FE. Additionally, ISD_i generates Ad_5, and subsequently employs the ASCON decryption Algorithm to extract (P_3, MAC_3^*). The integrity of P_3 is verified by applying the condition $MAC_3 == MAC_3^*$. Upon validating that $MAC_3 == MAC_3^*$ holds true, ISD_i considers the received message to be both accurate and valid. After selecting R_4 and T_3, ISD_i derives the encryption key K_1 which will serve as the foundation for ASCON-based encryption. This process also involves determining the plaintext P_4, associating data Ad_6, and generating the session key SK_{ISD_i} that ensures secure encrypted communication in the future. Additionally, ISD_i calculates C_g, C_h, and MAC_4 using the ASCON encryption Algorithm. Finally, a message $\{T_3, C_g, C_h, Ad_6, MAC_4\}$ is meticulously constructed and subsequently transmitted to U_k via an open communication channel.

Algorithm 3 Validation of M_2 and Creation of M_3

Input: $\{T_2, C_d, C_e, C_f, MAC_3, Ch_i\}$
Output: $\{T_3, C_g, C_h, Ad_6, MAC_4$ and $SK_{ISD_i}\}$
procedure ALG-3($\{T_2, C_d, C_e, C_f, MAC_3, Ch_i\}$),
  if $T_{di} \leq |T_r - T_2|$ **then**
    $(Res_i) \leftarrow PUF(Ch_i)$
    $(B_{kd}) \leftarrow Rep(Res_i, hdi)$
    $SID_j \leftarrow Z \oplus H(B_{kd})$
    $Ad_5 \leftarrow (SID_i \oplus T_2)$
    $(P_3, MAC_3^*) \leftarrow D_{B_{kd}}\{(Ad_5), (C_d, C_e, C_f)\}$
    if $MAC_3 == MAC_3^*$ **then**
      $P_3 \leftarrow \{R_3, R_2 \oplus PID_t \oplus SID_i, PID_t^n\}$
      generate R_4 and T_3
      $K_1 \leftarrow H(R_2 \oplus PID_t \oplus SID_j \oplus SID_i \oplus T_3)$
      $P_4 \leftarrow \{PID_t^n, R_4 \oplus R_3\}$
      $SK_{ISD_i} \leftarrow H(K_1 \oplus P_4 \oplus SID_i)$
      $Ad_6 \leftarrow H(SK_{ISD_i})$
      $((C_g, C_h), MAC_4) \leftarrow E_{K_1}\{(Ad_6), (P_4)\}$
    else
      Stop the execution
    end if
  else
    Stop the execution
  end if
end procedure

4) VALIDATION OF M_3 AND CREATION OF SK_{UK}

Upon obtaining M_3, the U_k entity verifies the authenticity of M_3. Initially, U_k assesses the freshness of the message M_3 by applying the condition $T_{di} \leq |T_{re} - T_3|$. If M_3 is deemed fresh, U_k proceeds to derive the encryption key denoted as K_{enc}, which will be employed during the decryption process. Subsequent to decryption, U_k validates the condition $MAC_4 = MAC_4^*$ to ensure that the resulting plaintext P_4 is both valid and the received message maintains its authenticity. Moreover, U_k computes the session key referred to as SK_{uk}, serving the purpose of facilitating encrypted communications in subsequent interactions. Furthermore, the correctness of the session key is verified through the condition $Ad_6 = H(SK_{uk})$. Satisfying this criterion prompts U_k to substitute PID_t with PID_t. Proceeding, U_k calculates values for C_a and MAC_5^* using the ASCON encryption Algorithm. Ultimately, these computed values $\{C_a^*, MAC_5^*\}$ are replaced with $\{C_a, MAC_1\}$ in the memory of SD_k. The process outlined in Algorithm 4 is employed to validate M_3 and generate the session key SK_{uk}.

C. PASSWORD CHANGE PHASE

The proposed LEAF-IIoT scheme introduces the capability for users to modify or refresh their secret credentials. This functionality is established through Algorithm 5. Initially, the user submits their existing credentials and subsequently engages in a series of computations as demonstrated in Algorithm 5, resulting in the derivation of P_a^o and MAC_1^o. Furthermore, the authenticity of the retrieved plaintext is validated via the condition $MAC_1 == MAC_1^o$. Upon successful validation, the user gains permission to input new secret credentials. Subsequently, SD_k computes new parameters, specifically C_a^n and MAC_1^n, and subsequently

Algorithm 4 Validation of M_3 and Creation of SK_{uk}

Input: $\{T_3, C_g, C_h, Ad_6, MAC_4\}$
Output: $\{SK_{uk}$ and authentication successful$\}$

procedure ALG-4($\{T_3, C_g, C_h, Ad_6, MAC_4\}$),
  if $T_{di} \leq |T_{re} - T_3|$ **then**
    $K_2 \leftarrow H(R_2 \oplus PID_t \oplus SID_j \oplus SID_i \oplus T_3)$
    $(P_4, MAC_4^*) \leftarrow D_{K_2}\{(Ad_6), (C_g, C_h)\}$
    if $MAC_4 == MAC_4^*$ **then**
      $P_4 \leftarrow \{PID_t^n, R_4 \oplus R_3\}$
      $SK_{uk} \leftarrow H(K_1 \oplus P_4 \oplus SID_i)$
      if $Ad_6 == H(SK_{uk})$ **then**
        update PID_t^n with PID_t
        $P_a^* \leftarrow \{Ch_{uk}, SID_i, SID_j, PID_t^n\}$
        $(C_a, MAC_5^*) \leftarrow E_{A_1^*}\{(Ad_6), P_a^*\}$
        update $\{C_a^*, MAC_5^*\}$ with $\{C_a, MAC_1\}$
        both session keys are the same
        authentication successful
      else
        Stop the execution
      end if
    else
      Stop the execution
    end if
  else
    Stop the execution
  end if
end procedure

substitutes these calculated values C_a^n and MAC_1^n with C_a and MAC_1 in the memory storage of SD_k.

Algorithm 5 User Password and Bio-Metric Change

Input: $\{ID_{uk}, PW_{uk}^o, Bio_{uk}^o, C_a, MAC_1, hdk\}$
Output: $\{C_a^n, MAC_1^n, hdk^n\}$

procedure ALG-5($\{ID_{uk}, PW_{uk}^o, Bio_{uk}^o, C_a, MAC_1, hdk\}$)
  $B_k^o \leftarrow Rep(Bio_{uk}^o, hdk)$
  $A_1^o \leftarrow H(ID_{uk} \parallel PW_{uk}^o \parallel B_k^o)$
  $(P_a^o, MAC_1^o) \leftarrow D_{A_1^o}\{C_a^o\}$
  if $MAC_1 == MAC_1^o$ **then**
    $P_a^o \leftarrow \{Ch_{uk}, SID_i, SID_j, PID_t\}$
    Allow the user to generate new credentials
    $(B_k^o, hdk^n) \leftarrow Gen(Bio_{uk}^n,)$
    $A_1^n \leftarrow H(ID_{uk} \parallel PW_{uk}^n \parallel B_k^n)$
    $(C_a^n, MAC_1^n) \leftarrow E_{A_1^n}\{P_a^n\}$
  else
    Stop the execution
  end if
end procedure

VI. SECURITY VALIDATION

We undertake both informal (non-mathematical) and formal (mathematical) analyses to ensure the resilience of LEAF-IIoT against a range of security attacks. Additionally, we establish the robustness of LEAF-IIoT through formal proof, utilizing a software tool referred to as Scyther.

A. INFORMAL (NON-MATHEMATICAL) SECURITY ANALYSIS

1) PHYSICAL SECURITY USING PUF

A PUF at the GW_j in the proposed LEAF-IIoT decreases the likelihood of a privilege insider attack. By minimizing access to the long-term secret key in plaintext stored in the GW_j database, this integration protects against insider intrusion. PUF technology is additionally employed in SD_k, where it produces the secret key required to encrypt M_1. The lack of the PUF-generated private key at SD_k prevents an adversary from decrypting M_1. Likewise to this, PUF technology is implemented to generate the secret key for the ISD_i, preserving the encrypted data of secret parameters for the ISD_i. This approach prevents attacks regardless of the event that an attacker manages to get hold of ISD_i since they are incapable to execute any more attacks. Thus, PUF has been integrated in the LEAF-IIoT framework to boost its resistance against a wide range of potential attacks.

