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

Digital Object Identifier 10.1109/ACCESS.2020.DOI

Robust and Lightweight Key Exchange (LKE) Protocol for Industry 4.0

GURJOT SINGH GABA[1], (Member, IEEE), GULSHAN KUMAR[2], (Member, IEEE), HIMANSHU MONGA[3], (Member, IEEE), TAI-HOON KIM[4], (Member, IEEE), MADHUSANKA LIYANAGE[5], (Member, IEEE) AND PARDEEP KUMAR[6], (Member, IEEE)

[1]Department of Electronics and Electrical Engineering, Lovely Professional University, Phagwara 144411, India
[2]Department of Computer Science and Engineering, Lovely Professional University, Phagwara 144411, India
[3]Department of Electronics and Communication Engineering, Jawahar Lal Nehru Government Engineering College, Mandi 175018 India
[4]School of Economics and Management, Beijing Jiaotong University, Beijing 100044, China
[5]School of Computer Science, University College Dublin, Ireland and Centre for Wireless Communications, University of Oulu, Finland
[6]Department of Computer Science, Swansea University SA1 8EN, U.K.

Corresponding author: Gulshan Kumar (e-mail: gulshan3971@gmail.com), Tai-Hoon Kim (email: taihoonn@daum.net).

ABSTRACT Industry 4.0 has brought solutions for faster data accessibility, fault identification, performance analysis, and control of machines remotely by managers. Though beneficial but dangerous as the IoT (Internet of Things) nodes communicate over the unsecured wireless medium. The communication over unsecured wireless channel opened enormous ways for the illegitimate nodes to access the information and take control over the industrial machines despite being physically away. These threats can be overpowered with secure sessions; however, the exchange of keys to establish a secure session over a vulnerable channel becomes a challenge. Our approach (LKE) intend to solve this problem. LKE provides a lightweight key exchange platform to the legitimate IoT nodes and prohibit the unauthorized abuses. LKE uses lightweight Elliptic Curve Qu-Vanstone (ECQV) based implicit certificates for trust-building and generating keys among entities. All the messages exchanged are secured to prevent unauthorized access to information and preventing against forgery, replay, modification, impersonation and man-in-the-middle attacks, etc. The proposed scheme is tested on the *AVISPA* tool and results indicate its trustworthiness and strong resistivity against potential attacks. LKE has less computation and communication complexities due to the utilization of limited cryptographic operations which make it superior in comparison to other state-of-the-work.

INDEX TERMS Cyber-physical system, Industry 4.0, Industrial Internet of Things (IIoT), Implicit certificates, Key exchange, Security.

I. INTRODUCTION

INDUSTRY 4.0 has enabled the connectivity of physical devices such as robots to the internet. This revolution has brought extensive solutions to control the machines remotely along with retrieving of useful data from the remote locations [1]. The industrial revolution has been presented in Fig. 1. The transformation of industrial processes took ages to reach an autonomous state. It began in the decade of 1780 when machines were first used for performing industrial tasks. The next progress almost took a century which advanced the manufacturing process with the involvement of *massive manpower* and *assembly lines* (driven by electricity) for enhanced production. The year of 1968 brought another milestone in the history of industrial transformation. This generation of Industry experienced automation in production processes through the *integration* of *electronics* and *computers* into the machines. The present generation of Industry (I4.0) is even more powerful than all the predecessors. The machines of this generation are too smart; they can *sense*, *monitor*, and *measure* the physical quantities and seamlessly report to the connected devices. Industrial IoT enabled the administrators to monitor the processes in real time thus helping them to make instant decisions and analysis [2].

IIoT evolution has not only transformed the manufacturing processes of industry rather has helped the logistics department to locate the movement of goods carriers, predict the arrival timings and help the carriers in finding the path with less traffic and better road conditions [3], [4]. The amalgam of physical and cyber technology in industries are leaving footprints of success [5]. *Bosch Inc.* is using IIoT for monitoring the lubricating valves and filters to reduce manual testing and maintenance costs [6]. *Volkswagen Group*

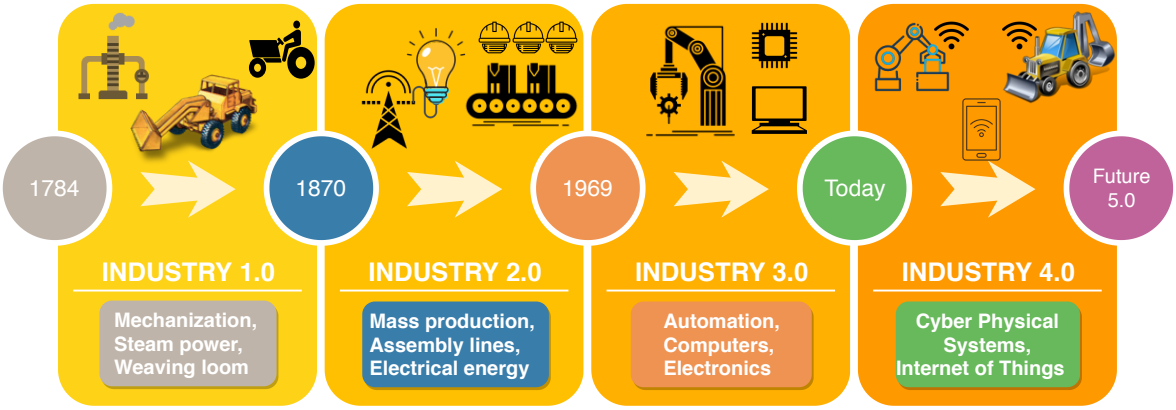

FIGURE 1. Industrial revolution.

manufactures the *lamborghini* in a smart factory where automatic guided vehicles carry the car components from one workstation to another. Apart from the movement, workers of the industry are able to see the progress, control and monitor the workstations processes remotely, thereby eliminating the need of physical presence of workers and managers in the industry [7]. Likewise, enormous features of IIoT has led the pharmacy and agriculture industry to incorporate I4.0 processes for medicine testing [8] and prediction of disease in crops, respectively [9].

Indeed few industries are able to transform but still lot many are struggling. The biggest challenge in realization of Industry 4.0 is *interoperability*, *compatibility*, and *reliability*; Interoperability amongst plethora of machines from various manufacturers, compatibility of machines with existing infrastructure and their operational reliability is still a major concern. The data security is yet another, but extremely critical parameter in the accomplishment of IIoT [10]. The authors in [11] stressed on the uncontrollable nature of the Machine to Machine (M2M) communications and highlighted the threats to large volume of critical data in absence of robust security measures. Absentia of security measures in IIoT may pave the way towards cyberattacks. Cyberattacks can cause physical damage to infrastructure of industry and may endanger workers lives [12].

Modern ambush on cyber physical networks upraise a solid security anxiety as such attacks can cause loss to customers, service providers, and manufacturers [13], [14]. The setback of the industry operators happened due to recent attacks on industrial networks: a network was created for controlling lights, fan, fire detection, and HVAC at Sochi arena for Olympics. But during inspection in 2018, it is found that 17,823 building automation control network (BACnet) devices and 78,000 SCADA devices were exposed to internet without security protections. The incompetence of key exchange and mutual authentication protocol enabled the attackers to get illegal access of the complete BACnet [15].

Another incidence was brought into limelight by forbes, where attackers used malicious codes and radio hardware to exploit the industrial network. Attackers got successful when they took over the control of construction cranes, excavators, scrapers and other large machinery from legitimate engineers of the industry. Another instance Zimperium Inc. reported recently about the electric scooter manufactured by Chinese company Xiaomi Inc. The electric scooter was accepting commands like acceleration, braking, locking and unlocking from even illegitimate users and devices [16]. In addition, a survey paper concludes that IIoT networks may suffer from masquerade and disclosure attacks if the network is not enabled with proper authentication mechanisms [17].

Many potential attacks are conducted in the recent past, e.g., *Mirai* and *IoTroop* botnet where attackers exploited the vulnerabilities of the system i.e., *access control* procedures, *incompatibility* of security protocols due to *heterogeneous* nature of devices etc. [18]. These attacks in *Cyber-physical systems* (CPS) are majorly caused due to use of unsecured medium for signalling actuators [19]. The vulnerability in the IIoT can be more dangerous due to sensitive nature of data, for instance, a little loss of precision in chemical formation could produce a complete different medicine, thus posing disastrous health effects. The key vulnerabilities found behind the aforementioned incidents are inadequate and improper mutual authentication and key exchange procedures. Therefore, security analysts have advised to implement secure key exchange and strong mutual authentication procedures for ensuring security and privacy of the data [20], [21].

The entities involved in the key exchange and mutual authentication are usually heterogeneous and have different resource availability like gateways are resource-rich devices whereas smart IoT nodes are resource-deprived. Therefore, security protocols must be computation and communication inexpensive [22], [23]. Traditional models of authentication are too clumsy (computation and communication overhead) and cannot be applied directly to IIoT environment [24], [25]–[27]. Therefore, new security and privacy paradigms must be developed to cater the need of IIoT networks.

A. LITERATURE REVIEW

Das et al. in [24] raised a concern on security and privacy of Industrial IoT networks due to use of open channel for communication. The authors believed that existing schemes may not be suitable in IIoT specific environment due to excessive overheads. The authors formulated a Biometric-based privacy preserving authentication scheme to combat against unauthorized intrusions with limited overheads. The scheme makes use of biometric and smart card as a 2 factor authentication process. The protocol has been simulated on NS2 to verify its behaviour. The authors performed formal and informal security analysis and declared their scheme as robust against various attacks. In spite of 2 factor authentication, the scheme fails to ensure privacy and protection against known key attacks.

Li et al. in [28] discussed the challenges in implementing security protocols i.e., open nature of wireless medium and resource constrained nodes. The authors proposed a 3 factor user authentication protocol for WSN-IIoT environment while keeping these challenges into consideration. The three factors used to authenticate are *user's identity*, *password* and *biometric*. The user is only able to access the sensor's data if all the factors generate positive results. The authors declare that their scheme is resistant to impersonation, replay attack, etc. however validation using formal analysis is found missing. The scheme is communication inefficient as the resource constrained node *transmits* and *receives* a total of 2688 bits for the key exchange process. Consequently, the scheme is unfit for resource constrained applications of IIoT.

Esfahani et al. in [29] presented an authentication model for M2M communications in IIoT environment. The authors stated that traditional schemes cannot be used in IIoT due to excessive overheads which may drain the node resources. Therefore, authors have devised a new security model which computes only *hash* and *ex-or* operations during authentication. Due to use of few cryptography operations, the authors declared their scheme as computation efficient. The authors further claimed that their scheme exhibits the security properties such as session key agreement, anonymity, etc. and is also resistant against replay, man-in-the-middle (MITM) attacks, etc. Indeed the scheme is providing many security benefits, the authors have not performed vulnerability assessment and formal analysis, thus behaviour of the scheme is unpredictable under compromised conditions. In addition, the scheme spends a lot of energy in communicating large sized mutual authentication and key exchange messages, which makes the scheme energy inefficient. Therefore, the proposed scheme is not suitable for IIoT networks due to its unpredictable behaviour and high energy consumption.

ECC based authentication protocol for IIoT has been presented by Li et al. in [30]. The authors emphasized on the need of authentication mechanism to prevent from unauthorised access due to unsecured nature of medium in wireless sensor networks. Their scheme makes use of biometrics to identify the legitimacy of the entity. The authors simulated their scheme on NS3 to determine the performance. Regardless of the claimed advantages, it is found that authors have not considered Denial of Service (DoS) and MITM attacks during security analysis which may pose threats to network existence. It is evident that scheme fails to provision privacy and message freshness for all exchanged messages due to absence of ciphering and nonce, respectively.

