LightIoT: Lightweight and Secure Communication for Energy-Efficient IoT in Health Informatics

Mian Ahmad Jan, *Senior Member, IEEE*, Fazlullah Khan, *Senior Member, IEEE*, Spyridon Mastorakis, *Member, IEEE*, Muhammad Adil, *Graduate Student Member, IEEE*, Aamir Akbar, *Member, IEEE*, and Nicholas Stergiou

***Abstract*—Internet of Things (IoT) is considered as a key enabler of health informatics. IoT-enabled devices are used for in-hospital and in-home patient monitoring to collect and transfer biomedical data pertaining to blood pressure, electrocardiography (ECG), blood sugar levels, body temperature, etc. Among these devices, wearables have found their presence in a wide range of healthcare applications. These devices generate data in real-time and transmit them to nearby gateways and remote servers for processing and visualization. The data transmitted by these devices are vulnerable to a range of adversarial threats, and as such, privacy and integrity need to be preserved. In this paper, we present LightIoT, a lightweight and secure communication approach for data exchanged among the devices of a healthcare infrastructure. LightIoT operates in three phases: initialization, pairing, and authentication. These phases ensure the reliable transmission of data by establishing secure sessions among the communicating entities (wearables, gateways and a remote server). Statistical results exhibit that our scheme is lightweight, robust, and resilient against a wide range of adversarial attacks and incurs much lower computational and communication overhead for the transmitted data in the presence of existing approaches.**

***Index Terms*—Health informatics, energy-efficient IoT, lightweight communication, wearables, authentication.**

I. Introduction

THE 21^{st} century has witnessed significant advancement in the development of smart devices and wireless communication technologies. These devices and technologies have found their presence in numerous applications such as smart healthcare, smart industrial automation, and smart surveillance [1]–[3]. In these applications, the Internet of Things (IoT) interconnect various sensors, actuators and smart devices with the edge servers and cloud data centres by regulating the exchange of data among them [4]. In the context of healthcare, the IoT is assumed to connect medical devices with the communication technologies to enable new applications by supporting intelligent decision-making for healthcare data [5]. Like IoT, smart healthcare technologies have improved at a rapid pace due to a massive increase in the volume of biomedical data. Therefore, IoT can play a pivotal role in the development of cost-effective and smarter healthcare applications that can monitor the patients in real-time to save their lives in an event of emergency, e.g., heart failure, sudden and acute pain, asthma attack, etc. The proliferation in mobile communication bridges the gap among the smart devices and the practitioners by providing seamless and reliable delivery of gathered data [5], [6]. This proliferation has led to a patient-centric approach that enables the remote monitoring of patients with shorter hospital stays and, in most cases, avoiding the hospital altogether.

Healthcare devices such as smart watches, fitness trackers, etc. have enabled improvements in quality of living in recent years [7], [8]. These devices sense human activities and generate real-time data about step count, sleep cycle, heart rate, and pulse count, breathing rate, and others. These devices are typically low-powered, resource-constrained, and transmit the gathered data to a nearby mobile device using wireless communication technologies [9]. For these devices, green communication is highly desirable to conserve their resources. The biomedical data generated by these devices are always sensitive, confidential, and need to be securely transmitted with their privacy preserved. In wireless networking, the communication channels are lossy and prone to various malicious attacks, for example, Denial of Service (DoS), Sybil, impersonation, and eavesdropping, are a few to mention. To this end, smart healthcare devices need to be secure, tamper-proof, and accessed by authorized and authentic users only. In health informatics, unauthorized access to the data by adversaries can wreak havoc in the healthcare sector [10].

In traditional communication networks, data security techniques are strong enough to defend against various adversarial attacks. These techniques are based on cryptography and provide data security and privacy at the expense of network resources. However, IoT-enabled smart healthcare systems have different requirements in terms of data

Manuscript received December 28, 2020; revised April 18, 2021; accepted April 27, 2021. Date of publication May 4, 2021; date of current version August 19, 2021. This work was supported in part by NIH under Grant P20GM109090; in part by NSF under Grant CNS-2016714; and in part by the Nebraska University Collaboration Initiative. *(Corresponding authors: Fazlullah Khan; Spyridon Mastorakis.)*

Mian Ahmad Jan, Fazlullah Khan, and Aamir Akbar are with the Department of Computer Science, Abdul Wali Khan University Mardan, Mardan 23200, Pakistan (e-mail: mianjan@awkum.edu.pk; fazlullah@awkum.edu.pk; amirakbar@awkum.edu.pk).

Spyridon Mastorakis is with the Department of Computer Science, University of Nebraska at Omaha, Omaha, NE 68182 USA (e-mail: smastorakis@unomaha.edu).

Muhammad Adil is with the Department of Computer Science, Virtual University of Pakistan, Lahore 54000, Pakistan (e-mail: muhammad.adil@ieee.org).

Nicholas Stergiou is with the Department of Biomechanics, University of Nebraska at Omaha, Omaha, NE 68182 USA (e-mail: nstergiou@unomaha.edu).

Digital Object Identifier 10.1109/TGCN.2021.3077318

security and system architecture. In this context, the existing cryptography-based solutions cannot be migrated directly [11]. In a smart healthcare system, the devices are connected with the Internet via a gateway that expose them to various malevolent entities. If these devices are compromised, it will be difficult to predict the nature of attacks posed by them. As a result, smart healthcare applications face botnets along with thingbots at the same time [12]. To secure the system, data integrity, data confidentiality, data availability, authenticity, and non-repudiation need to be considered [13]–[15]. Therefore, it is essential to address these challenges while keeping the resource-starving nature of healthcare devices in mind.

In this paper, we propose LightIoT, a lightweight approach for the secure transmission of biomedical data among the communicating entities. LightIoT provides secured exchange of data and robust registration for devices interested in communication. Our approach is equally applicable in any application of IoT that has security requirements, e.g., industrial automation, smart homes, smart cities, etc. In LightIoT, the resource-constrained wearables collect patients data and transmit them to a remote server via gateways (mobile terminals) [16]. LightIoT operates in three phases and makes the following contributions.

1) We propose a registration phase for the resource-constrained wearable devices. To avoid excessive delay and computational power, these devices are registered directly with a remote server in an offline phase. They are no longer required to register with the remote server via the intermediate entities, i.e., gateways. The direct registration enables these wearables to immediately deliver time-critical and delay-sensitive biomedical data for decision-making. Besides, this phase ensures green communication by conserving the resources of these wearable devices.
2) Unlike the existing approaches, we propose a significantly lightweight authentication phase that requires fewer hash functions and Exclusive OR (XOR) operations. Our proposed authentication is lightweight yet highly robust to ensure that secure sessions are established among the communicating devices, i.e., wearables, gateways and a remote server. The presence of non-reproducible pseudo random numbers ensures the privacy preservation of transmitted biomedical data.
3) Our proposed approach conserves the energy of wearables by prolonging the lifetime of the network. Besides, the lightweight security primitives reduce the end-to-end delay for exchanged messages among the communicating entities.