2) PRIVILEGED INSIDER ATTACK

In this scenario, the potential attacker might indeed be legitimate but curious. This attacker could gain access to sensitive information related to users and ISDs within the IIoT environment from the GW_j's database. By utilizing this extracted information, the attacker could execute various malicious actions. However, in the proposed LEAF-IIoT framework, the attacker can only obtain $\{SID_i, C_a, Tag_a\}$ and $\{ID_j, hd, Ch_j\}$ from GW_j's database. Extracting K_{GW}, B_{k1}, and B_{kd} from the information stored GW_j's database in poses a considerable challenge to the attacker. These keys are vital to carrying out potential insider attacks. Notably, K_{GW} is generated via the PUF function, while K_{ISD} is stored in an encrypted state. The credentials at hand, including $\{PID_t, C_u, MAC_u\}$, $\{SID_i, C_d, MAC_d\}$ and $\{ID_j, hd, Ch_j\}$, do not provide the inside attacker with the means to execute any form of attack. Consequently, the LEAF-IIoT proposal demonstrates resilience against privileged insider attacks.

3) JAMMING ATTACK

The execution of LEAF-IIoT is constantly under threat from jamming attacks, which poses a serious risk to the ongoing procedure. These attacks have the potential to seriously impede LEAF-IIoT's progress and, more concerningly, jeopardize the security system's overall efficacy. For instance, the device access phase can fail if a jamming attack is used, as seen in the example in [26]. The procedure in [26] of updating pseudo identities during the drone access phase is responsible for this failure. The LEAF-IIoT, in comparison, takes a different tack by forgoing the exchange of fictitious identities once the ASKG phase has been successfully completed. This crucial distinction allows the LEAF-IIoT to effectively shield against jamming attacks, safeguarding the integrity of this critical phase.

4) SECRET CREDENTIAL CHANGE ATTACK

This attack is executed offline by the malicious actor upon capturing the SD_k of the user. Within this SD_k are critical parameters, specifically $\{C_a, MAC_1, hdk, hdk1\}$, which are stored in its memory. Once in possession of these parameters, the attacker's objective is to alter the user's secret credentials. To achieve this, the attacker employs a series of steps involving the selection of random passwords, identities, and biometric information, followed by the following computations $B_k' = Rep(Bio_{uk}', hdk)$ $A_1' = H(ID_{uk} \parallel PW_{uk}^o \parallel B_k^o)$, and $(P_a', MAC_1') = D_{A_1'}\{C_a'\}$. Finally, the attacker must validate the condition $MAC_1 == MAC_1'$. If this condition is met, the attacker gains the ability to modify the user's secret credentials. Nonetheless, it's crucial to note that the attacker cannot alter these secret credentials without prior knowledge of the valid ones. Hence, the proposed scheme LEAF-IIoT resists the password change attack or secret credential change attack.

5) ANONYMITY/UNTRACEABILITY

In this scenario, the assailant attempts to track the participants engaged in the ASKG process by intercepting the messages, denoted as M_1 :$\{T_1, PID_t\ C_b, C_c, MAC_2\}$, M_2 :$\{T_2, C_d, C_e, C_f, MAC_3\}$, and M_3 :$\{T_3, C_g, C_h, Ad_6, MAC_4\}$. Despite these intercepted messages, the attacker faces significant challenges in acquiring the necessary information to trace the network entities, including users. This challenge arises because all transmitted messages undergo encryption through the ASCON encryption Algorithm. Consequently, the attacker is incapable of extracting any identifying information such as ID_{uk}, which is crucial for user tracking. Moreover, the messages are intentionally designed to be random, preventing the attacker from establishing connections between messages sourced from the same origins. Given these stringent security measures, the proposed LEAF-IIoT system ensures that the attacker cannot obtain any parameters necessary for tracing specific entities within the IIoT environment. In essence, LEAF-IIoT boasts features that provide anonymity and untraceability.

6) REPLAY ATTACK

In this cyberattack, the perpetrator intercepts all the transmitted messages that occur during the execution of the ASKG phase within the LEAF-IIoT system. The attacker then attempts to manipulate these captured messages. However, the communication messages are embedded with the latest timestamps, and the legitimacy of these incorporated timestamps is verified at the recipient entity. To elaborate, there are distinct conditions denoted as $T_{di} \leq |T_{re} - T_1|$, $T_{di} \leq |T_{re} - T_2|$, and $T_{di} \leq |T_{re} - T_3|$, which are individually inspected to ensure that the received message's timeline aligns appropriately with the expectations at GW_j, ISD_i, and U_k, respectively. If a received message surpasses the acceptable time delay, it will be disregarded, leading to an interruption in the ASKG process. Hence, the proposed LEAF-IIoT framework effectively thwarts replay attacks.

7) U_K IMPERSONATION ATTACK

In this scenario, the attacker attempts to create a message with specific parameters, denoted as M_1' :$\{T_1', PID_t', C_b', C_c', MAC_2'\}$, in order to impersonate a legitimate U_k. To craft a valid message M_1', the attacker would need knowledge of the legitimate B_{k1}, which is generated through a process involving PUF and FE. B_{k1} serves as the encryption key for generating the parameters C_b, C_c, and MAC_2. However, the attacker lacks the capability to determine the correct B_{k1}, and consequently, cannot produce the legitimate parameters C_b, C_c, and MAC_2. Furthermore, GW_j checks whether the condition $MAC_2 == MAC_2^*$ holds to ensure the integrity of message M_1, a condition that cannot be satisfied without knowing of B_{k1}. As a result, the attacker cannot successfully impersonate the legitimate U_k. Thus, the proposed LEAF-IIoT resists the U_k impersonation attack.

8) GW_J IMPERSONATION ATTACK

In this scenario, the attacker endeavors to fabricate a message with specific parameters denoted as M_2' : $\{T_2, C_d', C_e', C_f', MAC_3'\}$, with the aim of assuming the genuine GW_j. To create a valid message M_2', the attacker would need access to the legitimate B_{kd}, which is stored in the database of GW_j. B_{kd} acts as the encryption key for generating the parameters C_d, C_e, C_f, and $MAC4$. However, the attacker lacks the capability to ascertain the correct B_{kd}, and consequently, cannot generate the genuine parameters C_d, C_e, C_f, and MAC_3. Furthermore, ISD_i verifies whether the condition $MAC_3 == MAC_3^*$ is satisfied to ensure the integrity of message M_2, a condition that cannot be met without knowledge of B_{kd}. Consequently, the attacker is thwarted in their attempt to successfully impersonate the authentic GW_j.

9) ISD_I IMPERSONATION ATTACK

In this attack scenario, the malevolent actor attempts to craft a message denoted as M_3' :$\{T_3, C_g', C_h', Ad_6', MAC_4'\}$ with the intention of impersonating the legitimate ISD_i. However, the successful creation of a valid message M_3 is made difficult due to the absence of essential parameters, namely SID_j and K_1. These parameters are crucial for constructing a message that can be recognized as legitimate. Furthermore, the condition U_k employs to verify the authenticity of a received message from SID_j relies on the equality of MAC_4 and MAC_4^*. This condition cannot be satisfied without access to the confidential parameters SID_j and K_1, which are exclusively known to both U_k and ISD_i. Consequently, the proposed LEAF-IIoT system proves effective in thwarting impersonation attacks against ISD_i.

10) MITM ATTACK

In LEAF-IIoT, three messages are exchanged: M_1 :$\{T_1, PID_t, C_b, C_c, MAC_2\}$, M_2 :$\{T_2, C_d, C_e, C_f, MAC_3\}$, and M_3 :$\{T_3, C_g, C_h, Ad_6, MAC_4\}$. An attacker, having intercepted these messages and tampered with their contents, attempts to resend them to a specific entity in order to establish a session key. However, in LEAF-IIoT, all messages undergo validation at the receiving entity based on the conditions $MAC_2 == MAC_2^*$, $MAC_3 == MAC_3^*$, and $MAC_4 == MAC_4^*$. These conditions can only be satisfied when the sensitive secret parameters are available. If any of these conditions fail to hold true, the ASKG process will be terminated. Consequently, LEAF-IIoT proves effective in thwarting MITM attacks.