Paliwal in [31] has expressed his concern over integrity and confidentiality of data in IIoT networks. The author emphasized that sensitive information collected by the sensor nodes in Wireless Sensor Networks (WSN) should be accessible to intended recipients only. The article briefs the various existing authentication schemes along with their vulnerabilities. The scheme makes use of hash to achieve mutual authentication and key establishment whilst ensuring anonymity of identities. The scheme is claimed as lightweight and efficacious due to limited computations and resistance against many significant attacks. The author has affirmed that the scheme has undergone formal and informal analysis and is declared secured to be used in IIoT environment. Despite the fact the scheme is asserted robust, the scheme does not ensure privacy. Though scheme does not make use of any ciphering model but extensive use of hash and large size of exchanged messages over burdens the overall scheme.

Chang et al. in [32] introduced an authentication scheme for WSN to prevent unauthorised penetrations. Though claimed as efficient and secured but complex as it operates in twin modes. The authors have tried to overcome the deficiencies of existing authentication protocols by introducing a smart card based authentication scheme for WSN. Their proposed protocol works on two different algorithms and attains two different set of security properties accordingly. The authors have performed formal security analysis using Real-Or-Random (RoR) model to prove the robustness of their protocol. It is observed that their first protocol (P_1) does not offer complete security solutions whereas the second one (P_2) is resource expensive. IoT devices are usually resource constrained, therefore deploying this protocol can reduce the active lifetime of the devices and networks.

Gope et al. in [33] focused on the realization challenges of Industrial WSN (IWSN). Considering the security as the most significant challenge, the authors devised a new mutual authentication protocol for the real time data access applications of IWSN. The authors applied exclusive-or, one way hash, and physically unclonable functions (PUF), to name a few, in their algorithm. The main strength highlighted in the paper is the security of the credentials even if the sensor nodes are physically captured by the adversary. The scheme provides key security features such as mutual authentication, and integrity, etc. Despite the benefits, the scheme exchanges 6 messages to accomplish session key which is itself a challenge for resource constrained devices. The number of bits exchanged in those messages is quite much in quantity which further escalates the energy consumption bar. This immense energy consumption can deplete the energy reserves of IIoT nodes quickly. Moreover, the behavior of the schemes [32], [33] under the influence of the DoS attack is not observed,

therefore adversaries can exploit the hidden vulnerabilities to attack the IIoT networks.

In summary, the present techniques are found vulnerable to the prominent attacks (MITM, Known Key, and DoS etc.) and also incurs high communication and computation complexities, which makes the existing techniques unfit for Industrial IoT networks. The Industrial IoT is a sensitive application where a minor intrusion by illegitimate node can cause extensive irreparable losses. Therefore, the access to the IIoT network must be protected with a robust and efficient key exchange and mutual authentication model.

B. OUR CONTRIBUTION

- We propose a Robust and Lightweight Key Exchange (LKE) protocol for Industrial IoT networks.
- To achieve the robustness and efficiency, ECQV implicit certificates, asymmetric and symmetric key cryptography, keyed-hash, and nonces are used.
- The proposed scheme assures mutual authentication between industrial node and gateway before secret key generation.
- The proposed protocol provisions the renewal of expired certificates to support long term connectivity between entities and strengthening security measures (e.g., prevention from impersonation and replay attacks etc.).
- The strength of LKE is tested using formal and informal security analysis where it is found that LKE exhibits essential security properties, like authentication, confidentiality etc., and is also resistant against impersonation, replay, and MITM attacks etc.
- The performance of the proposed scheme is compared with the state-of-the-art to show its superiority over them in terms of computational and communicational efficiency.

The rest of the paper is organized as follows: section II presents system and adversary model together with security and other goals. Section III demonstrates the working of the proposed scheme. Section IV provides the formal and informal security analysis whereas section V highlights the performance and comparative analysis. Section VI draws the conclusions.

II. SYSTEM MODEL, ADVERSARY MODEL, AND SECURITY AND OTHER GOALS

A. SYSTEM MODEL

Fig. 2 depicts an IIoT network controlled and monitored over the internet. The architecture of the IIoT constitutes of IoT sensor nodes deployed at machines which communicates to Certification Authority (CA) and cloud via gateway using wireless bi-directional link. The user gets access to information through cloud.

1) WSN-IIoT network

The machines in the industry are equipped with the sensor nodes. The sensor nodes receive control signals (e.g., turn on/off the machine etc.) from operator, collect data from machines (e.g., production count, temperature of machine, pressure, etc.) and relay it wirelessly to the gateway using low powered modules e.g., Zigbee (IEEE 802.15.4) and Z-Wave (e.g., $ZW0500$).

2) Gateway

Gateway is usually stationery and powered with mains. Gateway acts as an intermediary to support the communication between smart IoT sensor node, cloud (e.g., Kinsta and Microsoft Azure) and CA. It supports IEEE 802.3 and IEEE 802.11 standard for transporting the data over the internet.The gateway is responsible for authenticating the nodes deployed in the IIoT network before relaying their information to cloud and vice versa.

3) Certification Authority

The certification authority (e.g., *Symantec*, *GeoTrust*, etc.) creates a database of the nodes deployed in the network and utilizes it later to conduct mutual authentication before issuing certificates to nodes. CA issues unique implicit certificates to each sensor node which is required by them to construct their public and private keys.

B. ADVERSARY MODEL

The proposed scheme has adopted the Dolev-Yao adversary model advised in [33]–[35]. As per the threat model, adversary has the capabilities to discover the vulnerabilities of the industrial network; these vulnerabilities can be used to exploit the potential resources of the industries. Consider an IIoT enabled smart car manufacturing industry [36] where sensor nodes are deployed to monitor and control the activities of robotic arms, manage the logistics, and identify the raw material requirements at warehouse, etc. Following the Dolev-Yao adversary model, the robotic industrial machines (nodes), logistics and warehouse network devices (gateway), etc. are under threat in IIoT. An adversary in IIoT can eavesdrop all the communications that occurs between industrial nodes, gateway and CA. More specifically, an adversary can capture, modify and replay the messages exchanged between network entities to get privileged access of industrial robotic arms (e.g., welding, painting, transportation, and assembling), etc. Additionally, adversary can impersonate as legitimate industrial node to steal precious RFID tag information. Physical capturing of the devices (nodes and gateway) inside the smart industries is not possible as they are secured using physical locks along with monitoring through surveillance cameras. The adversary can try to modify the lifetime of the expired authenticator to intrude illegally into the industrial network for introducing malware in the computerised production units of industry. Moreover, the adversary can intercept the messages exchanged between the network entities to retrieve security parameters to generate future secret keys, actuate driverless cars, etc. The adversary can construct and inject new messages into the network to launch DoS attack to cause obstruction in sending control commands to

the industrial machines (e.g., warehouse storage sequencing error). Conclusively, the adversary has adequate capabilities to hinder the smooth and secure functioning of the manufacturing units, warehouses, and logistics etc. The adversarial attacks can result in financial and reputation loss, business disruption, and decreased efficiency etc.

C. SECURITY AND OTHER GOALS

Security goals subsection discusses the desirable security properties that a security protocol must exhibit to be declared as *robust*, whereas, *other goals* subsection discusses those preferable properties that prove the protocol as *efficient*.

1) Security Goals

LKE complies with the significant security properties. Note that the security properties are adopted from [37], [38].

1) **Mutual authentication and secret key establishment**: Industrial IoT networks are sensitive as industrial machines are involved. The nodes must perform mutual authentication followed by the secret key exchange to protect their communications from illegitimate nodes.
2) **Message integrity and freshness**: Alterations devastate the real content of the message and stale messages may trigger non-permissible actions. Therefore, security protocols must incorporate certain procedures to let the entities verify the message integrity and freshness.
3) **Defense against prominent attacks**: Impact of attacks can be mild or severe and may lead to temporary or permanent suspension of the industry operations. Therefore, security protocols must be resistant to prominent attacks like impersonation, replay, alteration of information, DoS, MITM, and known key.
4) **Data Privacy**: Industrial IoT network carries very sensitive information (e.g., control commands, confidential manufacturing process, secret keys or credentials, and authentication passcode, etc.). Any disclosure of such information may disrupt the business operations as well as can tarnish the reputation of the industry. The consequences of the disclosure of information to unauthorized entities may vary from benign to severe. Therefore, security protocols must ensure that information exchanged must remain confidential even if the adversary captures the messages.
5) **Identity Anonymity**: Adversaries are always seeking crucial details like identities of the industrial nodes and other network devices. These identities can be used by the adversaries as a useful element to conduct a MITM attack, etc. Therefore, it is desirable that the identity of the nodes and other network devices (e.g., gateway) should remain anonymous. Identity anonymity not only prevents attacks (e.g., MITM and impersonation attacks, etc). rather keeps the overall communication anonymous.

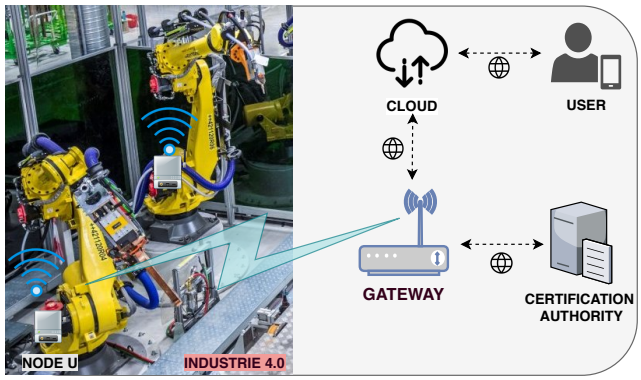

FIGURE 2. System Model for mutual authentication and key exchange between IoT devices in Industry 4.0.

2) Other Goals

LKE exhibits the prominent properties like *lightweightness* and *certificate renewal* to ensure *efficiency* and *long term connectivity*, respectively.

1) **Lightweightness**: As the IoT nodes are usually resource-deprived; therefore the nodes must perform limited computations and communications while still achieving the highest possible degree of security.
2) **Certificate Renewal**: The implicit certificates generated by CA for industrial nodes have time-bound validity. The expiration of the certificates terminates the communication session between industrial nodes and gateway. It is highly desirable to provide a certificate renewal process to allow the interested industrial nodes to re-establish a new secure session with the gateway. The certificates of the legitimate industrial nodes should be renewed with bare minimum computation and communication complexities.

III. PROPOSED SCHEME

This section describes the working of robust and lightweight key exchange protocol for distributed IIoT applications. Fig. 2 portrays a smart car manufacturing industry in German [36] where FANUC 2000 IC robots are being used. A system model considering this scenario is presented in Fig. 2. The FANUC 2000 IC robots are equipped with the IoT sensor nodes. The sensor nodes collect the data and forward it to the cloud via gateway. In order to ensure the security of this communication, a mutual authentication and key exchange protocol is presented in this section. The notations with their description, sizes and methodologies are provided in Table 1. The proposed scheme consists of 3 phases: (A) *System set-up* and *registration phase*, (B) *Certificate* and *Node Key generation phase*, and (C) *Light-weight Key establishment phase*. Furthermore, this section also demonstrates the renewal process of revoked certificates (D).