The rest of this paper is organized as follow. In Section II, the related work pertaining to LightIoT is presented. In Section III, the network model of LightIoT is discussed along with its design. In Section IV, we present a detailed security analysis of various malicious threats and the efficiency of LightIoT in combating them. In Section V, we present and validate our experimental results. Finally, the paper is concluded and future research directions are presented in Section VI.

II. Related Work

One of the first lightweight user authentication protocols for resource-constrained devices was proposed in 2006 [17]. This protocol is based on simple operations, such as an one-way hash function and XOR operations. However, this protocol is prone to replay, forgery, and stolen-verifier attacks. In [18], a secured healthcare system was proposed using a Wireless Body Area Network (WBAN). The use of cryptograhic primitives enable the proposed system to achieve efficiency and robustness and, at the same time, provides transmission confidentiality and authentication among the wearables and a backend server. However, the use of an asymmetric key algorithm, i.e., Elliptic-curve cryptography (ECC), incurs additional overhead for these intelligent wearables. In [19], the authors presented an authentication approach for wearables of a healthcare system. The proposed approach allows a user to authenticate his/her wearable device(s) and a mobile terminal, before establishing a session key between them. The use of bitwise XOR operations and hash functions make the proposed approach significantly lightweight for the resource-constrained wearables. A robust authentication protocol was proposed for intelligent wearables in [20]. This protocol ensures mutual authentication between a wearable and a remote server via the exchange of a session key. This exchange establishes a secure communication channel via the Internet for seamless transmission of biomedical data. However, the proposed protocol incurs computation burden on wearables due to the execution of resource-intensive cryptographic primitives.

In [21], the authors proposed a lightweight authentication approach with privacy preservation. In this approach, wearables and smartphones mutually authenticate each other in a three-step process by maintaining the anonymity of wearables. The proposed approach used XOR, concatenation, and hash functions for authentication, however, it lacks a clear explanation for achieving anonymity. Besides, it is vulnerable to Sybil, DoS and replay attacks. In [22], the authors proposed a lightweight and smart card-based authenticated key exchange scheme for resource-constrained devices. The proposed scheme uses two authentication protocols to preserves data privacy between resource-constrained devices and a gateway. The first protocol uses XOR operations and hash functions, while the second protocol uses elliptic curve cryptography along with XOR and hash functions for authentication. Chang and Le [22] scheme was investigated in [23] to verify the effectiveness and vulnerabilities factors. During statistical analysis it has been observed that the proposed model is susceptible to spoofing and user anonymity attacks.

In [24], the authors investigated the limitations and vulnerabilities of [22], [23] by demonstrating an adversary attack on these schemes. In [25], the author analyzed the lightweight RFID mutual authentication protocols to resolve the authentication problem in healthcare IoT networks. Turkanovic *et al.* [26], proposed a hash function-based lightweight authentication protocol for wearables healthcare IoT devices to resolve the validation problem in these networks. This protocol was efficient against a wide range of malicious attacks and is capable of authenticating a new device

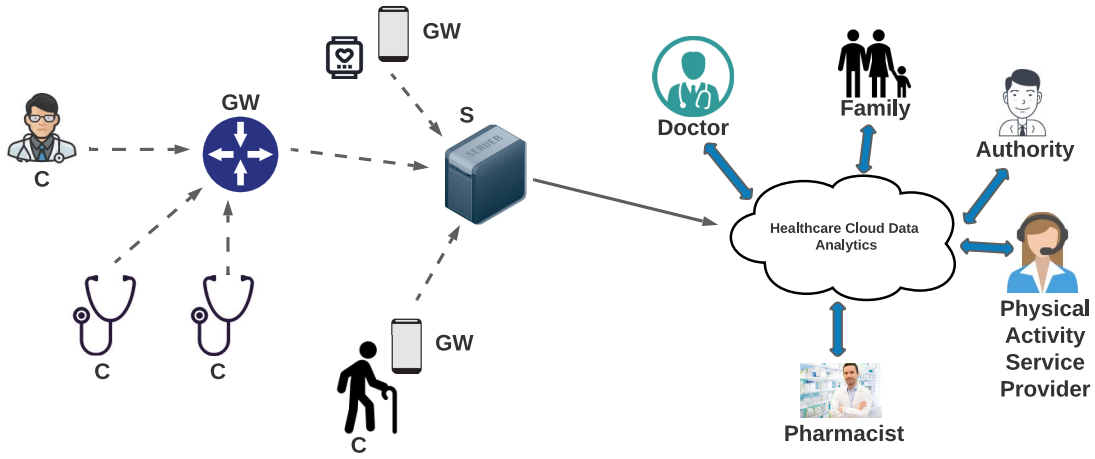

Fig. 1. Network Model of LightIoT.

upon joining the network. However, this protocol was analyzed by [27] and proved that it is vulnerable to impersonation, offline dictionary, and password-guessing attacks. In [28], the authors suggested a lightweight authentication protocol for wearables healthcare IoT devices, which is capable of achieving user anonymity and untraceability by using a dynamic update mechanism. However, this protocol was investigated by [29] and proved that it is prone to de-synchronization and cloning attacks. This scheme [28] is not capable to counter forward secrecy and DoS attacks due to message replacement. Recently some lightweight authentication schemes have been proposed for resource-constrained networks [30], [31], [32]. Contrary to their claims of being lightweight, these schemes involve too many security primitives during hashing that ultimately make them resource-intensive.

III. Network Model and Design of LightIoT

LightIoT consists of three phases: initialization, pairing, and authentication. During the first phase, a remote server generates the system parameters and stores important information about the clients and gateways. The second phase is responsible for registering each client with a trusted server. Finally, during the third phase, the clients and gateways mutually authenticate each other via the server, and a session key is generated for the current session to securely exchange the data [33]. In this section, first we discuss the network model of LightIoT followed by its design. The notations used in each phase of the design are illustrated in Table I.

A. Network Model

In this section, we discuss our proposed network model that is equally applicable for in-home and in-hospital scenarios. In Fig. 1, the sensor-embedded wearables, i.e., clients, are connected to a remote server via the network gateways. For some clients, such as a smartwatch, a smartphone in the patient's pocket acts as a gateway [34]. These gateways, act as intermediate entities to the remote server that is connected to healthcare cloud data analytics for feature extraction, visualization, and decision-making [35].

The network model of Fig. 1 is susceptible to various adversarial attacks that can ultimately lead to loss of the associated invaluable medical data [36]. An adversary may establish secured connections to the server or gateways if its authentication requests are accepted. An adversary may infiltrate the network by seizing the identities of clients and gateways to pose various threats. Moreover, it may clone itself for a large-scale adversarial effect on the overall system. To prevent such threats, we propose a lightweight yet secure and robust privacy-preserved approach for biomedical data. LightIoT is resilient against the following threats.