TABLE 3. BAN logic notations and inference rules.

Notation	Meaning
$B\mid\equiv X$	B is convinced of the veracity of X
$B \triangleleft X$	B has obtained message X
$B\mid\sim X$	B has transmitted message X
$B \Longrightarrow X$	B has jurisdiction over X
X_K	X is encrypted under the key K
$B \overset{K}{\leftrightarrow} Q$	B and Q can communicate with the shared key K
(X,Y)	X or Y is a part of the message (X,Y)
Rules	**BAN Inference**
Message Meaning Rule (MMR):	$\frac{B\mid\equiv B \overset{K}{\leftrightarrow} Q, P\triangleleft X_K}{B\mid\equiv Q\mid\sim X}$
Nonce verification rule (NVR):	$\frac{B\mid\equiv\#(X), B\mid\equiv Q\mid\sim X}{B\mid\equiv Q\mid\equiv X}$
Jurisdiction rule (JR):	$\frac{B\mid\equiv Q\mid\Longrightarrow X, P\mid\equiv Q\mid\equiv X}{B\mid\equiv X}$
Belief rule (BR):	$\frac{B\mid\equiv(X,Y)}{B\mid\equiv X}$
Freshness rule (FR):	$\frac{B\mid\equiv\#(X)}{B\mid\equiv\#(X,Y)}$

11) TEMPORARY SECRET LEAKAGE ATTACK

In the LEAF-IIoT proposed framework, the session key employed for encrypting future communications is determined as follows: $SK_{uk}(= SK_{ISD_i}) = H(K_1 \oplus P_4 \oplus SID_i)$, with $P_4 = \{PID_t^n, R_4 \oplus R_3\}$. This session key computation combines both long-term and short-term parameters. To compromise the security of this session key, an attacker would need to possess knowledge of both the short-term and long-term secret parameters

12) DOS ATTACK

In the LEAF-IIoT proposal, the user's smart device SD_k is required to complete a local authentication step before transmitting an authentication request to GW_j, aimed at mitigating potential DoS attacks. This involves verifying a condition: $MAC_1 == MAC_1^*$. If this condition is met, SD_k proceeds to send an authentication request to GW_j. However, if the condition is not satisfied, the ASKG process is terminated, and no authentication request is forwarded to GW_j. This strategy effectively safeguards against DoS attacks in the LEAF-IIoT system.

B. BAN LOGIC ANALYSIS

A formal security protocol analysis method called Burrows-Abadi-Needham (BAN) logic is employed to confirm the accuracy of the cryptographic protocol. The thorough and methodical reasoning regarding the authentication characteristics of cryptographic systems is made possible by the BAN logic. It entails examining the transmission of messages and cryptographic operations within a protocol employing formal rules and inference methods. The following are the key elements of BAN logic:

Beliefs: Beliefs constitute an entity's perceptions of the messages it has received, its understanding of the system, and the actions of other entities.

Messages: In the protocol, messages are passed back and forth between different parties. Every message has a distinctive organization, and its content is symbolically represented.

Rules of Inference: Based on the beliefs and messages communicated between parties, the BAN logic provides a set of rules of inference allowing conclusions to be drawn. The BAN logic notations and inference rules are given in Table 3.

1) GOALS

We set forth the following objectives that the LEAF-IIoT should meet through the analytical processes of BAN logic.

- Goal-1: $(U_k \overset{SK_{U_k}}{\leftrightarrow} ISD_i)$
- Goal-2: $(ISD_i \overset{SK_{ISD_i}}{\leftrightarrow} U_k)$

2) ASSUMPTIONS

We have formulated the following initial assumptions to substantiate the security of the proposed LEAF-IIoT.

- AS_1: $(U_k\mid\equiv U_k \overset{B_{k1}}{\leftrightarrow} GW_j)$
- AS_2: $(GW_j\mid\equiv GW_j \overset{B_{k1}}{\leftrightarrow} U_k)$
- AS_3: $(GW_j\mid\equiv GW_j \overset{B_{kd}}{\leftrightarrow} ISD_i)$
- AS_4: $(ISD_i\mid\equiv ISD_i \overset{B_{kd}}{\leftrightarrow} GW_j)$
- AS_5: $(ISD_i\mid\equiv ISD_i \overset{K_1}{\leftrightarrow} U_k)$
- AS_6: $(U_k\mid\equiv U_k \overset{K_1}{\leftrightarrow} ISD_i)$
- AS_7: $(U_k\mid\equiv \#T_1, \#T_3)$
- AS_8: $(GW_j\mid\equiv \#T_1, \#T_2)$
- AS_9: $(ISD_i\mid\equiv \#T_3, \#T_2)$
- AS_{10}: $(U_k\mid\equiv \#R_1)$
- AS_{11}: $(GW_j\mid\equiv \#R_2)$
- AS_{12}: $(ISD_i\mid\equiv \#R_3)$
- AS_{13}: $(ISD_i\mid\equiv U_k\mid\equiv (P_4)$

3) IDEALIZE FORM

In LEAF-IIoT, there are three messages exchanged to accomplish the ASKG phase. The idealized form of the communicated message can be defined as follows

- $IF_1 : \{T_1, R_2, SID_i, MAC_2\}_{B_{k1}}$
- IF_2:$\{T_2, R_2, R_3, MAC_3\}_{B_{kd}}$
- IF_3:$\{T_3, P_4, R_4, MAC_4\}_{K_1}$

4) SECURITY ANALYSIS

During this stage of BAN logic, the inference rules as presented in Table 3 are employed to ascertain whether LEAF-IIoT has successfully met its security objectives.

- **Step-1:** Utilizing the idealized representation IF_1 for the message M_1 and making reference to the assumptions AS_1, AS_2, and AS_7, while employing the MMR technique, we obtain the subsequent outcome:

$$\frac{GW_j\mid\equiv(U_k \overset{B_{k1}}{\leftrightarrow} GW_j), GW_j \triangleleft (\{T_1, R_2, SID_i, MAC_2\}_{B_{k1}})}{GW_j\mid\equiv U_k\mid\sim (\{T_1, R_2, SID_i, MAC_2\}_{B_{k1}})}. \tag{1}$$

From 1, it can be concluded that

$$GW_j\mid\equiv (\{T_1, R_2, SID_i, MAC_2\}_{B_{k1}}) \tag{2}$$

- **Step-2:** By leveraging IF_1, considering AS_7 and AS_{10}, and employing the FR, we can reach the following conclusion:

$$\frac{GW_j \mid\equiv \#(T_1)}{GW_j \mid\equiv \#(\{T_1, R_2, SID_i, MAC_2\}_{B_{k1}})}. \quad (3)$$

Based on Equation 2, we can infer that the received message is indeed recent or newly generated.

- **Step-3:** By following the outlined steps and applying the NVR, it becomes feasible to acquire (4), as shown at the bottom of the next page:
From 4, it can be concluded that

$$GW_j \mid\equiv (\{T_1, R_2, SID_i, MAC_2\}_{B_{k1}}) \quad (5)$$

- **Step-4:** Building upon Step-2 and applying the BR, we have arrived at the following deduction:

$$\frac{GW_j \mid\equiv U_k \mid\equiv (\{T_1, R_2, SID_i, MAC_2\}_{B_{k1}})}{GW_j \mid\equiv U_k \mid\equiv (R_2, SID_i)}. \quad (6)$$

Based on the equation provided above, GW_j can obtain R_1 and SID_i, leading to the following conclusion:

$$GW_j \mid\equiv U_k \mid\equiv (R_2, SID_i) \quad (7)$$

- **Step-5:** By employing the idealized form IF_1 for message M_1 and taking into account assumptions AS_3, AS_4, and AS_8, along with the application of the MMR technique, we derive the following result:

$$\frac{GW_j \mid\equiv (U_k \overset{B_{kd}}{\leftrightarrow} GW_j), GW_j \triangleleft (\{T_2, R_2, R_3, MAC_3\}_{B_{kd}})}{GW_j \mid\equiv U_k \mid\sim (\{T_2, R_2, R_3, MAC_3\}_{B_{kd}})}. \quad (8)$$