To demonstrate the working of protocol, some assumptions are considered; (a) CA is a trusted and tamper-proof entity and has no restrictions with respect to computational power and memory, (b) The CA, gateway and IIoT sensor

TABLE 1. Symbols, Abbreviations and Operators description

Notations	Descriptions	Size (bytes)	Method
r_U, r_{CA}	A random integer generated by node U and Certification Authority (CA)	2, 2	LCG
$G_{(x,y)}$, n	Base point generator and its order	16, 2	ECC
R_U	Elliptic curve point for certificate request sent by node U	16	ECC
$Cert_N$ & e	Implicit certificate of N^{th} node and its Hash value	16, 16	Implicit, MD5
d_{CA}, Q_{CA}	Private and public key of CA	32, 32	ECC-256
d_U, Q_U	Private and public key of node U	32, 32	ECC-256
d_G, Q_G	Private and public key of Gateway (G_w)	32, 32	ECC-256
$s_{(U/G)}, CR_{Req}$	Implicit signature, Certificate renewal request	32, 1	-
TS and LT	Time Stamp and Lifetime	8, 8	Date, time & time zone
id_U, id_G, id_{CA}	Identity of node U, Gateway and CA	1, 1, 1	-
K_{UG}	Shared Secret key between node U and Gateway	32	AES-256
N_X	It is a random positive integer called as nonce. X indicates the order of nonce.	8	LCG
E and D	Encryption and Decryption	-	AES-128
$\|, \oplus, +, mod$	Concatenation, XOR, Addition, modulus	-	-
K_T	Temporary key	16	AES-128
HMAC, Hash	Hash-based message authentication code, Hash (message digest)	16, 16	HMAC-MD5, MD5
A_N	Authenticator generated by CA for N^{th} node	65	ECC-256

Acronyms: **LCG**: Linear Congruential Generator, **ECC**: Elliptic Curve Cryptography, **MD5**: Message Digest, **AES**: Advanced Encryption Standard

nodes are assumed to have identical cryptographic systems (e.g., ciphering, hashing functions, etc.), (c) Gateway has no restrictions with respect to computational power, memory (tamper-proof), and broadcasts its ID (id_G) at regular intervals, (d) Gateway has finished the registration at CA and formed the pair of keys (public, Q_G and private key, d_G) through Authenticator A_G.

A. SYSTEM SET-UP AND REGISTRATION PHASE

Prior to the network deployment, all the IoT sensor nodes get registered offline to the CA and obtain security credentials such as *Generator point* and order of Elliptic Curve Cryptography (ECC). Note that we intentionally omitted the ECQV background, interested readers may refer to [39]. During registration, CA assigns unique identity (e.g., id_U) to each node and stores it in the node memory. In addition, CA provides its public key, $Q_{CA}(= d_{CA}G)$ to registered nodes. Finally, CA prepares a database of all registered nodes ($id_U, id_G ...$) and stores them in memory.

B. CERTIFICATE AND NODE KEY GENERATION PHASE

It is an initial phase where the deployed nodes configure themselves automatically. Let us consider a node U (id_U) as one of nodes deployed in the network. The node U requests CA for generating and provisioning its implicit certificate. This certificate is required by the node U to prove its legitimacy among other entities and also to generate its public (Q_U) and private key (d_U). This phase is invoked only during *first time network setup*. The complete process of certificate and node key generation is illustrated in Fig. 3 along with demonstration in this section.

Dialogue Exchange between Node U, Gateway & CA

{Note: O_N and M_N represents Operation and Message number, respectively (Here N comprises of positive integer values e.g., 1, 2, 3 etc.)}

At first, the Node U (N_U) generates a random integer, r_U (O_1) and elliptic curve (EC) point, R_U (O_2). Upon generation, N_U prepares a message comprising of its identity (id_U), gateway identity (id_G), EC point (R_U), and nonce (N_1). The message is hashed (O_3) and encrypted with Q_{CA} to ensure integrity and confidentiality, respectively. N_U sends the message M_1 to Gateway (G_w).

O_1: $r_U \; \varepsilon_R \; [1, ..., n-1]$

O_2: $R_U = r_U G$

O_3: $H_1 = Hash(id_U \| R_U \| id_G \| N_1)$

$\boxed{\mathbb{M}_1\text{: } E_{Q_{CA}}[id_U \| R_U \| id_G \| N_1 \| H_1]} \; \{Node\ U \rightarrow G_w\}$

G_w appends the credentials of CA (id_{CA}) and itself (id_G) together with the fresh nonce (N_2) to the received message M_1, encrypts it with Q_{CA} and sends it (M_2) to CA.

$\boxed{\mathbb{M}_2\text{: } E_{Q_{CA}}[id_G \| id_{CA} \| N_2 \| M_1]} \; \{G_w \rightarrow CA\}$

CA receives M_2 and decrypts it using d_{CA} (O_4) to extract M_1. Furthermore, CA decrypts M_1 using its private key, d_{CA} to fetch credentials of N_U (O_5). Post decryption, CA examine the nonces N_2 and N_1 for verifying the freshness of the received message. CA retrieves the identity of the gateway (id_G), and the identity of node U (id_U) from the messages M_2 and M_1, respectively to compare $\{(M_2)id_G == id_G(M_1)$ and $(M_1)id_U == id_U(CA_{Database})\}$, and prove that messages have arrived from trustworthy nodes only. After validating the freshness and faithfulness of the messages, CA computes and verifies the hash, $H_1' == H_1$ in O_6 to inspect the integrity of node credentials and request.

Afterwards, CA generates random integer, r_{CA} (O_7), implicit certificate, $Cert_U$ (O_8, O_9), signatures, s_U (O_{10}) followed by Authenticator (A_U) in O_{11}. As aforementioned A_G is stored in CA database because the gateway has finished the registration with CA prior to nodes. A_U is encrypted by d_{CA} and constitutes of node identity (id_U), certificate ($Cert_U$),

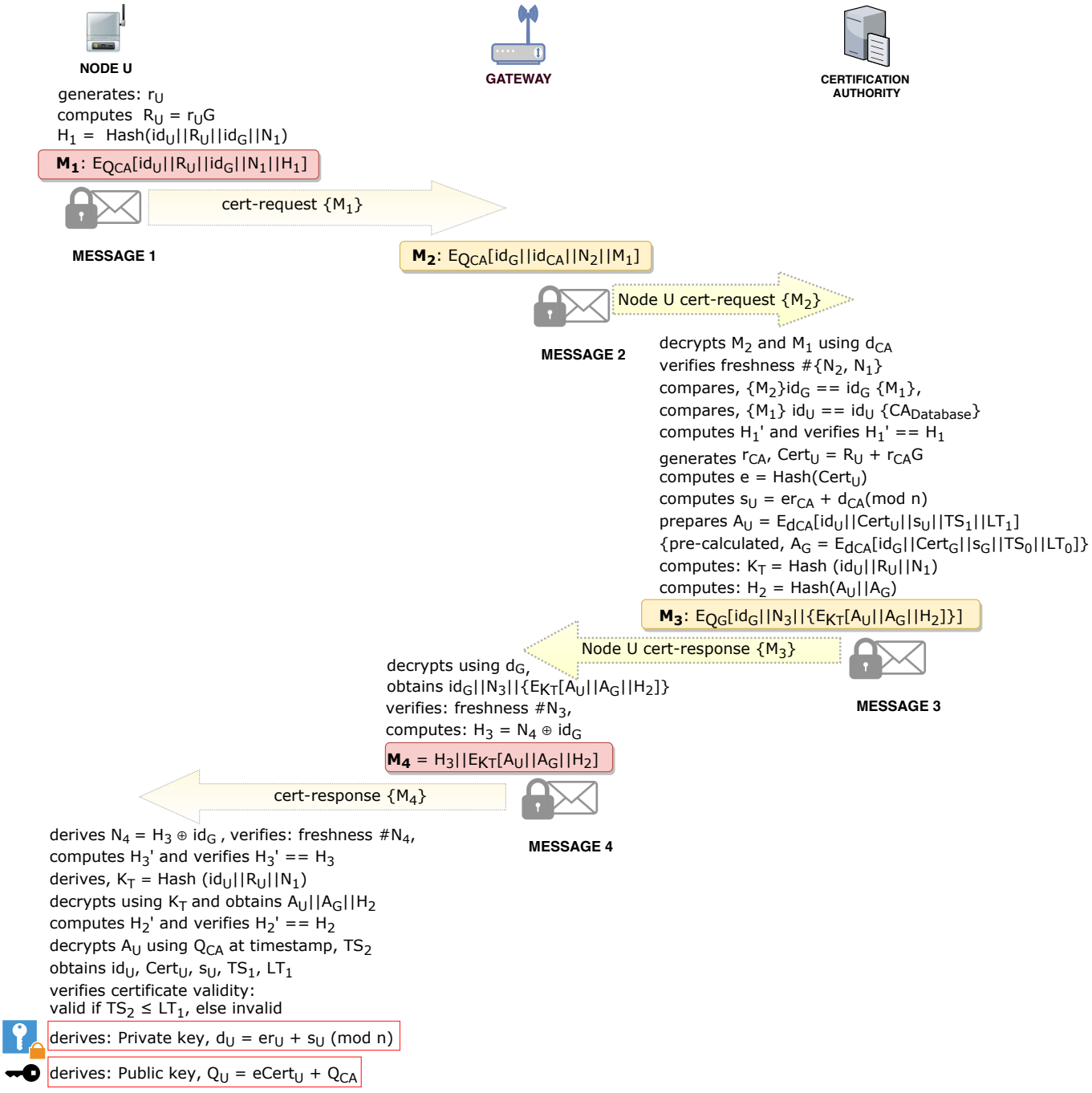

FIGURE 3. Certificate and Node Key Generation Phase.

signature (s_U), timestamp (TS_1) and lifetime (LT_1). TS_1 is the current timestamp of CA whereas TS_0 represents the timestamp of CA used during preparation of G_w authenticator (A_G). LT_0 and LT_1 defines the validity (lifetime) of the G_w and N_U certificate, respectively and their validity depends upon sensitivity of the application (may range from $3 \sim 12$ months). Timestamp and Lifetime parameters allows the message recipients to verify the legitimacy of the request which in turn prevents the network from replay and other similar attacks. A_U is resistant against modifications because the attacker does not have the secret key of CA (d_{CA}) required to perform the alterations.