1) *Replay:* An adversary may replay a stream of previously transmitted messages to the clients or servers.
2) *Forgery:* An adversary may launch a forgery attack on one or more of the network entities. It may seize and manipulate the exchanged messages and impersonate itself to these legitimate entities.
3) *Anonymity and Untraceability:* An adversary may launch this attack by extracting the pseudo-random numbers, and the identities of clients, gateways, and servers from the exchanged messages [37]. In doing so, it may interlink various sessions to maliciously affect these network entities.
4) *De-Synchronization:* An adversary may launch this attack by blocking the exchanged messages among the communicating entities to alter their sequence/ pattern.
5) *Key Compromise:* An adversary may launch this attack by forging or compromising the exchanged session key.

TABLE I
Notations of the LightIoT Design

Notations	Descriptions
C	Client
GW	Gateway
S	Server
ID_C	Identity of C
P_{ID_c}	Pseudo-identity of C
λ_C	Secret key of C
ID_{GW}	Identity of GW
$P_{ID_{GW}}$	Pseudo-identity of GW
λ_{GW}	Secret key of GW
t_{c_1}, t_{c_2}	Time stamps of C for pairing
t_s	Time stamp of S for pairing
r_c	Random Number generated by C for pairing
T_{c_1}, T_{c_2}	Time stamps of C for authentication
T_{gw_1}, T_{gw_2}	Time stamps of GW for authentication
T_s	Time stamp of S for authentication
δT	Legal delay time interval
R_c	Random Number generated by C for authentication
R_{gw}	Random Number generated by GW for authentication
$\mathrm{M}_1, M_2, ..., M_6$	Messages

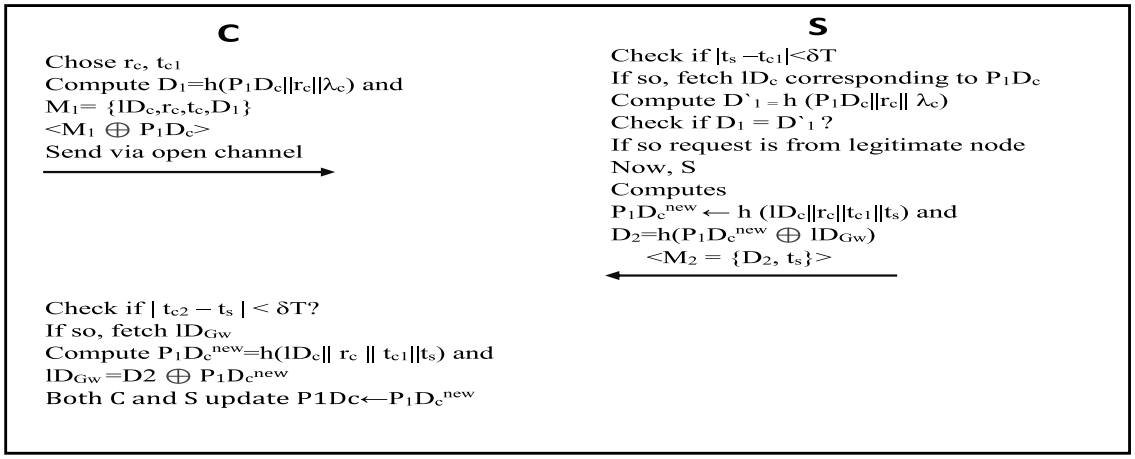

Fig. 2. Pairing Phase.

B. Design of LightIoT

The design of LightIoT consists of three phases: initialization, pairing and authentication. In this section, we discuss these three phases.

1) Initialization: A remote server (*S*) serves the purpose of a trusted third party and generates the systparameters. *S* stores information about each WBAN client (*C*) and each gateway (*GW*). During initialization, *S* performs the following operations:

- It provides and stores information, i.e., λ_C and P_{ID_c} for a given *C* in its database as (λ_C, P_{ID_c}). Each *C* has a tuple ($ID_C, \lambda_C, P_{ID_c}$).
- It provides and stores information, i.e., λ_{GW} and $P_{ID_{GW}}$ for a given *GW* in its database as (λ_{GW}, $P_{ID_{GW}}$). Each *GW* has a tuple (ID_{GW}, λ_{GW}, $P_{ID_{GW}}$) and assumed to be registered and authorized by *S*.

2) Pairing: Each *C* needs to register itself with *S* to initiate communication request in the network. During this phase, the following steps are performed.

- *C* generates a random number r_c, picks its current time stamp t_{c_1} and calculates the hash D_1 by concatenating P_{ID_c}, r_c, and λ_C, as shown in Eq. (1). At this point, a message $M_1 = \{(ID_C, r_c, t_{c_1}, D_1\})$ is created, XOR with P_{ID_c}, i.e., $M_1 \oplus P_{ID_c}$, and the encrypted message is send to *S*.

$$D_1 \leftarrow h(P_{ID_c} \| r_c \| \lambda_C). \tag{1}$$

- Upon receiving M_1, *S* picks up its current timestamp t_s and checks if $|t_s - t_{c_1}| < \delta T$. If the time interval is not within the specified allowable δT, then M_1 is discarded and pairing request fails, otherwise further processing is performed [38]. Once M_1 is validated for time, then *S* uses P_{ID_c} to decrypt it for the retrieval of ID_C. Upon retrieval, *S* checks ID_C in its database. If it is found, then it means that *C* is a registered client. Next *S* checks a tuple (P_{ID_c}, λ_C) in its database, calculates a hash function D_1' and checks if it matches the D_1 received from *C*. If there is a match, it means that the registration/pairing request was received from a legitimate client. At this point, *S* calculates a new pseudo-identity $P_{ID_c}^{new}$ for *C* by generating the hash of ID_C, r_c, t_{c_1}, and t_s, as shown in Eq. (2a). Here, $P_{ID_c}^{new}$ serves as a new pseudo-identity for *C*. Next, *S* generates a hash D_2 by encrypting $P_{ID_c}^{new}$ with ID_{GW}, as shown in Eq. (2b). Finally, *S* creates a message $M_2 = \{D_2, t_s\}$ and broadcasts to *C*.

$$P_{ID_c}^{new} \leftarrow h(ID_C \| r_c \| t_{c_1} \| t_s), \tag{2a}$$

$$D_2 \leftarrow h\big(P_{ID_c}^{new} \oplus ID_{GW}\big). \tag{2b}$$

- Upon receiving M_2, *C* picks up its current timestamp t_{c_2} and checks if $|t_{c_2} - t_s| < \delta T$. If the time interval is not within the specified allowable δT, then M_2 is discarded, otherwise, further processing is performed. After the validation of M_2, *C* calculates its new pseudo-identity $P_{ID_c}^{new}$ by generating the hash of ID_C, r_c, t_{c_1} and t_s, as shown in Eq. (3a). In this case, $P_{ID_c}^{new}$ serves as the new pseudo-identity for *C*. It is worth mentioning that the same pseudo-identity for *C* was earlier generated by *S*. *C* then obtains ID_{GW} from D_2 using Eq. (3b), calculates D_2', and checks whether D_2' matches D_2. If a correct hash function is calculated, then the session request for pairing is validated, and *C* updates its pseudo-identity, i.e., $P_{ID_c}^{new}$ becomes the new P_{ID_c}. The complete procedure of our pairing phase is shown in Fig. 2.

$$P_{ID_c} \leftarrow P_{ID_c}^{new} \leftarrow h(ID_C \| r_c \| t_{c_1} \| t_s), \tag{3a}$$

$$ID_{GW} \leftarrow D_2 \oplus h\big(P_{ID_c}^{new} \| t_s\big). \tag{3b}$$

3) Authentication: For authentication, all the three entities (*C*, *GW*, and *S*) participate. During this process, *C* and *GW* mutually authenticate each other and a session key is generated for further communication between them. The following steps are involved during the authentication phase.