From above we can conclude that

$$GW_j \mid\equiv (\{T_2, R_2, R_3, MAC_3\}_{B_{kd}}) \quad (9)$$

- **Step-6:** Based on IF_2 and considering AS_8 and AS_{11}, applying the FR leads to the following conclusion:

$$\frac{ISD_i \mid\equiv \#(T_2)}{GW_j \mid\equiv \#(\{T_2, R_2, R_3, MAC_3\}_{B_{kd}})}. \quad (10)$$

From 7, it can be concluded that

$$ISD_i \mid\equiv (\{T_2, R_2, R_3, MAC_3\}_{B_{kd}}) \quad (11)$$

- **Step-7:** Drawing from the information presented in Step-5 and Step-6, and utilizing the NVR approach, it becomes feasible to attain (12), as shown at the bottom of the next page:
From above we can conclude that

$$ISD_i \mid\equiv (\{T_2, R_2, R_3, MAC_3\}_{B_{kd}}) \quad (13)$$

- **Step-8:** Taking into account the aforementioned steps and employing the BR, the following outcomes can be realized as:

$$\frac{ISD_i \mid\equiv GW_j \mid\equiv (\{T_2, R_2, R_3, MAC_3\}_{B_{kd}})}{ISD_i \mid\equiv GW_j \mid\equiv (R_2, R_3)}. \quad (14)$$

From 14, it can be concluded that

$$ISD_i \mid\equiv GW_j \mid\equiv (R_2, R_3) \quad (15)$$

- **Step-9:** Now, by applying AS_{13} repeatedly and incorporating the conclusion derived from the preceding steps, we can get $ISD_i \mid\equiv SK_{ISD_i}$. In addition, we can arrive at the following:

$$(ISD_i \overset{SK_{ISD_i}}{\leftrightarrow} U_k) \quad (Goal - 1) \quad (16)$$

- **Step-10:** Utilizing the idealized representation IF_3 for message M_3 and taking into account assumptions AS_5 and AS_6, along with the application of the MMR approach, we obtain the following:

$$\frac{U_k \mid\equiv (iSD_I \overset{K_1}{\leftrightarrow} U_k), U_k \triangleleft (\{T_3, P_4, R_4, MAC_4\}_{K_1})}{U_k \mid\equiv ISD_i \mid\sim (\{T_3, P_4, R_4, MAC_4\}_{K_1})}. \quad (17)$$

From above we can conclude that

$$U_k \mid\equiv (\{T_3, P_4, R_4, MAC_4\}_{K_1}) \quad (18)$$

- **Step-11:** By using AS_9 and AS_{12} and by applying FR. We can conclude the following

$$\frac{U_k \mid\equiv \#(T_3)}{U_k \mid\equiv \#(\{T_3, P_4, R_4, MAC_4\}_{K_1})}. \quad (19)$$

- **Step-12:** Based on Step 10 and by applying the NVR, it is possible to obtain (20), as shown at the bottom of the next page
From above we can conclude that

$$U_k \mid\equiv (\{T_3, P_4, R_4, MAC_4\}_{K_1}) \quad (21)$$

- **Step-13:** Based on Step 11 and by applying the BR, we can achieve the following

$$\frac{U_k \mid\equiv ISD_i \mid\equiv (\{T_3, P_4, R_4, MAC_4\}_{K_1})}{U_k \mid\equiv ISD_i \mid\equiv (P_4, R_4)}. \quad (22)$$

From above we can conclude that

$$U_k \mid\equiv ISD_i \mid\equiv (P_4, R_4) \quad (23)$$

- **Step-14:** Now, by applying AS_{13} repeatedly and incorporating the conclusion derived from the preceding steps, we can get $U_k \mid\equiv SK_{U_k}$. In addition, we can arrive at the following:

$$(U_k \overset{SK_{U_k}}{\leftrightarrow} ISD_i) \quad (Goal - 2) \quad (24)$$

C. SCYTHER TOOL-BASED VALIDATION

Scyther is a tool for automatically verifying security protocols, and it is employed for analyzing cryptographic protocols for probable security flaws. For assessing the security features of cryptographic protocols, Scyther makes utilization of formal techniques and symbolic analysis tools. It takes advantage of the DY model, which implies that cryptographic primitives are fully secure, and it emphasizes the analysis of protocol messaging and potential attacks.

The Scyther tool's key characteristics include Input Description: Utilizing a simple and comprehensible input language, the user provides the protocol specification.

TABLE 4. Scyther parameters settings.

Parameters	Setting
“Maximum number of runs"	5
“Matching type"	Find all types of flaws
“Search pruning"	Find all attacks
“Maximum number of patterns per claim "	6

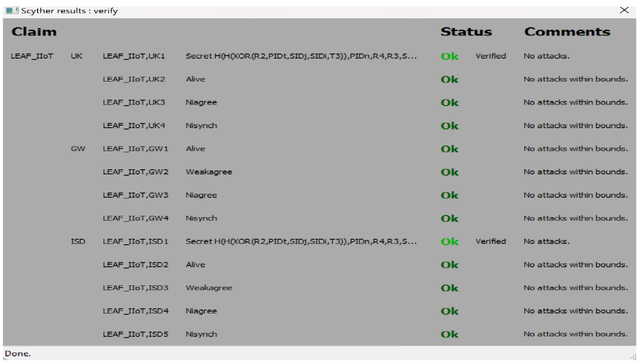

FIGURE 2. Security analysis of Scyther using LEAF-IIoT.

The protocol's messages, cryptographic procedures, and assumptions on the adversary's capacities are all specified in this specification. Automatic Verification: Scyther evaluates the protocol specification programmatically by checking for security features like authentication, secrecy, and freshness. It investigates potential attack conditions by simulating the adversary's actions. Reporting Vulnerabilities: If Scyther finds possible security flaws in the protocol, it creates a comprehensive report detailing the precise attacks that an adversary could launch. Cryptographic Primitives: Scyther implements a broad range of cryptographic primitives that are commonly employed in cryptographic protocols, which makes it advantageous in a variety of real-world scenarios. Interactive Mode: Scyther also provides a mode that is interactive that enables users to interactively examine the functioning of the protocol and improve their analysis.

In this article, we'll be employing Scyther to evaluate LEAF-IIoT's security attributes. The Security Protocol Description Language (SPDL) is the language utilized for the implementation of LEAF-IIoT, and it contains three roles: the GW_j gateway role, the ISD_i IIoT smart device role, and the U_k/SD_k user role. As seen in Figure 2, the SPDL code contains claims both manually established and autonomously generated, all of which are subject to Scyther inspection. According to this investigation, LEAF-IIoT is very well protected and secure, as can be seen in Figure 2. Considering the Scyther parameters that are shown in Table 4, we accomplish the security analysis. All the security properties are explained in the Table 5.

VII. PERFORMANCE COMPARISON

In this section, we assess the effectiveness of the LEAF-IIoT approach by examining its computational, communication, and storage costs in comparison to the ASKG framework introduced by Wazid et al. [26], Irshad et al. [1], Sutrala et al. [27], Srinivas et al. [20], and Sureshkumar et al. [28]. For simulating GW_j, we employed a system (setup-2) equipped with an Intel(R) Core(TM) i3 Processor @ 3.0GHz and 4GB of RAM, running the Ubuntu operating system. Furthermore, to simulate devices ISD_i and SD_k, we utilized a Raspberry Pi-3 system (setup-1) with a CPU clocked at 1.2 GHz and 1GB of RAM, also running the Ubuntu operating system. We utilized the Python-based cryptographic library ‘Pycrypto’ for implementing the proposed LEAF-IIoT. PUF's execution time (T_{pu}) 54μs [32]. Additionally, we employed the Python code available at [10] for ASCON. The execution times for each cryptographic primitive are presented in Table 6, which were derived from one hundred executions of each cryptographic primitive.