O_4: $D_{d_{CA}}[id_G \| id_{CA} \| N_2 \| M_1]$
O_5: $D_{d_{CA}}[id_U \| R_U \| id_G \| N_1 \| H_1]$
O_6: $H_1' = Hash(id_U \| R_U \| id_G \| N_1)$ $\{H_1' == H_1\}$
O_7: $r_{CA}\ \varepsilon_R\ [1, ..., n-1]$
O_8: $Cert_U = R_U + r_{CA}G$
O_9: $e = Hash(Cert_U)$

O_{10}: $s_U = er_{CA} + d_{CA} (\text{mod } n)$
O_{11}: $A_U = E_{d_{CA}}[id_U \| Cert_U \| s_U \| TS_1 \| LT_1]$
{pre-calculated $A_G = E_{d_{CA}}[id_G \| Cert_G \| s_G \| TS_0 \| LT_0]$}
CA computes K_T in O_{12} using identity of N_U (id_U), EC point of N_U (R_U) and nonce (N_1). CA concatenates gateway identity (id_G), fresh nonce (N_3) along with K_T encrypted message (A_U, A_G, H_2) and encrypts it with Q_G (O_{13}, M_3). The A_U, A_G cannot be decrypted and forged by any unauthorized entity as EC point knowledge is only available with N_U. *Nonce* is also used to prevent from replay attacks. The prepared message M_3 is sent to the gateway.
O_{12}: $K_T = Hash(id_U \| R_U \| N_1)$
O_{13}: $H_2 = Hash(A_U \| A_G)$
$\boxed{\mathbb{M}_3: E_{Q_G}\{id_G \| N_3 \| E_{K_T}[A_U \| A_G \| H_2]\}}$ $\{CA \rightarrow G_w\}$
Gateway decrypts the received message, M_3 using his private key, d_G and verifies the nonce, N_3 (O_{14}). Post successful verification, gateway forwards the message M_4 to N_U. Message M_4 comprises of H_3 $(N_4 \oplus id_G; O_{15})$, K_T encrypted authenticators (A_U, A_G) and hash (H_2).
O_{14}: $D_{d_G}\{id_G \| N_3 \| [E_{K_T}[A_U \| A_G \| H_2]\}$
O_{15}: $H_3 = N_4 \oplus id_G$
$\boxed{\mathbb{M}_4: H_3 \| E_{K_T}[A_U \| A_G \| H_2]}$ $\{G_w \rightarrow \text{Node } U\}$
Node U derives N_4 and verifies its freshness. In addition, Node U computes H_3' and check for integrity O_{16}. Node U accepts the message if the nonce is fresh $(\#N_4)$ and integrity is preserved $(H_3' == H_3)$. Node U computes K_T and recovers A_U and A_G in O_{17} and O_{18}, respectively. Further N_U computes H_2' for verifying message integrity (O_{19}) followed by decryption of A_U using Q_{CA} in O_{20}. N_U verifies the validity of the $Cert_U$ before processing further. N_U computes private key, d_U and public key, Q_U using $Cert_U$, s_U, r_U and Q_{CA} $(O_{21} - O_{22})$.
O_{16}: $H_3' = N_4 \oplus id_G$ $\{H_3' == H_3\}$
O_{17}: $K_T = Hash(id_U \| R_U \| N_1)$
O_{18}: $D_{K_T}[A_U \| A_G \| H_2]$
O_{19}: $H_2' = Hash(A_U \| A_G)$ $\{H_2' == H_2\}$
O_{20}: $D_{Q_{CA}}[id_U \| Cert_U \| s_U \| TS_1 \| LT_1]$ (Decrypted at TS_2)
Note: $Cert_U$ is valid if this condition is true: $TS_2 \leq LT_1$, else invalid.
O_{21}: $d_U = er_U + s_U (\text{mod } n)$ {private key}
O_{22}: $Q_U = d_U G$
$= (er_U + s_U (\text{mod } n))G$
$= (er_U + er_{CA} (\text{mod } n) + d_{CA} (\text{mod } n) (\text{mod } n))G$
$= (er_U + er_{CA} (\text{mod } n) + d_{CA} (\text{mod } n))G$
$= e(r_U + r_{CA})G + d_{CA}G$
$= e(r_U G + r_{CA} G) + Q_{CA}$
$= e(R_U + r_{CA} G) + Q_{CA}$
$Q_U = eCert_U + Q_{CA}$ {public key}
Node U has successfully constructed Q_U and d_U.

C. LIGHT-WEIGHT KEY ESTABLISHMENT PHASE

Key establishment process is initiated by N_U. Fig. 4 illustrates the whole process. Note that S_N and I_N represents Operation and Message number, respectively (Here N comprises of positive integer values e.g., 1, 2, 3 etc.). N_U derives the credentials of G_w by decrypting the A_G with Q_{CA} (S_1). Subsequently, N_U verifies the lifetime of the $Cert_G$ and if found unexpired then it retrieves Q_G (S_2, S_3). Finally shared secret key is produced i.e., $K_{UG} = d_U Q_G$ (S_4). Post generation of K_{UG}, N_U computes HMAC of id_G, N_5, A_U with secret key, K_{UG} (S_5). Following that N_U prepares I_1 and sends it to G_w.
S_1: $D_{Q_{CA}}[id_G \| Cert_G \| s_G \| TS_0 \| LT_0]$ (Decrypted at TS_3)
Note: $Cert_G$ is valid if this condition is true: $TS_3 \leq LT_0$, else invalid.
S_2: $e = Hash(Cert_G)$
S_3: $Q_G = eCert_G + Q_{CA}$
S_4: $\mathbb{K}_{\mathbb{UG}} = d_U Q_G$ {shared secret key}
S_5: $H_4 = HMAC[K_{UG}, id_G \| N_5 \| A_U]$
$\boxed{\mathbb{I}_1: E_{Q_G}[id_G \| N_5 \| A_U \| H_4]}$ $\{Node\ U \rightarrow G_w\}$
S_6: $D_{d_G}[id_G \| N_5 \| A_U \| H_4]$
S_7: $D_{Q_{CA}}[id_U \| Cert_U \| s_U \| TS_1 \| LT_1]$ (Decrypted at TS_4)
Note: $Cert_U$ is valid if this condition is true: $TS_4 \leq LT_1$, else invalid.
S_8: $Q_U = eCert_U + Q_{CA}$
S_9: $\mathbb{K}_{\mathbb{UG}} = d_G Q_U$ {shared secret key}
S_{10}: $H_4' = HMAC[K_{UG}, id_G \| N_5 \| A_U]$ $\{H_4' == H_4\}$

G_w decrypts the received message, I_1 using d_G and Q_{CA} (S_6, S_7) and produces Q_U (S_8). Note that gateway evaluates the validity of the certificate before producing Q_U. Later, Gateway utilizes Q_U to produce shared secret key i.e., $K_{UG} = d_G Q_U$. As a result, both the entities generate the same secret keys securely (S_{10}). Note that lifetime of the keys {public (Q_{CA}, Q_G, Q_U), private (d_{CA}, d_G, d_U), secret key (K_{UG})} depend upon sensitivity of data and is application dependent.

D. CERTIFICATE RENEWAL PHASE

In real time scenarios, each certificate is integrated with validity. After the lapse of certificate validity, the secret key (e.g., $\mathbb{K}_{\mathbb{UG}}$) becomes invalid and results in termination of communication session between an industrial node (e.g., N_U) and gateway (e.g., G_w). Consequently, the industrial nodes that seek to continue the communication with the gateway initiates a certificate renewal process with the CA. Upon the accomplishment of certificate renewal, the new secret key is negotiated between the industrial node and gateway. The process of renewal is depicted in Fig. 5 as well as justified through dialogue exchange in this section.
{Note: C_N and D_N represents operation and message number, respectively (Here N comprises of positive integer values e.g., 1, 2, 3 etc.)}
C_1: $r_{2U}\ \varepsilon_R\ [1, ..., n-1]$
C_2: $R_{2U} = r_{2U} G$
C_3: $H_5 = Hash(CR_{Req} \| A_U \| R_{2U} \| N_6)$
$\boxed{\mathbb{D}_1: E_{K_T}[CR_{Req} \| A_U \| R_{2U} \| N_6 \| H_5]}$ {Node $U \rightarrow G_w$}
$\boxed{\mathbb{D}_2: E_{Q_{CA}}[id_G \| id_{CA} \| N_7 \| D_1]}$ $\{G_w \rightarrow CA\}$
C_4: $D_{d_{CA}}[id_G \| id_{CA} \| N_7 \| D_1]$
C_5: $D_{K_T}[CR_{Req} \| A_U \| R_{2U} \| N_6 \| H_5]$
C_6: $A_{2U} = E_{d_{CA}}[id_U \| Cert_{2U} \| s_{2U} \| TS_5 \| LT_2]$

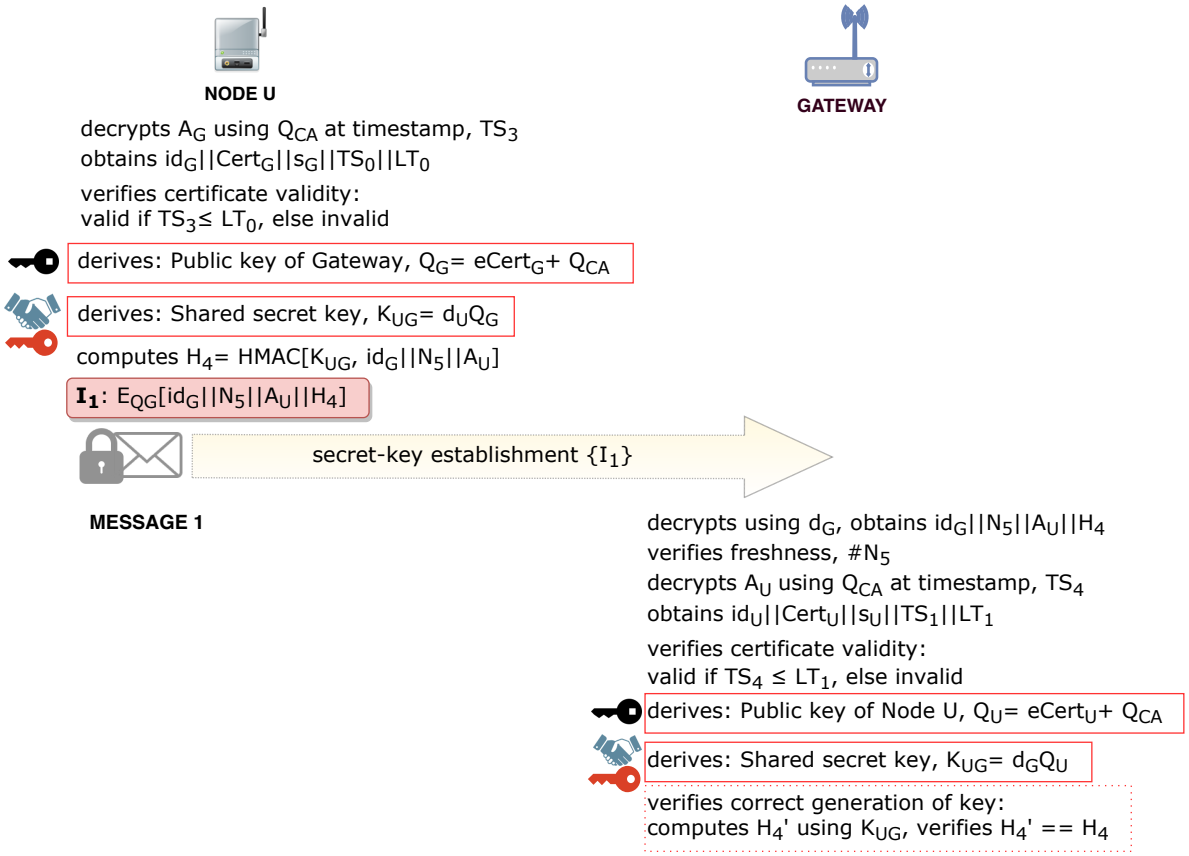

FIGURE 4. Key Establishment between Node U and Gateway.

C_7: $K_{2T} = Hash(id_U \| R_{2U} \| N_6)$
C_8: $H_6 = Hash(A_{2U})$
$\mathbb{D}_3$: $E_{Q_G}[id_G \| N_8 \| \{E_{K_{2T}}[A_{2U} \| H_6]\}]$ $\{CA \rightarrow G_w\}$
C_9: $D_{d_G}[id_G \| N_8 \| \{E_{K_{2T}}[A_{2U} \| H_6]\}]$
C_{10}: $H_7 = N_9 \oplus id_G$
$\mathbb{D}_4$: $H_7 \| \{E_{K_{2T}}[A_{2U} \| H_6]\}$ $\{G_w \rightarrow Node\ \mathrm{U}\}$
C_{11}: $K_{2T} = Hash(id_U \| R_{2U} \| N_6)$
C_{12}: $D_{K_{2T}}[A_{2U} \| H_6]$
C_{13}:$D_{Q_{CA}}[id_U \| Cert_{2U} \| s_{2U} \| TS_5 \| LT_2]$ (Decrypted at TS_6)
Note: $Cert_{2U}$ is valid if this condition is true: $TS_6 \leq LT_2$, else invalid.
C_{14}: $d_{2U} = er_{2U} + s_{2U} (\mathrm{mod}\ n)$ {private key}
C_{15}: $Q_{2U} = eCert_{2U} + Q_{CA}$ {public key}

IV. SECURITY ANALYSIS

The strength of the proposed protocol, LKE has been analyzed through formal and informal analysis. The inferences obtained from analysis are presented in this section.