1) *C* generates a random number R_c, picks up its current timestamp T_{c_1}, and calculates a hash C_1 by concatenating ID_C, λ_C, and R_c, as shown in Eq. (4). At this point, a message $M_3 = \{C_1, R_c, T_{c_1}, P_{ID_c}\}$ is created, XOR with ID_{GW}, i.e., $M_3 \oplus ID_{GW}$, and the encrypted message is sent to *GW*, as an authentication request.

$$C_1 \leftarrow h(ID_C \| \lambda_C \| R_c). \tag{4}$$

2) Upon receiving M_3, *GW* picks up its current timestamp T_{gw_1} and checks if $|T_{gw_1} - T_{c_1}| < \delta T$. If the time interval is not within the specified allowable δT, M_3 is discarded, otherwise, further processing is carried out. At this point, *GW* generates a random number R_{gw}, and calculates a hash C_2 by concatenating ID_{GW}, λ_{GW}, and R_{gw}, as shown in Eq. (5). A message $M_4 = \{C_1, C_2, P_{ID_c}, T_{gw_1}\}$ is created, XOR with $P_{ID_{GW}}$, i.e., $M_4 \oplus P_{ID_{GW}}$, and the encrypted message is sent to *S*, as an authentication request.

$$C_2 \leftarrow h\big(ID_{GW} \| \lambda_{GW} \| R_{gw}\big). \tag{5}$$

3) Upon receiving M_4, *S* picks up its current timestamp T_s, and checks if $|T_s - T_{gw_1}| < \delta T$. If the time interval is not within the specified allowable δT, then M_4 is discarded, otherwise, further processing is carried out. Once M_4 is validated for time, then *S* checks for the validity of *C* and *GW* in its database. If it finds the tuples (P_{ID_c}, λ_C) for *C* and ($P_{ID_{GW}}$, λ_{GW}) for *GW* in its database, the nodes were previously paired. *S* recalculates the hash C_1' and checks if it matches the hash C_1 received from *C*. If the same hash was calculated at *S*, *C* is a registered client and further processing can take place. Similarly, *S* recalculates the hash C_2', and checks if it matches the hash C_2 received from *GW*. If there is a match, *GW* is genuine and further processing can take place. In either case, a mismatch signifies that the request is received from an illegitimate gateway and will be ignored.

4) After the validation of *C* and *GW*, *S* calculates a new pseudo-identity P_C^{New} for *C* by generating the hash of ID_C, λ_C, R_c, T_{c_1} and T_s, as shown in Eq. (6). Here, P_C^{New} serves as a new pseudo-identity for *C*, i.e., P_{ID_c}.

$$P_{ID_c} \leftarrow P_C^{New} \leftarrow h(ID_C \| \lambda_C \| R_c \| T_{c_1} \| T_s), \tag{6}$$

S also calculates a new pseudo-identity P_{GW}^{New} for *GW* by generating the hash of ID_{GW}, λ_{GW} R_{gw}, T_{gw_1} and T_s, as shown in Eq. (7). Here, P_{GW}^{New} serves as a new pseudo-identity for *GW*, i.e., $P_{ID_{GW}}$.

$$\begin{aligned} P_{ID_{GW}} &\leftarrow P_{GW}^{New} \\ &\leftarrow h\big(ID_{GW} \| \lambda_{GW} \| R_{gw} \| T_{gw_1} \| T_s\big). \end{aligned} \tag{7}$$

5) Next, *S* generates a series of hash functions and a session key K_S for *GW*, as shown in Eq. (8). K_S contains all the security primitives intended for *GW* because the whole of data exchange between *C* and *S* will transit via *GW*. A hash C_3 is generated by concatenating ID_C, T_{c_1}, and T_s. A hash C_4 is generated by concatenating K_S, C_3, and $P_{ID_{GW}}$. Finally, a hash C_5 is generated by concatenating C_3 and R_c.

$$C_3 \leftarrow h(ID_C \| T_{c_1} \| T_s), \tag{8a}$$
$$K_S \leftarrow h\big(ID_{GW} \| \lambda_{GW} \| R_{gw} \big\| P_{ID_{GW}} \big\| T_s\big), \tag{8b}$$
$$C_4 \leftarrow h\big(K_S \| C_3 \| P_{ID_{GW}}\big), \tag{8c}$$
$$C_5 \leftarrow h(C_3 \| R_c). \tag{8d}$$

S generates $M_5 = \{T_s, C_3, C_4, C_5\}$ and broadcast to *GW*. The generation of different hash functions in Eq. (8) makes M_5 extremely difficult for adversaries to crack. Moreover, these hash functions make it extremely difficult to predict K_S in M_5.

6) Upon receiving M_5, *GW* picks up its current time stamp T_{gw_2} and checks if $|T_s - T_{gw_2}| < \delta T$. If the time interval is not within the specified allowable δT, then M_5 is discarded, otherwise, further processing is carried out. After the validation of M_5, *GW* calculates its new pseudo-identity $P_{ID_{GW}}$ by generating the hash of ID_{GW}, λ_{GW}, R_{gw}, T_{gw_1} and T_s, as shown in Eq. (9a). In this case, $P_{ID_{GW}}$ serves as the new pseudo-identity for *GW*, similar to the one generated by *S*.

$$P_{ID_{GW}} \leftarrow h\big(ID_{GW} \| \lambda_{GW} \| R_{gw} \big\| T_{gw_1} \big\| T_s\big), \tag{9a}$$
$$K_{GW} \leftarrow h\big(P_{ID_c} \| ID_{GW} \| R_c \| R_{gw}\big), \tag{9b}$$
$$C_6 \leftarrow h(K_{GW} \| C_3). \tag{9c}$$

7) Next, a session key K_{GW} is generated by *GW* using a hash function to concatenate P_{ID_c}, ID_{GW}, R_c and R_{gw}, as shown in Eq. (9b). Finally, a hash C_6 is calculated by concatenating K_{GW} with C_3, as shown in Eq. (9c). At this point, *GW* creates a message $M_6 = \{C_5, C_6, T_s, T_{gw_2}\}$, XOR with $P_{ID_{GW}}$, i.e., $M_6 \oplus P_{ID_{GW}}$, and the encrypted message is broadcast to *C*.