A. ANALYSIS OF SECURITY FEATURES

When considering Wazid et al. [26], it exhibits vulnerability to identity de-synchronization and privilege insider attacks. As for Srinivas et al. [20], its security strategy proves to be susceptible to identity guessing, man-in-the-middle (MITM) attacks, privilege insider issues, as well as user and device impersonation threats. In the case of the framework proposed in [1], it fails to provide adequate resistance against privileged insider attacks due to the storage of all secret information in an unencrypted form, potentially enabling attackers to exploit this information for various types of attacks. Furthermore, the scheme presented in [27] is also incapable of resisting de-synchronization and shares a similar vulnerability as the scheme in [1]. Similarly, the scheme

$$\frac{GW_j \mid\equiv \#(\{T_1, R_2, SID_i, MAC_2\}_{B_{k1}}),\ GW_j \mid\equiv U_k \mid\sim (\{T_1, R_2, SID_i, MAC_2\}_{B_{k1}})}{GW_j \equiv U_k \mid\equiv (\{T_1, R_2, SID_i, MAC_2\}_{B_{k1}})}. \quad (4)$$

$$\frac{ISD_i \mid\equiv \#(\{T_2, R_2, R_3, MAC_3\}_{B_{kd}}),\ ISD_i \mid\equiv GW_j \mid\sim (\{T_2, R_2, R_3, MAC_3\}_{B_{kd}})}{ISD_i \equiv GW_j \mid\equiv (\{T_2, R_2, R_3, MAC_3\}_{B_{kd}})}. \quad (12)$$

$$\frac{U_k \mid\equiv \#(\{T_3, P_4, R_4, MAC_4\}_{K_1}),\ U_k \mid\equiv ISD_i \mid\sim (\{T_3, P_4, R_4, MAC_4\}_{K_1})}{U_k \equiv ISD_i \mid\equiv (\{T_3, P_4, R_4, MAC_4\}_{K_1})}. \quad (20)$$

TABLE 5. Explanation of security properties.

Security Property	Explanation
"Alive"	"Alive" is to provide evidence that a communication party successfully carried out particular actions.
"Weakagree"	The protocol ensures that there is weak agreement between one participant and the other when Weakagree happens to be reached.
"Niagree"	Niagree shows the protocol provides data consistency and unilateral authentication during the protocol's overall execution.
"Nisynch"	Nisynch means that every message sent by the sender is received by the receiver.

TABLE 6. Execution time and parameters size.

Primitive	Setup-1	Setup-2	Size of Parameters
"SHA Execution Time (T_h)"	0.07 ms	0.037 ms	SHA output size 256 bits
"ECC Execution Time (T_{ec})"	1.57 ms	0.76 ms	ECC output size 320 bits
"ECC Addition Execution Time (T_{ea})"	0.090 ms	0.030 ms	MAC output size 128 bits
"Symmetric Encryption Execution Time (T_{enc}) "	0.61 ms	0.5 ms	AES block size 128 bits
"FE Execution Time (T_b)"	1.57 ms	0.76 ms	Random number size 128 bits
"ASCON Execution Time (T_{as})"	0.42 ms	0.039 ms	Block size 128 bits

TABLE 7. Analysis of security features.

Scheme/Features	PUF	PIA	DoS	MITM	DSA	IA	DSA	SLA
Wazid [26]	×	×	✓	✓	×	✓	✓	✓
Irshad [1]	×	×	✓	✓	✓	✓	✓	✓
Anil [27]	×	×	✓	✓	×	✓	✓	✓
Srinivas [20]	×	×	✓	×	✓	×	✓	✓
Sureshkumar [28]	×	×	✓	×	✓	✓	✓	×
LEAF-IIoT	✓	✓	✓	✓	✓	✓	✓	✓

PUF: "Physical uncloneable function", PIA: "Privileged insider attack", DSA: "De-Synchronization attack", IA: "Impersonation attack ", MITM: "MITM attack", AU: "Anonymity/Un-traceability", SLA: " Secret leakage attack", ✓"indicates that a feature is provided"; × "indicates that a feature is not provided".

TABLE 8. Communication and computational cost analysis.

Framework/Scheme	Computational Cost	Communication Cost
Wazid [26]	$32T_h + 13T_{ec} + 3T_{ea} + T_b \approx [20.32]$ **ms**	**3360 bits**
Irshad [1]	$34T_h + 8T_{ec} + 7T_{ea} + T_b \approx [18.65]$ **ms**	**3040 bits**
Anil [27]	$33T_h + 12T_{ec} + 5T_{ea} + T_b \approx [20.27]$ **ms**	**3200 bits**
Srinivas [20]	$35T_h + 8T_{ec} + 4T_{ea} + T_b \approx [21.15]$ **ms**	**2656 bits**
Sureshkumar [28]	$35T_h + 8T_{ec} + 4T_{ea} + T_b \approx [21.32]$ **ms**	**4416 bits**
LEAF-IIoT	$11T_h + 7T_{enc} + 5T_{cm} + T_b \approx [8.66]$ **ms**	**1760 bits**

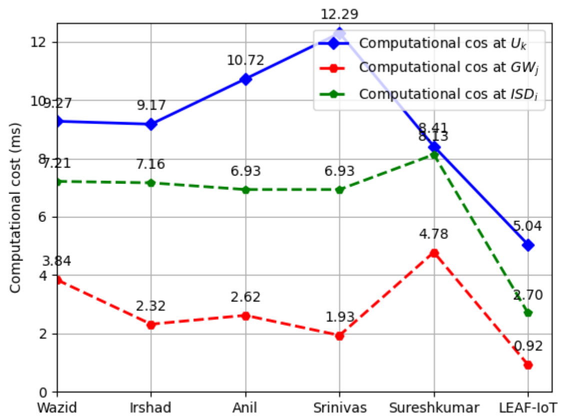

FIGURE 3. Computational cost required by SD_k, GW_j, and ISD_i during the completion of ASKG phase.

introduced in [28] demonstrates weaknesses against MITM attacks and temporary secret leakage. In contrast, LEAF-IIoT not only stands strong against privileged insider threats but also bolsters physical security.

B. ANALYSIS OF COMPUTATIONAL COST

The assessment of computational cost for the proposed LEAF-IIoT framework is detailed in this section. To evaluate the computational cost of LEAF-IIoT, we analyze the computational intricacies of various cryptographic primitives, as outlined in Table 6. The cumulative computational cost of LEAF-IIoT is $7T_h + 10T_{as} + 4T_b + 4T_{pu} \approx 8.66$ ms. Furthermore, the computational costs at SD_k, GW_j, and ISD_i are denoted as $3T_h + 4T_{as} + 2T_b + 2T_{pu} \approx 5.04$ ms, $4T_{as} + T_{pu} + T_b \approx 2.70$ ms, and $4T_h + 2T_{as} + T_{pu} + T_b \approx 0.92$ ms, respectively. In the ASKG framework introduced in [26], the computational requirements for U_k, GW_j, and ISD_i are given as $19T_h + 4T_{ec} + T_{ea} + T_b \approx 9.27$ ms, $T_h + 5T_{ec} + T_{ea} \approx 7.21$ ms, and $12T_h + 4T_{ec} + T_{ea} \approx 3.84$ ms, respectively. The total computation demanded by the framework proposed in [26] sums up to $32T_h + 13T_{ec} + 3T_{ea} + T_b \approx 20.32$ ms. In the ASKG presented in [1], the computational costs at U_k, GW_j, and ISD_i are $15T_h + 4T_{ec} + 3T_{ea} + T_b \approx 9.17$ ms, $9T_h + 2T_{ec} + 2T_{ea} + 2T_{enc} \approx 7.16$ ms, and $10T_h + 4T_{ec} + 2T_{ea} \approx 2.32$ ms, respectively. The total computation required by the framework proposed in [1] is $34T_h + 8T_{ec} + 7T_{ea} + 2T_{enc} + T_b \approx 18.65$ ms. In the ASKG framework detailed in [27], the computational cost for U_k, GW_j, and ISD_i amount to $16T_h + 5T_{ec} + 2T_{ea} + T_b \approx 10.72$ ms, $9T_h + 3T_{ec} + 2T_{ea} \approx 6.93$ ms, and $8T_h + 4T_{ec} + T_{ea} \approx 2.62$ ms, respectively. The overall computational load imposed by the ASKG framework proposed in [27] is approximately $33T_h + 12T_{ec} + 5T_{ea} + T_b \approx 20.27$ ms. In an ASKG framework introduced in [20], the computational costs at U_k, GW_j, and ISD_i are also expressed as $16T_h + 6T_{ec} + 2T_{ea} + T_b \approx 12.29$ ms, $11T_h + 2T_{ec} + 2T_{ea} \approx 6.93$ ms, and $8T_h + 4T_{ec} + T_{ea} \approx 1.93$ ms, respectively. The total computation required by this framework is $35T_h + 12T_{ec} + 5T_{ea} + T_b \approx 21.15$ ms. In an ASKG framework introduced in [28], the computational costs at U_k, GW_j, and ISD_i are likewise expressed as $8T_h + 5T_{ec} \approx 8.41$ ms, $6T_h + 6T_{ec} \approx 8.13$ ms, and $4T_h + 5T_{ec} \approx 4.78$ ms, respectively. The total computation required by this framework is $18T_h + 16T_{ec} \approx 21.32$ ms. Based on the observations made in Fig. 3 and Fig. 4, it is evident that the LEAF-IIoT requires a lower computational cost compared to the state-of-the-art ASKG framework. Specifically, LEAF-IIoT exhibits performance improvements of 57.4%, 53.58%, 57.3%, 59.08%, and 59.41% in comparison to the related ASKG frameworks.