A. FORMAL ANALYSIS

Following [22], [25], [27], [31], [37], and [40], we have used AVISPA (Automated Validation of Internet Security Protocols and Applications) tool to examine the robustness of the proposed protocol under the influence of the Dolev-Yao adversary model. The examination using the AVISPA requires conversion of security protocol algorithm to High Level Protocol Specification Language (HLPSL). AVISPA transforms the HLPSL script file to an Intermediate Format (IF) using a HLPSL2IF translator. The Intermediate Format is then provided to the backend (e.g., on-the-fly model-checker (OFMC)) of the AVISPA for compilation of results. The discussion on various backends of AVISPA is intentionally omitted, interested readers may refer to [41]. Conclusively, the backend produces the Output file (OF) inferring the protocol as safe or unsafe.

The HLPSL script initially discusses the basic roles to be played by the agents and define local declarations. Basic role represents the change in the states of the node when certain events are met. Contrarily, composition role does not make any transitions rather administer numerous sessions concurrently. The environment role is the last section of the script which constitutes of one or more sessions and global constants. In addition, the behaviour of the intruder (i) is also defined in the environment role. It is also mentioned in this role that communication between the entities happen over the compromised channel (dy), i.e., the channel is vulnerable to all types of attacks mentioned in the Dolev-Yao (DY) adversary model.

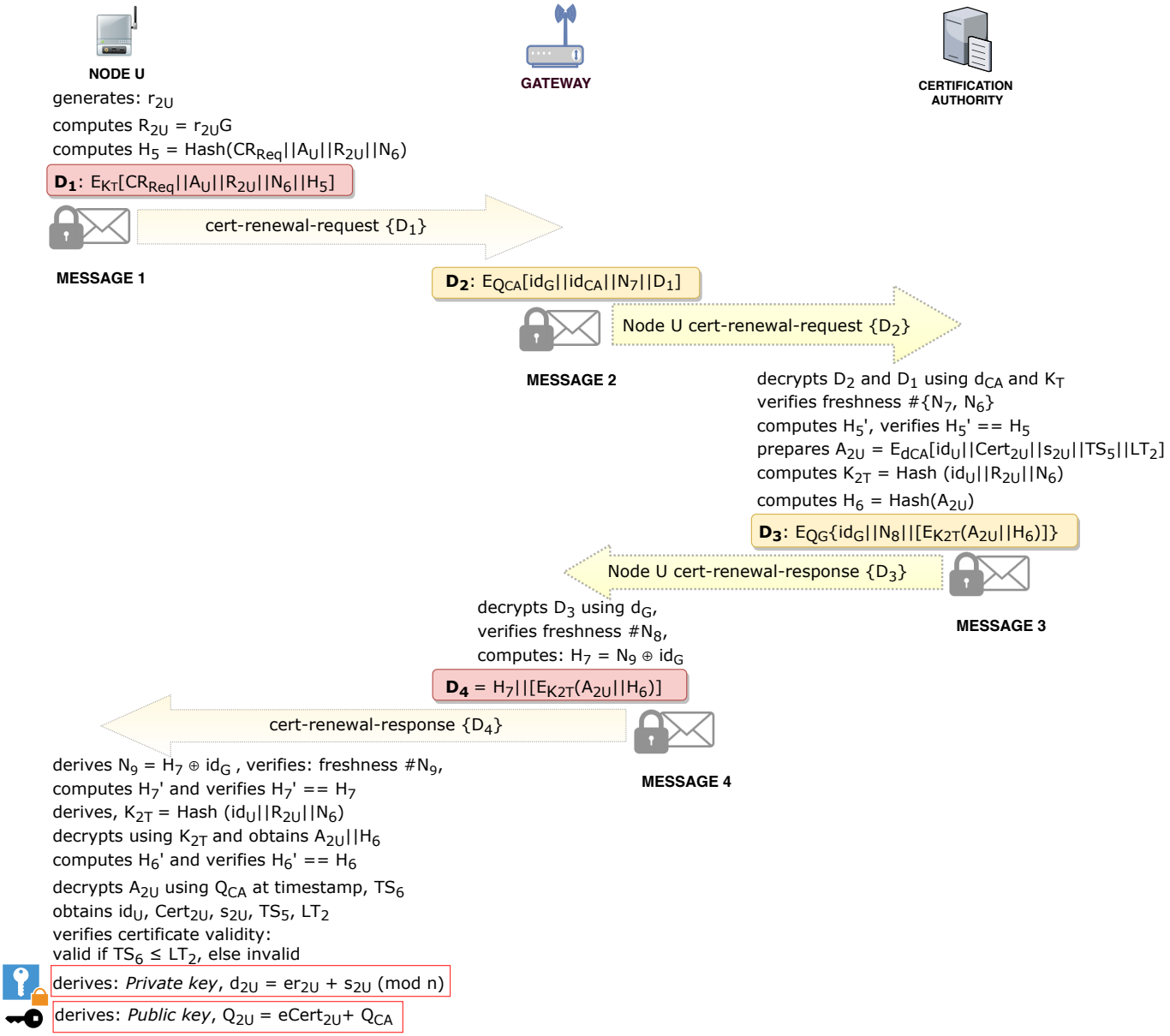

FIGURE 5. Certificate Renewal Phase.

To evaluate the robustness of LKE, the mutual authentication and secret key establishment phase is scripted in HLPSL and examined on AVISPA. At first, basic roles of node U and Gw are described which includes agent attributes (U, Gw), crypto operations, local declarations (Qu, Du, etc.), channel (dy), initial state and transitions. Node U initiates the communication. Post initialization at *State* = 0 [RCV($start$)], it succeeds to *State* = 1, where fresh nonce is constructed, $N5' := new()$ and appended with $Au' = \{Idu.Certu.Su.Ts1.Lt1\}\_Qca$, and $H4' = Hmac(Kug.Idg.N5.Au)$. Node U transmits $I1'$ to the gateway for achieving mutual authentication and secret key establishment assuming dolev-yao (dy) channel characteristics. The goal predicates set by the Node U is the privacy of the authenticator, i.e., Au' & anonymity of the gateway identity i.e., Idg' as depicted in Fig. 6 (a).

Gateway receives the $I1'$ in its initial state, *State* = 1 [RCV($I1'$)] and retrieves the data during 2^{nd} *State*. Gateway executes specific operations for the strong realization of mutual authentication and key establishment as presented in Fig. 6 (b). Gw decrypts $I1'$ using Dg and extracts Idg,$N5$,Au,$H4$. Similarly, Gw decrypts Au' using Qca and recovers node U credentials (Idu,$Certu$,Su) with timestamp ($Ts1$) and lifetime ($Lt1$). The verification of $N5'$ and $Lt1'$ is formed in terms of goals predicate *witness* $\{nodeU\_gateway\_lt1\}$ and $\{nodeU\_gateway\_n5\}$. Witness makes sure that the life-

```
role nodeU (U,Gw: agent,
            Hmac: hash_func,
       Qca,Qg,Qu: public_key,
       Dg,Du,Kug: symmetric_key,
         SND,RCV: channel (dy))
played_by U def=
local
State: nat,
Idu,Idg,Certu,Certg,Su,Sg,Ts0,
Ts1,Lt0,Lt1,N5,Au,Ag,H4:text,
I1: message
init State:= 0
transition
1. State = 0
/\ RCV(start) =|>
   State':= 1
/\ N5':= new()
/\ Ag':= {Idg.Certg.Sg.Ts0.Lt0}_Qca
/\ Au':= {Idu.Certu.Su.Ts1.Lt1}_Qca
/\ H4':= Hmac(Kug.Idg.N5.Au)
/\ I1':= {Idg.N5.Au.H4}_Qg
/\ SND(I1')
/\ secret({Idg,Au'},sub1,{U,Gw})
end role
```

(a)

```
role gateway (U,Gw: agent,
              Hmac: hash_func,
         Qca,Qg,Qu: public_key,
         Dg,Du,Kug: symmetric_key,
           SND,RCV: channel (dy))
played_by Gw def=
local
State :nat,
Idu,Idg,Certu,Su,
Ts1,Lt1,N5,Au,H4:text,
I1: message
init State:= 1
transition
1. State = 1
/\ RCV(I1') =|>
   State':= 2
/\ I1':= {Idg.N5.Au.H4}_Dg
/\ Au':= {Idu.Certu.Su.Ts1.Lt1}_Qca
/\ H4':= Hmac(Kug.Idg.N5.Au)
/\ witness(Gw,U,nodeU_gateway_n5,N5)
/\ witness(Gw,U,nodeU_gateway_lt1,Lt1)
end role
```

(b)

FIGURE 6. Role Specification of the Node U and Gateway.

```
role session (U,Gw: agent,
              Hmac: hash_func,
         Qca,Qg,Qu: public_key,
         Dg,Du,Kug: symmetric_key)
def=
local SU,RU,SGw,RGw: channel(dy)
composition
  nodeU(U,Gw,Hmac,Qca,Qg,Qu,Dg,Du,Kug,SU,RU)
/\gateway(U,Gw,Hmac,Qca,Qg,Qu,Dg,Du,Kug,SGw,RGw)
end role
```

(a)

```
goal
secrecy_of sub1
authentication_on nodeU_gateway_n5
authentication_on nodeU_gateway_lt1
end goal
environment ()
```

(c)

```
role environment ()
def=
const    nodeU,gateway: agent,
             qca,qg,qu: public_key,
dg,du,kug,dgi,dui,kugi: symmetric_key,
idu,idg,certu,certg,su,sg,
ts0,ts1,lt0,lt1,n5,au,ag,h4: text,
hmac: hash_func,
nodeU_gateway_n5,nodeU_gateway_lt1,
sub1: protocol_id
intruder_knowledge =
{nodeU,gateway,hmac,dgi,dui,qca,qg,qu}
composition
  session(nodeU,gateway,hmac,qca,qg,qu,dg,du,kug
/\session(nodeU,i,hmac,qca,qg,qu,dgi,dui,kugi)
/\session(i,gateway,hmac,qca,qg,qu,dgi,dui,kugi)
end role
```

(b)

FIGURE 7. Specification of the session, environment and goal for the proposed LKE.

time (LT) of the certificate ($Certu$) and freshness ($N5$) of the message ($I1'$) is validated before use. Gateway at *State* = 2, examines (witness(Gw,U,$nodeU\_gateway\_lt1$,Lt)) the validity of $Certu$ along with freshness (witness(Gw,U,$nodeU\_gateway\_n5$,$N5$)) before initiating the process of secret key establishment.