8) Upon receiving M_6, *C* picks up its current time stamp T_{c_2} and checks if $|T_{c_2} - T_{gw_2}| < \delta T$. If the time interval is not within the specified allowable δT, then M_6 is discarded, otherwise, further processing is carried out. After the validation of M_6, *C* calculates its new pseudo-identity $P_{ID_c}^{New}$ by generating the hash of ID_C, λ_C, R_c, T_{c_1} and T_s, as shown in Eq. (10a). In this case, $P_{ID_c}^{New}$ serves as a new pseudo-identity for *C*. It is worth mentioning that the same pseudo-identity for *C* was generated earlier by *S*.

$$P_{ID_c}^{New} \leftarrow h(ID_C \| \lambda_C \| R_c \| T_{c_1} \| T_s), \tag{10a}$$
$$K_C \leftarrow h\Big(P_{ID_{gw}} \| ID_C \| R_c \| R_{gw}\Big). \tag{10b}$$

It then recalculates the hash C_5. If $P_{ID_c}^{New}$ holds, i.e., $P_{ID_c}^{New} == h(\lambda_C \| C_5)$, the identity of *GW* is successfully verified. At this point, *C* generates a session key K_C based on a hash function and concatenating $\mathrm{P}_{ID_{gw}}$, ID_C, R_c and R_{gw}, as shown in Eq. (10b). To check the validity of K_C, *C* recalculates C_6, i.e., C_6', which is calculated as $h(P_{ID_c} \| ID_{GW} \| R_c \| R_{gw} \| C_3)$. It can also be calculated as $h(\mathrm{K}_{GW} \| C_3$. If C_6' matches the C_6 received from *GW*, i.e., $C_6 == h(K_C \| T_{c_1})$, K_C is valid.

Going through this process successfully, *C* and *GW* have mutually authenticated each other and are authorized to transmit the healthcare data to *S*. The overall authentication process is shown in Fig. 3.

IV. Security Analysis

To check the validity of the LightIoT design, informal analysis is conducted, which shows that LightIoT is resilient against a number of adversarial attacks. In LightIoT, IDs and pseudo-random numbers are 128 bit, and timestamps are 32 bit in length. We used the SHA3-256 hash function to generate a hash digest of 256-bit length.

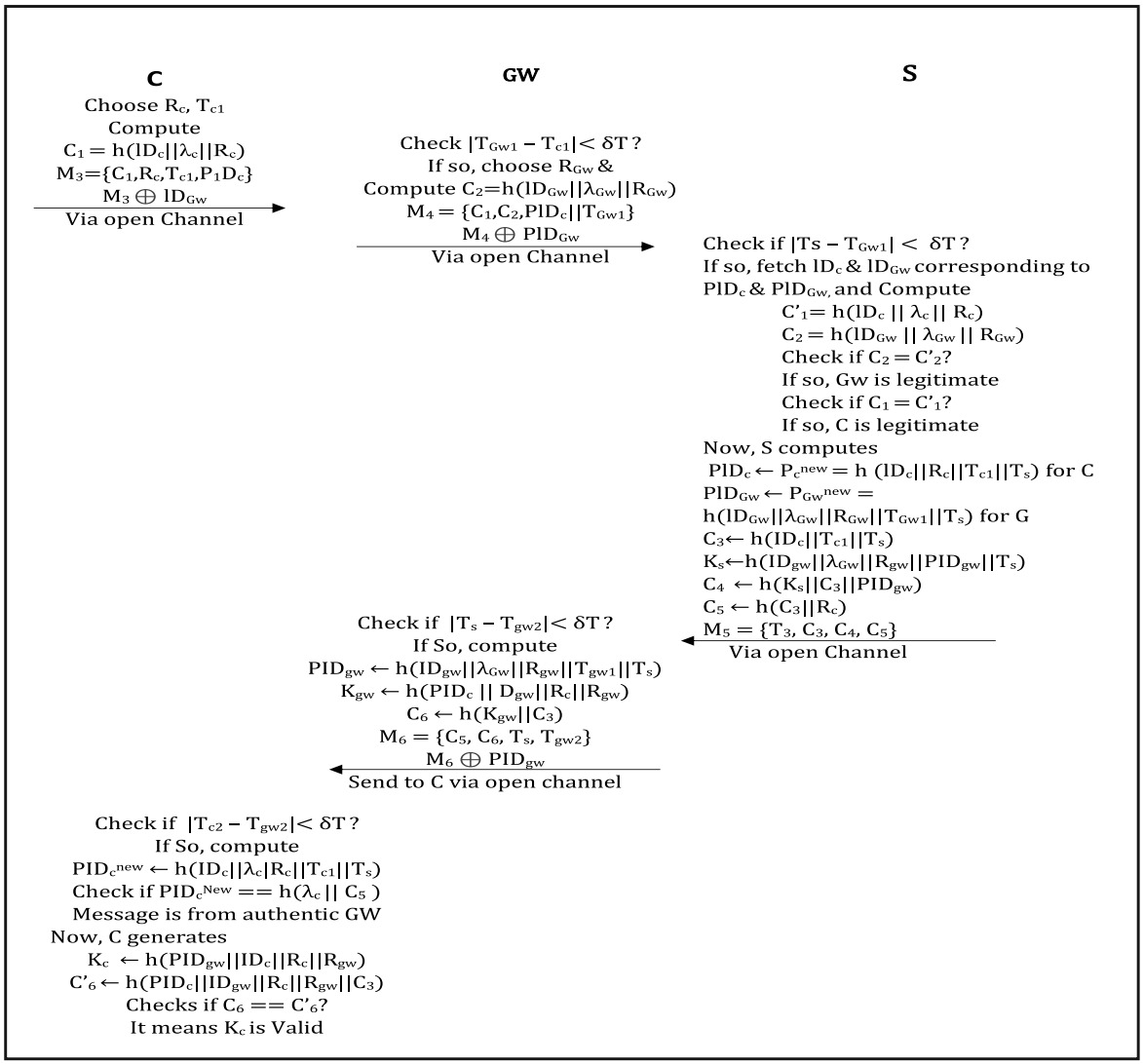

Fig. 3. Authentication Phase.

A. Replay Attack

A timestamp is used in each message by *C*, *GW* and *S* to protect the content of these messages from replay attack. Therefore, the validity of each message can be checked. If a message is not within the legal time delay, i.e., δt, it will be discarded. Similar to LightIoT, the existing schemes are resilient to replay attacks.

B. Forgery Attack

An adversary can launch a forgery attack on all the network entities (clients, servers, and gateways). We discuss all the possible scenarios below.

C. Forgery Attack on Server

If an adversary launches a forgery attack on *S*, it will need to capture and manipulate M_1 and M_4. For M_4, the adversary needs to provide a valid C_1, C_2 and P_{ID_c} to *S*. Due to the encrypted M_4 ($M_4 \oplus P_{ID_{GW}}$), the adversary will initially require $P_{ID_{GW}}$ to extract the content (C_1, C_2 and P_{ID_c}). Even if it acquires $P_{ID_{GW}}$, it will require λ_C to crack C_1 and ID_{GW} to crack C_2. An adversary may also try to eavesdrop and manipulate M_1 to launch a forgery attack on *S*. However, due to the encrypted $M_1 \oplus P_{ID_c}$, the adversary will require P_{ID_c} to crack this message. Even if it cracks it, the adversary would still need λ_C and r_c to regenerate a valid D_1. The use of hash functions, pseudo-random numbers and secret keys makes it extremely difficult to launch forgery attacks on *S*.