It is crucial to acknowledge the possibility of unforeseen circumstances or the emergence of new types of attacks that could potentially disrupt the execution of LEAF-IIoT. While the LEAF-IIoT technique has demonstrated its resilience and effectiveness in countering attacks within the predefined threat model, it's important to consider the likelihood of random attacks, such as jamming attacks, occurring at any

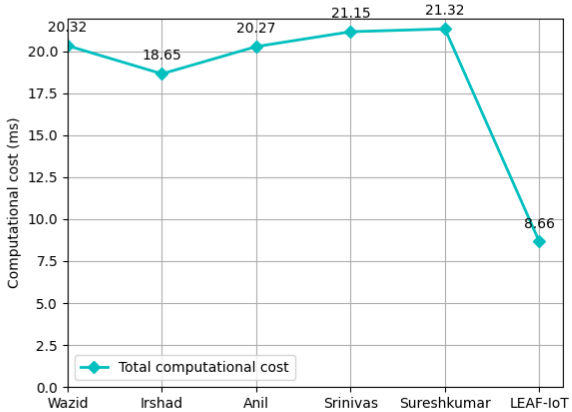

FIGURE 4. Aggregated computational cost required for completion of ASKG phase.

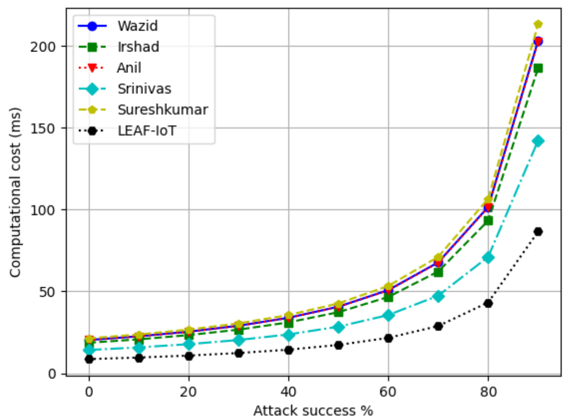

FIGURE 5. Computational cost required to accomplish the ASKG phase in the presence of an attack.

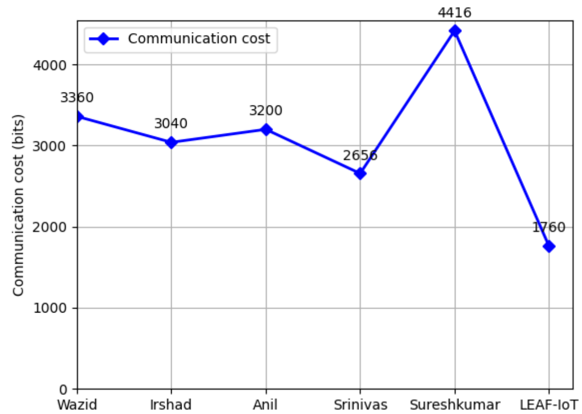

FIGURE 6. Communication cost required to complete the ASKG phase.

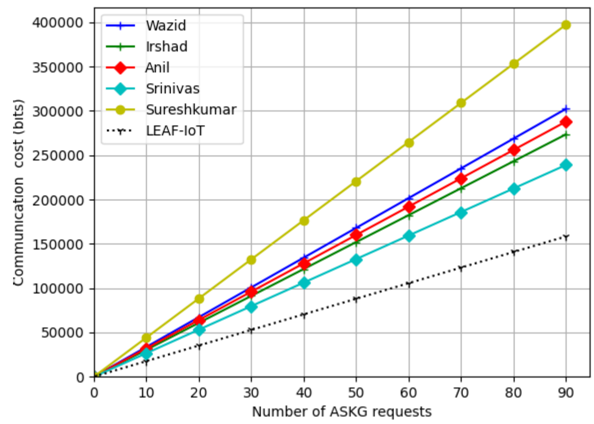

FIGURE 7. Communication cost required to complete the ASKG phase with increasing the number of authentication requests.

point during the LEAF-IIoT framework's execution, which could lead to interruptions. To assess the performance of the LEAF-IIoT framework and determine the average duration required to complete the drone access phase, we conducted 100 protocol runs. The computational cost can be computed as $ct = \frac{\sum_{i=1}^{100} T_i}{100\times(1-\text{Likelihood of effective attacks})}$. In our analysis, the term $\sum T_i$ denotes the cumulative number of protocol runs, and 'ct' represents the total computational time needed to complete the authentication phase within the LEAF-IIoT framework. As the count of successful attacks rises, the average time required for the entire execution of the LEAF-IIoT framework also increases. This phenomenon is a consequence of the occurrence of attacks, which can temporarily halt the LEAF-IIoT process. Subsequently, LEAF-IIoT resumes its execution, resulting in an extended overall execution time. Figure 8 provides a visual comparison of the time consumed for authentication during handovers between the LEAF-IIoT framework and related frameworks.

C. ANALYSIS OF COMMUNICATION COST

The communication process of the LEAF-IIoT system is orchestrated while accounting for credentials of varying sizes, as outlined in Table 6. This communication involves three distinct messages: M_1, M_2, and M_3, each associated with parameters $\{T_1, PID_t\ C_b, C_c, MAC_2\}$, $\{T_2, C_d, C_e, C_f, MAC_3\}$, and $\{T_3, C_g, C_h, Ad_6, MAC_4\}$, respectively. The sizes of these messages are 544 bits, 544 bits, and 672 bits, resulting in a cumulative total of $\{544 + 544 + 672\} = 1760$ bits.

In the context of the ASKG scenario detailed in [26], the bit exchange unfolds as follows: U_k sends 1152 bits to GW_j, GW_j forwards 1184 bits to ISD_i, and ISD_i sends back 1024 bits to U_k. The cumulative bit exchange during the ASKG phase amounts to 3360 bits. In the context of the ASKG scenario outlined in [1], the bit exchange unfolds as follows: U_k sends 1312 bits to GW_j, GW_j forwards 1344 bits to ISD_i, and ISD_i transmits 384 bits in return to U_k. In aggregate, a total of 3040 bits are transmitted to successfully conclude the ASKG phase. In the ASKG described in [27], the following bit transfers occur: U_k transmits 1152 bits to GW_j, GW_j conveys 1024 bits to ISD_i, and ISD_i transmits 1024 bits back to U_k. In total, 3200 bits are exchanged to complete the ASKG phase. In the context of the ASKG scenario outlined in [20], the data flow unfolds as follows: U_k sends 1152 bits to GW_j, GW_j subsequently transfers 672 bits to ISD_i, and ISD_i forwards 832 bits in

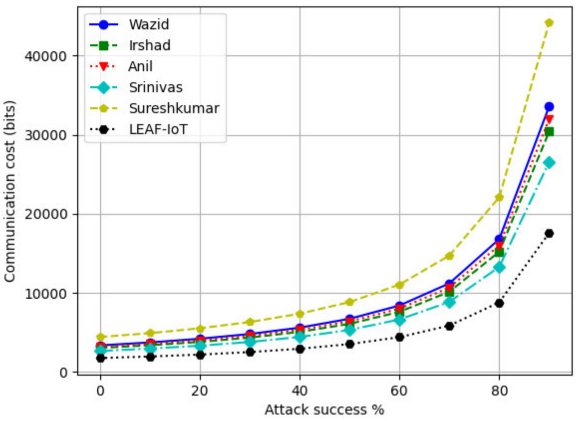

FIGURE 8. Communication cost required in the occurrence of jamming/eavesdropping attack.

return to U_k. The cumulative bit exchange during the ASKG phase amounts to 2656 bits. In the context of the ASKG scenario outlined in [28], the data flow unfolds as follows: U_k sends 1152 bits to GW_j, GW_j subsequently transfers 2304 bits to ISD_i, and ISD_i forwards 960 bits in return to U_k. The cumulative bit exchange during the ASKG phase amounts to 4416 bits. Based on the observations made in Fig. 6 and Fig. 7, it is evident that the LEAF-IIoT requires a lower communication cost compared to the state-of-the-art ASKG frameworks. Specifically, LEAF-IIoT exhibits performance improvements of 47.62%, 42.11%, 45.0%, 33.73%, and 60.14% in comparison to the related ASKG frameworks.