Fig. 7 (a) demonstrates the structure of agents arguments. $(U, Gw, Hmac, Qca, Qg, Qu, Dg, Du, Kug, SU, RU)$ $(U, Gw, Hmac, Qca, Qg, Qu, Dg, Du, Kug, SGw, RGw)$ Aforementioned arguments are either transmitted or applied by the agents during the session. The most significant is the environment role because it declares global constants, describes intruder behaviour, elucidates organization of sessions, and establishes goals of interest. Following DY adversary model, an attacker can eavesdrop, obstruct, and examine the information e.g., $\{nodeU$,$gateway$,$hmac$,dgi,dui,qca,qg,$qu\}$ etc. The intruder information is declared in the environment role and is utilized by the AVISPA (OFMC, Constraint-Logic-based Attack Searcher (CL-AtSe)) during the vulnerability assessment of the LKE against attacks. The subsequent segment of the environment role (Fig. 7 (b)) defines the numerous

```
% OFMC
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/
              results/IIOT.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.04s
  visitedNodes: 18 nodes
  depth: 4 plies
```

(a)

```
% CL-AtSe
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/
              results/IIOT.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed    : 0 states
  Reachable   : 0 states
  Translation: 0.01 seconds
  Computation: 0.00 seconds
```

(b)

FIGURE 8. LKE results using OFMC and CL-AtSe backend.

sessions of dialogue exchanges between entities.

Although it is anticipated to have sessions between legitimate agents only ($nodeU$,$gateway$,$hmac$,qca,qg,qu,dg,du, kug), but the likelihood of intruder intruding in the session of authentic nodes also exists ($nodeU$,i,$hmac$,qca,qg,qu,dgi, dui,$kugi$), (i,$gateway$,$hmac$,qca,qg,qu,dgi,dui,$kugi$).

Overall, 3 goals are defined out of which one is linked with secrecy, and the other 2 corresponds to authentication as exhibited in Fig. 7 (c). The summary of the goals are:

- Secrecy_of sub1 represents that $\{Au, Idg\}$ are kept secret between node U and gateway.
- Authentication_on nodeU_gateway_lt1 states that the lifetime (i.e., $Lt1$) of certificate $\{Certu\}$ will be validated at the gateway.
- Authentication_on nodeU_gateway_n5 states that the freshness (i.e., $N5$) of message $\{I1'\}$ will be confirmed at the gateway.

The strength of the LKE against attacks is tested using the OFMC backend. Fig. 8 (a) and Fig. 8 (b) demonstrate that LKE can resist critical attacks and is declared safe to use in Industrial IoT applications. Similarly, the CL-AtSe backend also declared the protocol as safe. Consequently, the attacks studied in the Dolev-Yao adversary model cannot damage the LKE security protocol.

B. INFORMAL ANALYSIS

The informal analysis proves the robustness of the proposed protocol against many known attacks.

Prevention against Replay: LKE can resist against replay attack. Suppose adversary (i.e., Eve) eavesdrops the message exchanged between Node U and Gateway and captures either,
M_1: $E_{Q_{CA}}[id_U \| R_U \| id_G \| N_1 \| H_1]$,
M_4: $H_3 \| E_{K_T}[A_U \| A_G \| H_2]$,
I_1: $E_{Q_G}[id_G \| N_5 \| A_U \| H_4]$ or all.
An adversary may launch the replay attack by resending the message M_1' or I_1' at different time intervals to the gateway to perform unauthorized operations. Replayed M_1' is received and processed by the Gateway, M_2: $E_{Q_{CA}}[id_G \| id_{CA} \| N_1 \| M_1']$ and sent to CA. Since M_1' contains the old nonce (N_1), therefore verification fails at CA. Similarly, adversary replay's I_1' to gateway but it is also perceived as dishonest as it contains the old nonce (N_5). In the same way, adversary may eavesdrop messages exchanged between CA and G_w e.g., M_2' (M_2: $E_{Q_{CA}}[id_G \| id_{CA} \| N_2 \| M_1]$) and M_3' (M_3: $E_{Q_G}\{id_G \| N_3 \| [E_{K_T}[A_U \| A_G \| H_2]\}$) and replay it to obtain authorizations. However, it will be identified as fraudulent due to presence of old nonces (N_2, N_3) in the replayed messages. Furthermore, adversary cannot read and alter the nonces (N_1, N_2, N_3, N_5) as messages M_1, M_2 are ciphered with the public key of CA (Q_{CA}) and M_3 is encrypted with public key of the Gateway (Q_G) and hence any alteration requires either the private key of CA or gateway which is unknown to Eve. Thus, proposed scheme is resilient to replay attacks.

Prevention against Impersonation: Impersonation is an identity theft which may lead to disclosure of information to non legitimate entities. In this attack, eve creates the fraudulent message $E_{Q_{CA}}[id_{eve} \| R_{eve} \| id_G \| N_1' \| Hash(id_{eve} \| R_{eve} \| id_G \| N_1)]$ to initiate new session by being Node U. Eve could not obtained real identity of Node U while intercepting the information, therefore eve constructed id_{eve} for impersonating node U. Nonetheless, CA could not verify the fake identity of eve in the database ($id_{eve} \neq id_U$) and aborts the request. Even impersonating Node U during key establishment phase $E_{Q_G}[id_G \| N_5 \| A_U \| HMAC_1[K_{UG}, id_G \| N_5 \| A_U]$ would not be possible for eve as he does not possess K_{UG} which is required for generating $HMAC_1$. Thus, it is not feasible to launch impersonation attacks in LKE.

Prevention against Modification of Messages: Assuming that eve captured the messages e.g., M_1, M_2 etc. Eve intentionally try to forge the messages such as $E_{Q_G}[id_G \| N_5 \| A_U \| HMAC_{eve}[K_{Ueve}, id_G \| N_5 \| A_U]$. It can be detected easily at the gateway since $HMAC_{eve}$ is not computed using the correct key, K_{UG}. Similarly, any alterations in message, M_4 requires the knowledge of symmetric key K_T, which is available either with CA or Node U. It can be witnessed that all the messages exchanged (M_1-M_4, I_1) are sent after ciphering (using any of these keys $E_{Q_{CA}}, E_{Q_G}, E_{K_T}, K_{UG}$) and hashing ($H, HMAC_1$), thus leaving no scope for adversary to conduct modifications. Therefore, LKE is free from message forgery attack.

Prevention against Denial of Service (DoS): Assume an attacker can make use of old captured messages, and can send them to keep the system busy that would lead to the DoS attack [42], [43]. The DoS attacks does not only disrupt the services to be offered to the legitimate entity rather it leads to wastage of node resources like bandwidth, and power etc. LKE mitigates the DoS attacks to some extent. The Eve may intercept and replay M_1 $\{E_{Q_{CA}}[id_U \| R_U \| id_G \| N_1 \| Hash(id_U \| R_U \| id_G \| N_1)]\}$ to initiate DoS. As the replayed message contains the old nonce (N_1), therefore CA identifies it as a replay attack.

TABLE 2. Storage Cost of Proposed Algorithm

Parameters	Node	Gateway	CA
n, G	✓		✓
r_U	✓		
r_{CA}			✓
R_U	✓		✓
id_U, id_G, Q_G, Q_{CA}	✓	✓	✓
Id_{CA}		✓	✓
d_U	✓		
Q_U	✓	✓	
d_G		✓	
d_{CA}			✓
K_T	✓		✓
K_{UG}	✓	✓	
A_U	✓	✓	✓
A_G	✓		✓
N_1	✓		✓
N_2		✓	✓
N_3		✓	✓
N_4	✓		
N_5	✓	✓	
Total Cost (bytes)	368	252	305

TABLE 3. Analysis and Comparison of Protocols based on protection against attacks and security goals

$\mathcal{ASF}$	[24]	[28]	[29]	[30]	[31]	[32]	[33]	LKE
$\mathcal{A}_1$	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{A}_2$	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{A}_3$	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{A}_4$	✓	×	×	×	✓	×	×	✓
$\mathcal{A}_5$	✓	×	✓	×	✓	×	✓	✓
$\mathcal{A}_6$	×	×	✓	✓	✓	✓	✓	✓
$\mathcal{SF}_1$	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{SF}_2$	✓	×	×	×	×	×	×	✓
$\mathcal{SF}_3$	✓	×	×	✓	✓	✓	✓	✓
$\mathcal{SF}_4$	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{SF}_5$	✓	✓	✓	×	✓	✓	✓	✓
$\mathcal{SF}_6$	✓	✓	$\mathcal{P}$	✓	$\mathcal{P}$	$\mathcal{P}$	✓	✓

Acronyms: ✓: Protected against attacks/Compliance to security and other goals, ×: Vulnerable against attacks/non compliance to security and other goals, $\mathcal{ASF}$: Attacks and Security features, $\mathcal{A}_1$: Replay, $\mathcal{A}_2$: Impersonation, $\mathcal{A}_3$: Modification of messages, $\mathcal{A}_4$: DoS, $\mathcal{A}_5$: MITM, $\mathcal{A}_6$: Known key, $\mathcal{SF}_1$: Mutual authentication, $\mathcal{SF}_2$: Data privacy, $\mathcal{SF}_3$: Session key security, $\mathcal{SF}_4$: Message integrity, $\mathcal{SF}_5$: Message freshness, $\mathcal{SF}_6$: Identity anonymity, $\mathcal{P}$: Partially achieved

Thus, irrespective of initiating new session with the illegitimate node, CA aborts the request and preserves its resources for legitimate nodes. Moreover, the Eve could not alter the nonce of M_1 as it is encrypted. Similarly, $M_2 - M_4$ and I_1 are prevented from *DoS* attacks as they all constitutes of fresh nonces, $N_2 - N_5$, respectively. Thus, the proposed scheme can resist such *DoS* attacks.

Prevention against MITM: The intruder in this attack intercepts the information exchanged between the two legitimate parties and breaks their connection virtually. The intruder process is so transparent and smooth that the legitimate communicating parties never become aware of this virtual breakage. Let's suppose the intruder eavesdrop $\{E_{Q_{CA}}[id_U \| R_U \| id_G \| N_1 \| Hash(id_U \| R_U \| id_G \| N_1)]\}$ the information, and tries to modify it for playing *MITM*. This attempt would be unsuccessful because any modifications are permitted with use of d_{CA} which is not available with Eve. Nevertheless, eve may still try a vague attempt to modify with a forged key and replaces the information with $E_{Q_{CA}}[id_U \| R_U \| id_G \| N_1 \| Hash(id_U \| R_U \| id_G \| N_1)]_{eve}$.

However, this attempt can be detected at CA as decrypted information would not produce the correct message, $id_U \| R_U \| id_G \| N_1 \neq Hash(id_U \| R_U \| id_G \| N_1)$. Similarly, the eve would not be able to perform *MITM* using the remaining messages as they are also encrypted with secret keys, $E_{Q_{CA}}[id_G \| id_{CA} \| N_2 \| M_1]$; $E_{Q_G}\{id_G \| N_3 \| E_{K_T}[A_U \| A_G \| H_2]\}$; $H_3 \| E_{K_T}[A_U \| A_G \| H_2]$; $E_{Q_G}[id_G \| N_5 \| A_U \| H_4]$. Thus, adversary cannot play *MITM* in LKE protocol.

Prevention against Known Key: Consider that eve has intercepted previous message exchanges and is trying to retrieve secret key related information from intercepted messages for producing new secret keys. As aforesaid that secret keys (e.g., K_{UG}) in LKE uses a secret random integer (e.g., r_U) which is fresh and independent for each certificate, thereby making the future secret key ($K_{UG1} = d_U Q_V$) different and independent. So even if Eve obtains the old secret key (K_{UG}) somehow, he would not be able to construct new secret key (K_{UG1}) as it requires the knowledge of r_{U1} which is not available with eve. Therefore, having the knowledge of past secret keys does not help the eve to initiate new sessions.