D. Forgery Attack on Client

To launch a forgery attack on *C*, an adversary will need to capture and manipulate M_2 and M_6. To forge M_2, a valid D_2 needs to be presented to *C*. To do so, the adversary would require P_{ID_c} of *C* and ID_{GW} of *GW*. For M_6, $P_{ID_{GW}}$ is required to decrypt it. Even if an adversary decrypts M_6, the former will require to crack C_5 and C_6 to launch a forgery attack on *C*. In LightIoT, C_5 and C_6 are the most resilient and robust hashes as they are composed of secret keys and pseudo-random numbers. The keys themselves are hashed making it highly unlikely for an adversary to crack them even with the most sophisticated hardware and software platforms. For a

TABLE II
RESILIENCE AGAINST VARIOUS ATTACKS

Attacks	[27]	[39]	[40]	[41]	*LightIoT*
Replay	No	Yes	Yes	Yes	Yes
Resistance to Server Forgery	No	Yes	No	No	italic
Resistance to Client Forgery	Yes	No	No	Yes	Yes
Resistance to Gateway Forgery	Yes	No	No	Yes	Yes
Untraceability	No	Yes	No	No	Yes
Mutual Authentication	Yes	Yes	Yes	Yes	Yes
Key Agreement	Yes	Yes	Yes	Yes	Yes
De-Synchronization	No	No	No	No	Yes
Availability	No	No	No	No	Yes

TABLE III
COMPUTATION OVERHEAD COMPARISON

Schemes	Client (T_C)	Gateway (T_G)	Server (T_S)	Total Cost
Amin et. al [27]	$5T_h$+$3T_{XOR}$	$12T_h$+$7T_{XOR}$	$15T_h$+$7T_{XOR}$	$32T_h$+$17T_{XOR}$
Li et. al [39]	$13T_h$+$7T_{XOR}$	-	$4T_h$+$12T_{XOR}$	$17T_h$+$19T_{XOR}$
Jan et. al [40]	$6T_h$+$1T_{XOR}$	$7T_h$+$1T_{XOR}$	$10T_h$+$2T_{XOR}$	$23T_h$+$4T_{XOR}$
Gope et. al [41]	$3T_h$+$1T_{XOR}$	$14T_h$+$7T_{XOR}$	$9T_h$+$4T_{XOR}$	$26T_h$+$12T_{XOR}$
LightIoT	$5T_h$+$2T_{XOR}$	$4T_h$+$2T_{XOR}$	$8T_h$+$1T_{XOR}$	$17T_h$+$5T_{XOR}$

successful forgery attack on *C*, an adversary needs to know these hashes, keys, and pseudo-random numbers.

E. Forgery Attack on Gateway

To launch a forgery attack on *GW*, an adversary needs to capture and manipulate M_3 and M_5. To forge M_3, an adversary would initially require a valid ID_{GW} to crack it. Even if it cracks it, a valid C_1 and P_{ID_c} need to be presented to *GW*. For M_5, a number of hash functions (C_3, C_4, and C_5) are required. The complex combination of these hash functions in M_5 makes the latter extremely difficult for adversaries to decrypt. Moreover, these hash functions make it extremely difficult to predict K_S in M_5.

F. Untraceability of Client and Gateway

Both *C* and *GW* get a new pseudo-identity in every new session and these pseudo-identities are always different from previous ones due to their unique timestamps. Therefore, *C* and *GW* are untraceable because their real/actual identities are never disclosed in the exchanged messages.

G. Mutual Authentication and Key Agreement

Mutual authentication is guaranteed because none of the entities of any session can be forged. Every session is managed under a unique session key to encrypt the information exchanged during a session.

H. De-Synchronization Attack

If M_2 is not received by *C* during the pairing phase due to network delays or blockage by an adversary, then *GW* can continue its operations according to the last updated values for next pairing. If M_5 is not received by *GW* in the authentication phase due to network delays or blockage by an adversary, *GW* can also continue its operations according to the last updated values for next session. If M_6 is not received by *C* in the authentication phase due to network delays or blockage by an adversary, *GW* can use the latest P_{ID_c} to complete the process.

I. Availability

The majority of existing schemes use long-term keys at the beginning and maintain them for pairing and authentication. However, in LightIoT, there are no long-term keys for *C* and *GW*. The pairing phase is mandatory for every new *C* and *GW*, since they are not supposed to have any information about each other before their initial interaction.

V. PERFORMANCE EVALUATION

In this section, we evaluate and validate our proposed approach through experimental results in a simulation environment. In addition, we used NS-2 as a simulation tool to implement and validate different protocols. Initially, the network infrastructure is developed through the random deployment of sensor devices, gateways, and remote servers. To evaluate the efficiency of our scheme, we increased the number of sensor devices, gateways and remote servers in the deployed area followed by an increase in the network traffic. To highlight its efficiency, we compare LightIoT against existing approaches in terms of computational and communication overhead, individual device lifetime statistics followed by network lifespan, and latency.

A. Computation Overhead

In Table III, we provide a summary of the computational overhead comparison against the evaluated schemes. In this table, T_h and T_{XOR} refer to the computational time needed to perform the hash and XOR operations at *C*, *GW* and *S*, respectively. In [39], the gateways do not perform any computation. Instead, they forward the messages directly to a hub, i.e., a server. As a result, the computational overhead at the gateway is left blank. Among the existing schemes, [27] incurs relatively higher computational overhead in comparison to [39], [40] and [41]. The comparison in this table highlights the effectiveness of LightIoT as it generates highly secure and composite hash functions with the least computational overhead. More importantly, the relatively smaller computational

TABLE IV
COMMUNICATION OVERHEAD COMPARISON

Schemes	Number of Messages	Number of Bits
Amin et. al [27]	6	4096
Li et. al [39]	4	4672
Jan et. al [40]	5	3808
Gope et. al [41]	4	3184
LightIoT	6	3424

overhead is incurred at resource-constrained wearables, which makes LightIoT a feasible option for deployment in large-scale healthcare applications.