The communication expenses associated with LEAF-IIoT are influenced by the occurrence of jamming or eavesdropping attacks, as these illicit activities impede the normal progression of LEAF-IIoT. Fig. 8 visually depicts the communication costs of the LEAF-IIoT framework in relation to the success probability of these attacks.

VIII. CONCLUSION

IIoT is a new form of communication technology that makes it possible for devices with minimal resources to remotely monitor and manage industrial applications when they are deployed in an IIoT ecosystem. Different kinds of information are transferred between the IIoT device and the administrator during the monitoring and controlling tasks through the open Internet. The public Internet is accessible and subject to a variety of security attacks, which can impair the remote monitoring and control of an industrial control system. We developed an innovative ASKG called LEAF-IIoT to guarantee encrypted communication in the IIoT environment. In order to enable remote user authentication and session key generation, which are necessary for protecting subsequent communications, LEAF-IIoT employed advanced authenticated encryption and PUF technology. We leveraged BAN logic to confirm the veracity of LEAF-IIoT's effectiveness, and we carried out thorough evaluations utilizing the Scyther software tool to test its robustness against a variety of potential threats. The efficiency of LEAF-IIoT in terms of computing, storage, and communication resource requirements has been shown by the performance comparison. To be more accurate, we showed that LEAF-IIoT necessitates 53.58% to 59.41% of low computing resources, and 42.11% to 64.14% of low communication resources. These findings demonstrate that LEAF-IIoT is resource-friendly, making it a feasible approach for adoption in the IIoT context.

ACKNOWLEDGMENT

The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

REFERENCES

[1] A. Irshad, G. A. Mallah, M. Bilal, S. A. Chaudhry, M. Shafiq, and H. Song, "SUSIC: A secure user access control mechanism for SDN-enabled IIoT and cyber physical systems," *IEEE Internet Things J.*, vol. 10, no. 18, pp. 16504–16515, Sep. 2023.

[2] A. Allouch, O. Cheikhrouhou, A. Koubâa, K. Toumi, M. Khalgui, and T. Nguyen Gia, "UTM-chain: Blockchain-based secure unmanned traffic management for Internet of Drones," *Sensors*, vol. 21, no. 9, p. 3049, 2021.

[3] I. Darman, M. K. Mahmood, S. A. Chaudhry, S. A. Khan, and H. Lim, "Designing an enhanced user authenticated key management scheme for 6G-based industrial applications," *IEEE Access*, vol. 10, pp. 92774–92787, 2022.

[4] S. A. Chaudhry, A. Irshad, K. Yahya, N. Kumar, M. Alazab, and Y. B. Zikria, "Rotating behind privacy: An improved lightweight authentication scheme for cloud-based IoT environment," *ACM Trans. Internet Technol.*, vol. 21, no. 3, pp. 1–19, Aug. 2021.

[5] C.-M. Chen, S. A. Chaudhry, K.-H. Yeh, and M. N. Aman, "Security, trust and privacy for cloud, fog and Internet of Things," *Secur. Commun. Netw.*, vol. 2022, pp. 1–2, Jan. 2022.

[6] G. Ali, M. ElAffendi, and N. Ahmad, "BlockAuth: A blockchain-based framework for secure vehicle authentication and authorization," *PLoS ONE*, vol. 18, no. 9, Sep. 2023, Art. no. e0291596.

[7] A. K. Singh, A. Solanki, A. Nayyar, and B. Qureshi, "Elliptic curve signcryption-based mutual authentication protocol for smart cards," *Appl. Sci.*, vol. 10, no. 22, p. 8291, Nov. 2020.

[8] S. Jegadeesan, M. Azees, N. Ramesh Babu, U. Subramaniam, and J. D. Almakhles, "EPAW: Efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs)," *IEEE Access*, vol. 8, pp. 48576–48586, 2020.

[9] H. Alasmary, "RDAF-IIoT: Reliable device-access framework for the industrial Internet of Things," *Mathematics*, vol. 11, no. 12, p. 2710, Jun. 2023.

[10] *Ascon—Pypi*. Accessed: Aug. 14, 2023. [Online]. Available: https://pypi.org/project/ascon/

[11] K. Mahmood, S. Shamshad, M. F. Ayub, Z. Ghaffar, M. K. Khan, and A. K. Das, "Design of provably secure authentication protocol for edge-centric maritime transportation system," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 12, pp. 14536–14545, Dec. 2023.

[12] S. Tu, A. Badshah, H. Alasmary, and M. Waqas, "EAKE-WC: Efficient and anonymous authenticated key exchange scheme for wearable computing," *IEEE Trans. Mobile Comput.*, 2023, doi: 10.1109/TMC.2023.3297854.

[13] M. Tanveer, A. Alkhayyat, A. U. Khan, N. Kumar, and A. G. Alharbi, "REAP-IIoT: Resource-efficient authentication protocol for the industrial Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 23, pp. 24453–24465, Dec. 2022.

[14] Y. Zhang, D. He, P. Vijayakumar, M. Luo, and X. Huang, "SAPFS: An efficient symmetric-key authentication key agreement scheme with perfect forward secrecy for industrial Internet of Things," *IEEE Internet Things J.*, vol. 10, no. 11, pp. 9716–9726, Jun. 2023.