LKE adheres to all essential properties required to provision security in networks.

LKE attains Data Privacy: Disclosure of information or either key poses a threat to misuse of information. To avoid misuse, LKE encrypts all the messages to prevent unauthorized access. For instance, Node U encrypts $I_1 : E_{Q_G}[id_G \| N_5 \| A_U \| H_4]$, thus allowing only the Gateway to decrypt and interpret. Even other messages such as $M_1 - M_4$ are secured. Thus, even if the adversary intercepts the message $M_1 - M_4$ and I_1, he would not be able to access the content without the key, therefore preserving the data confidentiality.

LKE promises Message Integrity: Alteration ruins the real identity of the message. Forged messages must be detected to prevent the processing of counterfeited requests. LKE makes use of Hash in $M_1(Hash(id_U \| R_U \| id_G \| N_1))$, $M_2(Hash(id_U \| R_U \| id_G \| N_1))$, $M_3(Hash(A_U \| A_G))$, and $M_4(Hash(A_U \| A_G))$ whereas I_1 uses $HMAC([K_{UG}, id_G \| N_5 \| A_U])$. Hash and HMAC are the one way functions used to preserve integrity in all messages exchanged in the scheme. Thus, proposed scheme (LKE) exhibits the property of message integrity.

LKE ensures Message Freshness: Replicated authorization messages may provide adversary the access to high priv-

TABLE 4. Computation Cost of Scheme LKE for various phases of Operation

Phase	Node	Gateway	CA	Total Cost
Network Set-up Phase	$1AS_E + 1AS_D + 1S_D + 3H_G + 1H_V$	$1AS_E + 1AS_D$	$2AS_E + 2AS_D + 1S_E + 3H_G + 1H_V$	$4AS_E + 4AS_D + 1S_E + 1S_D + 6H_G + 2H_V$
Key Establishment Phase	$1AS_E + 1AS_D + 1H_G + 1HMAC_G$	$2AS_D + 1H_G + 1HMAC_V$	-	$1AS_E + 3AS_D + 2H_G + 1HMAC_G + 1HMAC_V$
Total	$2AS_E + 2AS_D + 1S_D + 4H_G + 1H_V + 1HMAC_G$	$1AS_E + 3AS_D + 1H_G + 1HMAC_V$	$2AS_E + 2AS_D + 1S_E + 3H_G + 1H_V$	$5AS_E + 7AS_D + 1S_E + 1S_D + 8H_G + 2H_V + 1HMAC_G + 1HMAC_V$

Acronyms: AS_E - Asymmetric encryption, AS_D - Asymmetric decryption, H_G - Hash generation, H_V - Hash verification, S_E - Symmetric encryption, S_D - Symmetric decryption, $HMAC_G$ - Hash based MAC generation, $HMAC_V$ - Hash based MAC verification, *Numerical values* - It indicates the number of times the cryptography operation is being executed.

TABLE 5. Computation Cost Comparison for Key Establishment Phase: Between Smart Node and Gateway

Schemes	Node	Gateway	Total Cost
[24]	$7H_G + 1R_G + 3L_{XOR}$	$9H_G + 5L_{XOR}$	$16H_G + 1R_G + 8L_{XOR}$
[28]	$4H_G + 2S_E$	$8H_G + 4S_E + 1M_{EC}$	$12H_G + 6S_E + 1M_{EC}$
[29]	$7H_G + 1R_G + 4L_{XOR}$	$7H_G + 1R_G + 6L_{XOR}$	$14H_G + 2R_G + 10L_{XOR}$
[30]	$5H_G + 1L_{XOR} + 2M_{EC}$	$9H_G + 1R_G + 4L_{XOR} + 1M_{EC}$	$14H_G + 1R_G + 5L_{XOR} + 3M_{EC}$
[31]	$6H_G + 3L_{XOR} + 1M_{EC}$	$15H_G + 10L_{XOR} + 2M_{EC}$	$21H_G + 13L_{XOR} + 3M_{EC}$
[32]	$7H_G + 3L_{XOR} + 2M_{EC}$	$10H_G + 1L_{XOR}$	$17H_G + 4L_{XOR} + 2M_{EC}$
[33]	$5H_G + 3L_{XOR}$	$12H_G + 2R_G + 8L_{XOR}$	$17H_G + 2R_G + 11L_{XOR}$
LKE	$1AS_E + 1AS_D + 1H_G + 1HMAC_G + 1L_{XOR}$	$2AS_D + 1H_G + 1HMAC_V + 1L_{XOR}$	$1AS_E + 3AS_D + 2H_G + 1HMAC_G + 1HMAC_V + 2L_{XOR}$

Acronyms: AS_E - Asymmetric encryption, AS_D - Asymmetric decryption, H_G - Hash generation, $HMAC_G$ - Hash based MAC generation, $HMAC_V$ - Hash based MAC verification, R_G - Random Number Generation, L_{XOR} - Logical Operation XOR, S_E - Symmetric encryption, M_{EC} - Scalar Multiplication ECC, *Numerical values* - It indicates the number of times the cryptography operation is being executed.

ileged and non authorized resources. LKE therefore possess freshness component i.e., timestamp $(TS_0 - TS_4)$ and nonce $(N_1 - N_5)$, in all messages exchanged between CA, gateway and nodes. The nonce and timestamp ensures the abortion of process at receiving entity when stale requests are received. Thus, LKE exhibits the property of message freshness.

LKE procured the property of Identity Anonymity: In LKE, the identity of the industrial node (id_U), gateway (id_G), and CA (id_{CA}) are exchanged as ciphertext to ensure attainment of identity anonymity [24], [28], [30], [31], [33]. Assume if an adversary captures the message I_1 $(E_{Q_G}[id_G \| N_5 \| A_U \| H_4])$ containing the identity details of the gateway (id_G), still the adversary would not be able to extract the identity information as it is secured using strong encryption algorithm. Therefore, the communication remains anonymous to others. Similarly, other messages M_1, M_2, and M_3 carrying identity details (id_U, id_G, and id_{CA}) preserve the anonymity. Thus, LKE exhibits the property of identity anonymity to some extent.

V. PERFORMANCE AND COMPARATIVE ANALYSIS

The employability of any scheme in practical environment depends upon its performance. The performance attributes of the proposed scheme (considering *Telos* B *mote* as the node) is observed and presented in this section. Table 2 presents the storage cost requirements for various entities involved in the proposed scheme. The storage cost requirements (*all phases*) for node, gateway and CA are 368, 252 and 305 bytes, respectively. The storage space available in CM5000 Telos B mote [44] is 1 MB whereas the storage requirement in proposed scheme for achieving authentication is just 0.03 %. Thus, LKE accomplishes the goal of performing authentication and key exchange with a small storage requirement.

Table 3 points out the various security features that LKE exhibit along with the various attacks that LKE can resist. From the table it is witnessed that LKE provides robustness against all the potential attacks mentioned in the Dolev-Yao attack model [34]. Table 3 signifies the superiority of LKE over existing techniques [24], [28]–[33] in terms of resistance against attacks and security features.

The various cryptography operations used by node, gateway and CA during network set-up and key establishment phase are given in Table 4. It can be well observed from the table 4 that resource constrained node executes only a few operations whilst performing registration and key establishment process. The cryptography operations used by the entities (node, G_W, CA) are asymmetric and symmetric ciphering, hash and hash based message authentication code (HMAC).

Table 5 provides a comparison of proposed scheme with state-of-the-work over computation cost between smart node and gateway. The comparison is carried out for *key establishment phase* only as the *registration phase* occurs once during network initialization. The parameters considered for comparison are asymmetric and symmetric ciphering, hash, HMAC, random number generation, exclusive-OR, and scalar multiplication in ECC. Results disclosed the efficiency

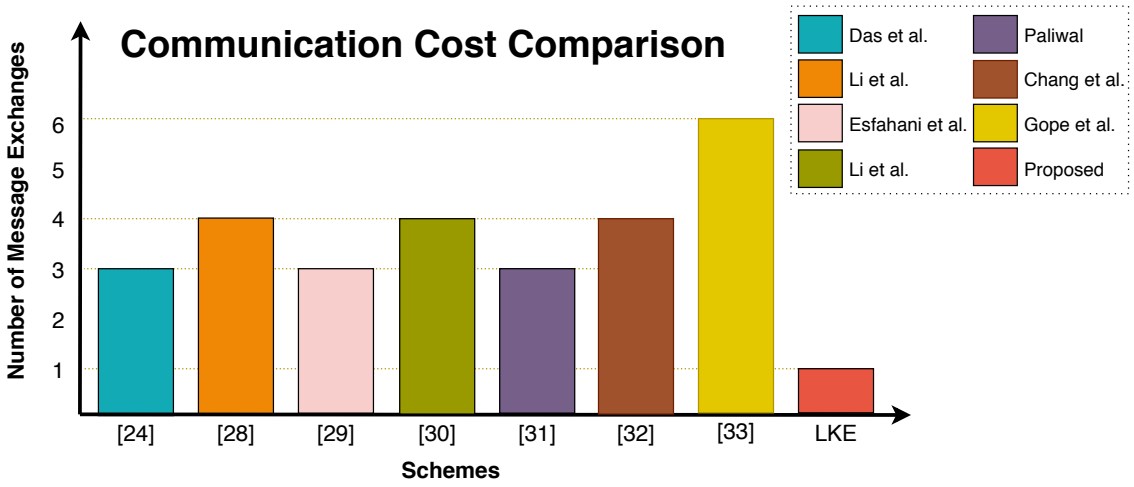

FIGURE 9. Communication Cost Comparison.

TABLE 6. Energy Cost for communication: Considering Resource Constrained Smart device (Key Establishment Phase)

	$T_X(mJ)$	$R_X(mJ)$	$T_{EC}(mJ)$
[24]	0.368	0.285	0.653
[28]	0.230	0.518	0.748
[29]	0.461	0.311	0.772
[30]	0.345	0.388	0.733
[31]	U_D	0.738	0.738
[32]	0.282	0.421	0.703
[33]	0.369	1.036	1.405
LKE	0.519	-	0.519

Acronyms: T_X - Transmission, R_X - Reception, T_{EC} - Total Energy Cost, U_D - Undisclosed, Hyphen (-) No consumption

of the scheme. LKE executes hash only twice whereas other schemes such as [24], [28]–[33] executes hash 16, 12, 14, 14, 21, 17, and 17 times, respectively in key establishment phase. In addition, LKE computes *XOR* operation 2 times in contrast to 8, 10, 5, 13, 4, and 11 times by the schemes [24], [29]–[33], respectively. Similarly, other operations (ciphering, scalar multiplication, etc.) as shown in Table 5 are being executed many times by the traditional techniques to perform key establishment, resulting in over-exhaustion of the node resources. Consequently, LKE attains all necessary features like data privacy, authentication, integrity and availability etc. with limited computations.

Communication energy cost of the LKE and existing schemes are mentioned in the Table 6. As per the specifications of the Telos B mote [44], transmission and reception of each bit cost 0.72×10^{-3} mJ and 0.81×10^{-3} mJ of energy, respectively. The total number of bits communicated by the resource constrained smart device during key establishment phase is 864 bits in [24], 960 bits in [28], 1024 bits in [29], 960 bits in [30], 912 bits in [31], 912 bits in [32], 1792 bits in [33], and 720 bits in LKE. Due to small overheads, the energy consumed by LKE is 0.519 mJ which is much lesser than the energy consumed by other schemes. Excessive energy consumption can deplete the energy reserves of the node, i.e., reducing effective lifetime of the node [24], [28]–[33]. Therefore, table 5 and table 6 proves that the LKE is considerably lightweight and energy efficient in contrast to other schemes.