B. Communication Overhead

In Table IV, we show the communication overhead incurred by the network entities while exchanging the messages among themselves. In LightIoT, the encrypted message ($M_1 \oplus P_{ID_c}$) is transmitted by *C*. M_1 has a length of 544 bits. The message M_2 is transmitted by *S* as $M_2 = \{D_2, t_s\}$ and the communication overhead incurred is 288 bits. The message M_3 is transmitted by *C* as $M_3 = \{C_1, R_c, T_{c_1}, P_{ID_c}\}$ and has a length of 544 bits. The encrypted M_4 ($M_4 \oplus P_{ID_{GW}}$) incurs a communication overhead of 672 bit on *GW*. The most sophisticated and complex $M_5 = \{T_s, C_3, C_4, C_5\}$ has multiple hash functions and incurs a communication overhead of 800 bits on *S*. Finally, the encrypted M_6 ($M_6 \oplus P_{ID_{GW}}$) incurs a communication overhead of 576 bits on *GW*. The total communication overhead incurred by network entities in our proposed approach is 3424 bits. In comparison to the existing schemes of [27], [39] and [40], LightIoT has a lower communication overhead, but it has relatively higher overhead compared to [41]. However, this comparison does not signify that [41] is superior to LightIoT in terms of communication overhead. In any scheme for resource-constrained wearable devices, the overhead imposed on wearables themselves is the most important factor. To this end, LightIoT incurs a communication overhead of 1088 bits on a wearable device compared to 1340 bits of [41].

C. Network Lifespan Analysis Against Field-Proven Schemes

The performance reliability of any authentication scheme is dependent on the network lifetime. Therefore, network lifespan needs special attention while designing a new authentication scheme for resource-limited networks. Keeping in mind the reliability factor of an authentication scheme, we evaluate LightIoT in terms of the lifetime of individual sensor devices and the whole network lifespan in comparison to existing schemes. The simple authentication with accurate results of LightIoT is effective in terms of network lifetime because the legitimate devices need only two messages to verify the legitimacy of communicating devices. Besides that, the simple authentication process of LightIoT with the least computation and communication costs minimizes the energy consumption during handshake among the participating devices. During simulations, LightIoT showed superior results of individual device lifetime and network lifespan, due to its light computation and storage overhead on wearable devices. Figures 4 and 5 present the results of LightIoT along with existing state-of-the-art schemes for individual device lifetime and network lifetime.

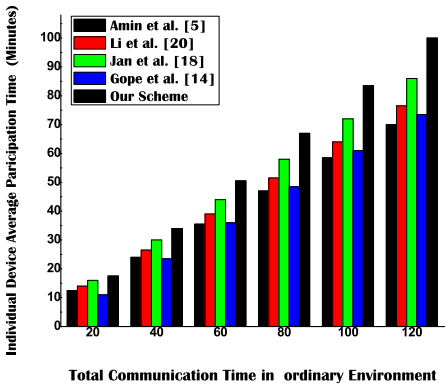

Fig. 4. Individual device lifespan results.

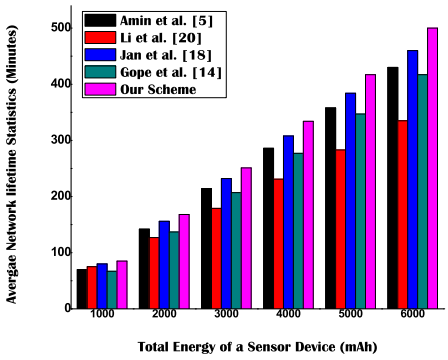

Fig. 5. Network lifespan results.

D. End-to-End Delay Analysis

In delay-sensitive applications of IoT networks, the performance of any protocol is dependent on latency, since additional delay in the deployed network disrupts its effectiveness. To this end, we have evaluated the latency of LightIoT. The simple authentication process and lightweight nature of LightIoT ensure its efficiency, while the time consistency observed during the communication process was noteworthy. Furthermore, we have increased network traffic with the addition of new devices in the simulation environment. However, during the communication process, the transmission and reception of messages showed a constant time frame throughout the entire process. Our results presented in Figure 6 demonstrate that LightIoT incurs significantly lower latency in comparison to state-of-the-art schemes.

VI. CONCLUSION

In this paper, we proposed LightIoT, a lightweight yet highly secure scheme for green communications, focusing on biomedical data in IoT-enabled health informatics. LightIoT has three phases that facilitate the resource-constrained wearable devices to initiate simple registration and authentication procedures with a mobile gateway and a remote server. The registration requires two messages to register the wearables with a remote server and the authentication relies on four such

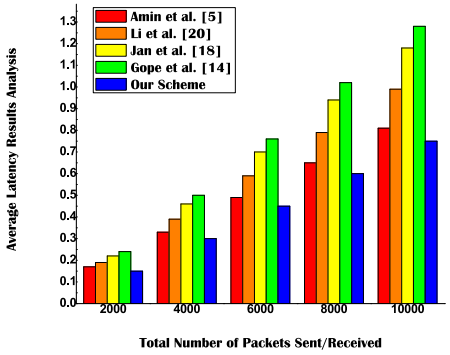

Fig. 6. Latency results.

messages to establish a secure end-to-end session for data exchange among the communicating entities. LightIoT uses lightweight hash functions and XOR operations to accomplish these phases and is highly efficient for the immediate delivery of time-critical and delay-sensitive data. The experimental results verify the efficiency of LightIoT, as it is highly resilient against a number of attack scenarios and, at the same time, incurs low computational and communication overheads. The limitation of LightIoT is the validation of mobile wearable devices in an operational environment, because the one step registration process is performed in the offline phase.

REFERENCES

[1] M. A. Jan *et al.*, "A lightweight mutual authentication and privacy-preservation scheme for intelligent wearable devices in industrial-CPS," *IEEE Trans. Ind. Informat.*, early access, Dec. 10, 2020, doi: 10.1109/TII.2020.3043802.

[2] M. A. U. Rehman, R. Ullah, B.-S. Kim, B. Nour, and S. Mastorakis, "CCIC-WSN: An architecture for single channel cluster-based information-centric wireless sensor networks," *IEEE Internet Things J.*, vol. 8, no. 95, pp. 7661–7675, May 2021.

[3] M. A. Jan *et al.*, "Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions," *J. Netw. Comput. Appl.*, vol. 175, Feb. 2021, Art. no. 102918.

[4] S. Mastorakis, A. Mtibaa, J. Lee, and S. Misra, "ICedge: When edge computing meets information-centric networking," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4203–4217, May 2020.

[5] F. Al-Turjman and S. Alturjman, "Context-sensitive access in Industrial Internet of Things (IIOT) healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2736–2744, Jun. 2018.

[6] M. A. Jan *et al.*, "An AI-enabled lightweight data fusion and load optimization approach for Internet of Things," *Future Gener. Comput. Syst.*, vol. 122, pp. 40–51, Sep. 2021.

[7] W. Fitbit, *Find a Fit for Everybody*. Accessed: Aug. 27, 2019. [Online]. Available: https://www.fitbit.com/whyfitbit

[8] F. Bader and S. Jagtap, *Internet of Things Linked Wearable Devices for Managing Food Safety in the Healthcare Sector*. Cambridge, MA, USA: Academic Press, 2019.

[9] S. Banerjee, T. Hemphill, and P. Longstreet, "Wearable devices and healthcare: Data sharing and privacy," *Inf. Soc.*, vol. 34, no. 1, pp. 49–57, 2018.