[15] H. Alasmary and M. Tanveer, "ESCI-AKA: Enabling secure communication in an iot-enabled smart home environment using authenticated key agreement framework," *Mathematics*, vol. 11, no. 16, p. 3450, 2023.
[16] M. Tanveer, A. Badshah, A. U. Khan, H. Alasmary, and S. A. Chaudhry, "CMAF-IIoT: Chaotic map-based authentication framework for industrial Internet of Things," *Internet Things*, vol. 23, Oct. 2023, Art. no. 100902.
[17] M. Tanveer, A. U. Khan, N. Kumar, and M. M. Hassan, "RAMP-IoD: A robust authenticated key management protocol for the Internet of Drones," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1339–1353, Jan. 2022.
[18] Z. Ashraf, A. Sohail, and M. Yousaf, "Robust and lightweight symmetric key exchange algorithm for next-generation IoE," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100703.
[19] S. S. Sahoo, S. Mohanty, K. S. Sahoo, M. Daneshmand, and A. H. Gandomi, "A three-factor-based authentication scheme of 5G wireless sensor networks for IoT system," *IEEE Internet Things J.*, vol. 10, no. 17, pp. 15087–15099, Sep. 2023.
[20] J. Srinivas, A. K. Das, M. Wazid, and A. V. Vasilakos, "Designing secure user authentication protocol for big data collection in IoT-based intelligent transportation system," *IEEE Internet Things J.*, vol. 8, no. 9, pp. 7727–7744, May 2021.
[21] F. Li, X. Yu, Y. Cui, S. Yu, Y. Sun, Y. Wang, and H. Zhou, "An anonymous authentication and key agreement protocol in smart living," *Comput. Commun.*, vol. 186, pp. 110–120, Mar. 2022.
[22] D. Kwon, S. Son, J. Lee, and Y. Park, "A secure user authentication protocol in smart living environment," in *Proc. IEEE Asia–Pacific Conf. Comput. Sci. Data Eng. (CSDE)*, Dec. 2022, pp. 1–6.
[23] M. Tanveer, H. Alasmary, N. Kumar, and A. Nayak, "SAAF-IoD: Secure and anonymous authentication framework for the Internet of Drones," *IEEE Trans. Veh. Technol.*, vol. 73, no. 1, pp. 232–244, Jan. 2024.
[24] V. Sureshkumar, R. Amin, M. S. Obaidat, and I. Karthikeyan, "An enhanced mutual authentication and key establishment protocol for TMIS using chaotic map," *J. Inf. Secur. Appl.*, vol. 53, Aug. 2020, Art. no. 102539.
[25] S. Yu, A. K. Das, Y. Park, and P. Lorenz, "SLAP-IoD: Secure and lightweight authentication protocol using physical unclonable functions for Internet of Drones in smart city environments," *IEEE Trans. Veh. Technol.*, vol. 71, no. 10, pp. 10374–10388, Oct. 2022.
[26] M. Wazid, A. K. Das, N. Kumar, and M. Alazab, "Designing authenticated key management scheme in 6G-enabled network in a box deployed for industrial applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 7174–7184, Oct. 2021.
[27] A. K. Sutrala, M. S. Obaidat, S. Saha, A. K. Das, M. Alazab, and Y. Park, "Authenticated key agreement scheme with user anonymity and untraceability for 5G-enabled softwarized industrial cyber-physical systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2316–2330, Mar. 2022.
[28] V. Sureshkumar, R. Amin, V. R. Vijaykumar, and S. R. Sekar, "Robust secure communication protocol for smart healthcare system with FPGA implementation," *Future Gener. Comput. Syst.*, vol. 100, pp. 938–951, Nov. 2019.
[29] G. Tyagi and R. Kumar, "An efficient user authentication and key agreement scheme for wireless sensor networks using physically unclonable function," *Int. J. Inf. Secur.*, 2023. [Online]. Available: https://doi.org/10.1007/s10207-023-00770-3
[30] S. Hussain, K. Mahmood, M. K. Khan, C.-M. Chen, B. A. Alzahrani, and S. A. Chaudhry, "Designing secure and lightweight user access to drone for smart city surveillance," *Comput. Standards Interfaces*, vol. 80, Mar. 2022, Art. no. 103566.
[31] V. Sureshkumar, P. Chinnaraj, P. Saravanan, R. Amin, and J. J. P. C. Rodrigues, "Authenticated key agreement protocol for secure communication establishment in vehicle-to-grid environment with FPGA implementation," *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 3470–3479, Apr. 2022.
[32] T. Alladi, N. Naren, G. Bansal, V. Chamola, and M. Guizani, "SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15068–15077, Dec. 2020.

MUHAMMAD TANVEER received the M.S. degree in computer science from IMS, Lahore, Pakistan, in 2017, and the Ph.D. degree in computer science from the GIK Institute of Engineering Sciences and Technology, Pakistan, in 2022. He is currently acting as an Assistant Professor with the University of Management and Technology, Lahore. His research interests include communication networks and network security.

AHMED A. ABD EL-LATIF (Senior Member, IEEE) received the Ph.D. degree (Hons.) from the Harbin Institute of Technology, China, in 2013. Since 2013 carried out a number of successful research projects and grants in Egypt, Russian Federation, Saudi Arabia, China, Malaysia, and Tunisia. He is a staff member at Menoufia University, Egypt, and at Prince Sultan University, Saudi Arabia. In more than 18 years of his professional experience, he published about 300 papers in journals/conferences including 12 books with over 10000 citations. Since 2022, he is a head of MEGANET 6G lab research in Russian Federation. His research interests include quantum communications and cryptography, cybersecurity, artificial intelligence of things, AI-based image processing, information hiding, and applications of dynamical systems (discrete-time models: chaotic systems and quantum walks) in cybersecurity. He is a Vice Chair of EIAS research lab, founder and deputy director of the centre of excellence in Quantum & Intelligent Computing (Prince Sultan University, Saudi Arabia). He was honored with several awards, including State Encouragement Award in Engineering Sciences 2016, Arab Republic of Egypt; the best Ph.D. student award from Harbin Institute of Technology, China 2013; Young scientific award, Menoufia University, Egypt 2014. He is serving as Chair/Co-Chair of many Scopus/ EI conferences. He is the EIC of International Journal of Information Security and Privacy. Series editor of Quantum Information Processing and Computing, and series editor of Advances in Cybersecurity Management. Also, an academic editor/associate editor for many indexed journals (WoS and Scopus journals' quartile ranking).

ABD ULLAH KHAN (Member, IEEE) received the B.S. degree (Hons.) in telecommunication from UST Bannu, in 2013, the M.S. degree in electrical engineering from COMSATS University Islamabad, in 2016, and the Ph.D. degree in computer science from the Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, Pakistan, in 2021. Part of his Ph.D. degree is from the National University of Sciences and Technology, Islamabad. He is currently working as an Assistant Professor with the National University of Science and Technology, Balochistan Campus, Quetta, Pakistan. His research interests include resource allocation and management in wireless networks, artificial intelligence, and network security. He was a recipient of the prestigious scholarship of the Higher Education Commission of Pakistan. He has received a Gold Medal for his B.S. degree. Besides, he is an Active Reviewer of IEEE Network, IEEE Internet of Things Journal, IEEE Systems Journal, IEEE Access, and Computer Communications (Elsevier).

MUSHEER AHMAD received the B.Tech. and M.Tech. degrees from the Department of Computer Engineering, Aligarh Muslim University, India, in 2004 and 2008, respectively, and the Ph.D. degree in chaos-based cryptography from the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India. From 2007 to 2010, he has worked in the Department of Computer Engineering, Aligarh Muslim University. Since 2011, he has been working as an Assistant Professor in the Department of Computer Engineering, Jamia Millia Islamia. He has published over 100 research papers in internationally reputed refereed journals and conference proceedings of the IEEE/Springer/Elsevier. He has more than 2700 citations of his research works with an H-index of 31, i-10 index of 70, and cumulative impact factor of more than 250. He has been listed among World's Top 2% Scientists in studies conducted by Elsevier BV and Stanford University in 2021 and 2022. His research interests include multimedia security, chaos-based cryptography, cryptanalysis, machine learning for security, image processing, and optimization techniques. He has served as a reviewer and a technical program committee member of many international conferences. He has also served as referee of some renowned journals, such as Information Sciences, Signal Processing, Expert Systems With Applications, Journal of Information Security and Applications, IEEE JSAC, IEEE TCYB, IEEE TPAMI, IEEE TII, IEEE TCSVT, IEEE TCAS, IEEE TNNLS, IEEE Transactions on Systems, Man and Cybernetics: Systems, IEEE TITS, IEEE TR, IEEE TNSE, IEEE Transactions on Nanobioscience, IEEE SYSJ, IEEE Multimedia, IEEE Access, ACM TSON, Wireless Personal Communications, Neural Computing and Applications, *International Journal of Bifurcation and Chaos*, Expert Systems with Applications, Engineering Applications of Artificial Intelligence, Chaos Solitons & Fractals, Physica A, Signal Processing: Image Communication, Neurocomputing, IET Information Security, IET Image Processing, Security and Communication Networks, Optik, Optics and Laser Technology, Complexity, Computers in Biology and Medicine, Computational and Applied Mathematics, and Concurrency and Computation.

ABDELHAMIED A. ATEYA (Senior Member, IEEE) received the B.Sc. and M.Sc. degree in electrical engineering from Zagazig University, Egypt, in 2010 and 2014, respectively, and the Ph.D. degree from the Saint - Petersburg State University of Telecommunications, Russia, in 2019. He is currently an Assistant Professor at the Department of Electronics and Communications Engineering, Faculty of Engineering, Zagazig University. He has coauthored more than 50 publications in high ranked journals. His current research interests include machine learning applications in communication networks, 5G/6G communications, the Internet of things, tactile internet and its standardization, and vehicular communications. He is a member of many scientific communities and ACM Prof. Member. He has been an active member of several international journals and conferences, with a contribution as an author, a reviewer, an editor, or a member of program committees.