Fig. 9 illustrates the total number of messages exchanged between the communicating entities during mutual authentication and key exchange phase. It can be noticed that LKE achieves the goal in just 1 message while other schemes [24], [28]–[33] exchanged minimum 3 messages to carry out the same piece of work. Excessive exchange of messages indicate more delay, overhead, and energy exhaustion [24], [28]–[33]. Therefore, LKE again proves the superiority of being energy and time efficient over existing traditional techniques.

VI. CONCLUSION

Industry 4.0 strives to achieve faster production, resource efficiency, reduced costs, better product quality, automation and quicker fault detection. All these benefits motivate the industry caretakers to converge to Industrial IoT (I4.0). But the threat of unauthorized abuses is causing hindrance to its realization. This paper unveils a Lightweight key exchange (LKE) scheme to prevent unauthorized entities from accessing the industrial network. The LKE protocol provides mutual authentication and secret key exchange mechanism with *computational* and *communicational efficiency*. Results from security analyzer tool *AVISPA* reveals that the suggested technique is reported safe to use in Industrial IoT applications. Moreover, informal security analysis proved that LKE fulfils the security requirements proposed by *NIST* for security protocols. The scheme has the *least* energy consumption (0.519 mJ) and message exchange requirement (1 *message*) in comparison to state-of-the-work which makes it fit for use in all types of Industrial networks.

ACKNOWLEDGMENT

The authors would like to thank Editor-in-Chief, Associate Editor and anonymous Reviewers for their valuable reviews.

REFERENCES

[1] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on industrial internet of things: A cyber-physical systems perspective," IEEE Access, vol. 6, pp. 78 238–78 259, 2018.
[2] Infosys, "Industry 4.0 as an evolution, not a revolution," https://www.infosys.com/about/knowledge-institute/insights/Documents/industry-4.0-evolution.pdf, 2019, online; accessed January 2, 2020.
[3] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–2243, 2014.
[4] Deloitte, "Industry 4.0: An introduction)," 2015, online; accessed January 2, 2020.
[5] B. Chen, J. Wan, L. Shu, P. Li, M. Mukherjee, and B. Yin, "Smart factory of industry 4.0: Key technologies, application case, and challenges," IEEE Access, vol. 6, pp. 6505–6519, 2017.
[6] M. Kohler, "Industry 4.0: 10 use cases for software in connected manufacturing," https://blog.bosch-si.com/industry40/industry-4-0-10-use-cases-for-software-in-connected-manufacturing/, 2018, online; accessed February 7, 2020.
[7] S. Souchet, "Industry 4.0 case studies," https://home.kpmg/xx/en/home/insights/2018/11/industry-4-0-case-studies.html, 2019, online; accessed February 7, 2020.
[8] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: a comprehensive survey," IEEE Access, vol. 3, pp. 678–708, 2015.
[9] S. Kim, M. Lee, and C. Shin, "Iot-based strawberry disease prediction system for smart farming," Sensors, vol. 18, no. 11, p. 4051, 2018.
[10] H. Mouratidis and V. Diamantopoulou, "A security analysis method for industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 14, no. 9, pp. 4093–4100, 2018.
[11] T. P. Raptis, A. Passarella, and M. Conti, "Data management in industry 4.0: State of the art and open challenges," IEEE Access, vol. 7, pp. 97 052–97 093, 2019.
[12] G. Aceto, V. Persico, and A. Pescapé, "A survey on information and communication technologies for industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges," IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3467–3501, 2019.
[13] E. T. Nakamura and S. L. Ribeiro, "A privacy, security, safety, resilience and reliability focused risk assessment methodology for iiot systems steps to build and use secure iiot systems," in 2018 Global Internet of Things Summit (GIoTS). IEEE, 2018, pp. 1–6.
[14] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security issues in iiot: A comprehensive survey of attacks on iiot and its countermeasures," in 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN). IEEE, 2018, pp. 124–130.
[15] S. L. Keoh, "Cyber-Physical Systems Are at Risk," https://www.infosecurity-magazine.com/next-gen-infosec/cyberphysical-systems-risk-1/ , 2019, online; accessed March 4, 2020.
[16] T. Armerding, "Cyber-physical attacks are growing alongside the IoT," https://www.synopsys.com/blogs/software-security/cyber-physicalattacks/ , 2019, online; accessed March 4, 2020.
[17] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the internet of things," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1636–1675, 2018.
[18] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1606–1616, 2018.
[19] N. Moustafa, E. Adi, B. Turnbull, and J. Hu, "A new threat intelligence scheme for safeguarding industry 4.0 systems," IEEE Access, vol. 6, pp. 32 910–32 924, 2018.
[20] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of things for smart healthcare: Technologies, challenges, and opportunities," IEEE Access, vol. 5, pp. 26 521–26 544, 2017.
[21] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—a survey," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802–1831, 2017.
[22] S. Khan, A. I. Alzahrani, O. Alfarraj, N. Alalwan, and A. H. Al-Bayatti, "Resource efficient authentication and session key establishment procedure for low-resource iot devices," IEEE Access, vol. 7, pp. 170 615–170 628, 2019.
[23] H. Kim and E. A. Lee, "Authentication and authorization for the internet of things," IT Professional, vol. 19, no. 5, pp. 27–33, 2017.
[24] 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 of Things Journal, vol. 5, no. 6, pp. 4900–4913, 2018.
[25] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for internet of things: a comprehensive survey," Security and Communication Networks, vol. 2017, 2017.
[26] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, and Y. Jin, "Internet-of-things security and vulnerabilities: Taxonomy, challenges, and practice," Journal of Hardware and Systems Security, vol. 2, no. 2, pp. 97–110, 2018.
[27] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (iot) authentication schemes," Sensors, vol. 19, no. 5, p. 1141, 2019.
[28] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K.-K. R. Choo, "A robust and energy efficient authentication protocol for industrial internet of things," IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1606–1615, 2018.
[29] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. Tauber, C. Schmittner, and J. Bastos, "A lightweight authentication mechanism for m2m communications in industrial iot environment," IEEE Internet of Things Journal, vol. 6, no. 1, pp. 288–296, 2019.
[30] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3599–3609, 2018.
[31] S. Paliwal, "Hash-based conditional privacy preserving authentication and key exchange protocol suitable for industrial internet of things," IEEE Access, vol. 7, pp. 136 073–136 093, 2019.
[32] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," IEEE Transactions on wireless communications, vol. 15, no. 1, pp. 357–366, 2015.
[33] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," IEEE transactions on industrial informatics, vol. 15, no. 9, pp. 4957–4968, 2019.
[34] D. Dolev and A. Yao, "On the security of public key protocols," IEEE Transactions on information theory, vol. 29, no. 2, pp. 198–208, 1983.
[35] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," IEEE Transactions on Industrial Informatics, vol. 14, no. 9, pp. 4081–4092, 2018.
[36] "Hungary's ratio of robot use among lowest in eu," https://bbj.hu/economy/hungarys-ratio-of-robot-use-among-lowest-in-eu_160380, accessed: 2019-03-29.
[37] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, and P. H. Ha, "Anonymous secure framework in connected smart home environments," IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 968–979, 2017.
[38] J. Kim, J. Baek, and T. Shon, "An efficient and scalable re-authentication protocol over wireless sensor network," IEEE Transactions on Consumer Electronics, vol. 57, no. 2, pp. 516–522, 2011.
[39] M. Campagna, "Sec 4: Elliptic curve qu-vanstone implicit certificate scheme (ecqv)," Technical Report, 2013.
[40] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar, "Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial internet of things," IEEE Transactions on Dependable and Secure Computing, 2018.
[41] L. Viganò, "Automated security protocol analysis with the avispa tool," Electronic Notes in Theoretical Computer Science, vol. 155, pp. 61–86, 2006.
[42] Y. Zhang, C. Chen, and J. He, "Dos attack on networked control system: From the viewpoint on communication-control cost," in 2019 Chinese Automation Congress (CAC). IEEE, 2019, pp. 5695–5700.
[43] N. Enneya, A. Baayer, and M. ElKoutbi, "A dynamic timestamp discrepancy against replay attacks in manet," in International Conference on Informatics Engineering and Information Science. Springer, 2011, pp. 479–489.

[44] S. Fajarado, "CM5000 Datasheet," http://www.epssilon.cl/files/EPS5000.pdf, 2010, online; accessed February 15, 2020.

GURJOT SINGH GABA is currently pursuing Ph.D. from Lovely Professional University (L.P.U.) in Electronics and Electrical Engineering with specialization in Security of Internet of Things (IoT). He is currently working as Assistant Professor in School of Electronics and Electrical Engineering, L.P.U. His current research interests include security in cyber-physical systems, sensor networks and Internet of Things.

GULSHAN KUMAR received his Ph.D. in Computer Science from Lovely Professional University (L.P.U.), Punjab, India. Currently, he is working as Assistant Dean and Associate Prof. with the Division of Research and Development, L.P.U. His current research interests include cyber physical systems, blockchain, edge and cloud computing. Kumar has authored and co-authored more than 35 research papers including international journals (IEEE IoT, IEEE Access, Sensors, IJDSN etc.) and conferences. He is a member of various technical organizations such as IEEE, ISCA etc.

HIMANSHU MONGA obtained his Ph.D. in Optical and Wireless Networks from Thapar Institute of Engineering and Technology, Punjab, India. Presently he is working as Dean Academics and Professor at Jawahar Lal Nehru Government Engineering college (Directorate of Technical Education, Government of Himachal Pradesh) and prior to that as Director/Principal in Jan Nayak Chaudhary Devi Lal Lal Vidyapeeth, Sirsa. His current research interests include Free space optics, 5G and Internet of Things. He has authored and co-authored more than 150 Research papers in reputed conferences and journals. He is a member of IEEE, ISTE. Monga has successfully completed 6 research grant projects along with consultancy projects.

TAI-HOON KIM received the B.E. and M.E. degrees from Sungkyunkwan University, South Korea, and the Ph.D. degrees from the University of Bristol, U.K., and the University of Tasmania, Australia. He is currently with Beijing Jiotong University, Beijing, China. His main research areas are security engineering for IT products, IT systems, development processes, and operational environments

MADHUSANKA LIYANAGE (S07, M16) received his Ph.D. in Communication Engineering in 2016 from University of Oulu, Oulu, Finland. Currently, he is working as Assistant Professor/Ad Astra Fellow at School of Computer Science, University College Dublin, Ireland. He has been a Visiting Research Fellow at the Department of Computer Science, University of Oxford, Data61, CSIRO, Sydney, Australia, the Infolabs21, Lancaster University, U.K., and Computer Science and Engineering, The University of New South Wales during 2015-2018. He is also an adjunct professor at the University of Oulu, Finland and a recipient of prestigious Marie Skłodowska-Curie Actions Individual Fellowship during 2018-2020. He has co-authored over 80 publications including three edited books and holds one patent. His research interests are SDN, IoT, Block Chain, mobile and virtual network security. URL: http://madhusanka.com

PARDEEP KUMAR received his Ph.D. in Computer Science in 2012 from Dongseo University, Busan, South Korea. Currently, he is working with the Department of Computer Science, Swansea University, United Kingdom. Previously, he worked with the Department of Computer Science, Oxford University, 2016-2018. His current research interests include security in sensor networks, smart environments, cyber physical systems, and Internet of Things.