[10] S. Mastorakis, X. Zhong, P.-C. Huang, and R. Tourani, "DLWIOT: Deep learning-based watermarking for authorized iot onboarding," in *Proc. IEEE 18th Annu. Consum. Commun. Netw. Conf. (CCNC)*, 2021, pp. 1–7.

[11] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, Jan. 2017.

[12] M. A. Jan, F. Khan, M. Alam, and M. Usman, "A payload-based mutual authentication scheme for Internet of Things," *Future Gener. Comput. Syst.*, vol. 92, pp. 1028–1039, Mar. 2019.

[13] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2590–2601, Dec. 2017.

[14] W. Yao *et al.*, "A secured and efficient communication scheme for decentralized cognitive radio-based Internet of Vehicles," *IEEE Access*, vol. 7, pp. 160889–160900, 2019.

[15] F. Khan, M. A. Jan, A. U. Rehman, S. Mastorakis, M. Alazab, and P. Watters, "A secured and intelligent communication scheme for IIOT-enabled pervasive edge computing," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 5128–5137, Jul. 2021.

[16] S. Mastorakis, T. Li, and L. Zhang, "DAPES: Named Data for Off-the-Grid File Sharing with Peer-to-Peer Interactions," in *Proc. 40th IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2020, pp. 710–720.

[17] K. H. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Proc. IEEE Int. Conf. Sensor Netw. Ubiquitous Trustworthy Comput. (SUTC)*, vol. 1, 2006, pp. 244–251.

[18] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wirelessbody area networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332–342, Feb. 2014.

[19] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K.-K. R. Choo, and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 4, pp. 1310–1322, Jul. 2018.

[20] F. P. Diez, D. S. Touceda, J. M. S. Camara, and S. Zeadally, "Toward self-authenticable wearable devices," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 36–43, Feb. 2015.

[21] F. Wu, X. Li, L. Xu, S. Kumari, M. Karuppiah, and J. Shen, "A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server," *Comput. Elect. Eng.*, vol. 63, pp. 168–181, Oct. 2017.

[22] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 357–366, Jan. 2016.

[23] A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, and X. Huang, "Provably secure user authentication and key agreement scheme for wireless sensor networks," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3670–3687, 2016.

[24] J. He, Z. Yang, J. Zhang, W. Liu, and C. Liu, "On the security of a provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 1, pp. 1–11, 2018.

[25] S. F. Aghili, H. Mala, P. Kaliyar, and M. Conti, "SecLAP: Secure and lightweight RFID authentication protocol for medical IoT," *Future Gener. Comput. Syst.*, vol. 101, pp. 621–634, Dec. 2019.

[26] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Netw.*, vol. 20, pp. 96–112, Sep. 2014.

[27] R. Amin and G. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Netw.*, vol. 36, pp. 58–80, Jan. 2016.

[28] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Gener. Comput. Syst.*, vol. 80, pp. 483–495, Mar. 2018.

[29] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Comput. Elect. Eng.*, vol. 63, pp. 182–195, Oct. 2017.

[30] R. Ali, A. K. Pal, S. Kumari, M. Karuppiah, and M. Conti, "A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring," *Future Gener. Comput. Syst.*, vol. 84, pp. 200–215, Jul. 2018.

[31] 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 Trans. Ind. Electron.*, vol. 14, no. 8, pp. 3599–3609, Aug. 2018.

[32] F. Wu *et al.*, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Gener. Comput. Syst.*, vol. 82, pp. 727–737, May 2018.

[33] S. Mastorakis, "Peer-to-peer data sharing in named data networking," Ph.D. dissertation, UCLA, Oakland, CA, USA, 2019.

[34] G. Yang, M. A. Jan, V. G. Menon, P. Shynu, M. M. Aimal, and M. D. Alshehri, "A centralized cluster-based hierarchical approach for green communication in a smart healthcare system," *IEEE Access*, vol. 8, pp. 101464–101475, 2020.

[35] M. Abbasi, H. Rezaei, V. G. Menon, L. Qi, and M. R. Khosravi, "Enhancing the performance of flow classification in SDN-based intelligent vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, early access, Aug. 13, 2020, doi: 10.1109/TITS.2020.3014044.
[36] H. Zhang, M. Babar, M. U. Tariq, M. A. Jan, V. G. Menon, and X. Li, "SafeCity: Toward safe and secured data management design for iot-enabled smart city planning," *IEEE Access*, vol. 8, pp. 145256–145267, 2020.
[37] T. Li, Z. Kong, S. Mastorakis, and L. Zhang, "Distributed dataset synchronization in disruptive networks," in *Proc. IEEE 16th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, 2019, pp. 428–437.
[38] M. Abbasi, A. Najafi, M. Rafiee, M. R. Khosravi, V. G. Menon, and G. Muhammad, "Efficient flow processing in 5g-envisioned SDN-based Internet of Vehicles using GPUs," *IEEE Trans. Intell. Transp. Syst.*, early access, Dec. 7, 2020, doi: 10.1109/TITS.2020.3038250.
[39] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Comput. Netw.*, vol. 129, pp. 429–443, Dec. 2017.
[40] M. A. Jan, M. Usman, X. He, and A. U. Rehman, "SAMS: A seamless and authorized multimedia streaming framework for WMSN-based IoMT," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1576–1583, Apr. 2019.
[41] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 63, no. 11, pp. 7124–7132, Nov. 2016.

Mian Ahmad Jan (Senior Member, IEEE) received the Ph.D. degree in computer systems from the University of Technology Sydney (UTS), Australia, in 2016. He is an Assistant Professor with the Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan. His research interests include energy efficient and secured communication in wireless sensor networks, Internet of Things, and edge computing. His research has been published in prestigious IEEE transactions and core-ranked conferences. He was the recipient of various prestigious scholarships during his Ph.D. studies. He was the recipient of International Research Scholarship, UTS, and Commonwealth Scientific Industrial Research Organization scholarships. He has been a Guest Editor of numerous special issues in various prestigious journals, such as IEEE TRANSACTIONS ON INDUSTRIAL INFORMATION, *Neural Networks and Applications* (Springer), and *Future Generation Computer Systems* (Elsevier).

Fazlullah Khan (Senior Member, IEEE) is an Assistant professor of Computer Science with Abdul Wali Khan University Mardan, Pakistan. His research interests are intelligent and robust protocol designs, security and privacy of wireless communication systems, Internet of Things, machine learning, and artificial intelligence. He has been involved in latest developments in the field of Internet of Vehicles security and privacy issues, software-defined networks, fog computing, and big data analytics. He has published his research work in top-notch journals and conferences. His research has been published in IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE INTERNET OF THINGS, IEEE ACCESS, *Computer Networks* (Elsevier), *Future Generations Computer Systems* (Elsevier), *Journal of Network and Computer Applications* (Elsevier), *Computers and Electrical Engineering* (Elsevier), and *Mobile Networks and Applications* (Springer). He was the recipient of various prestigious scholarships during his Ph.D. studies and has been awarded the Best Researcher Award for the year 2017.

Spyridon Mastorakis (Member, IEEE) received the 5-year Diploma (equivalent to M.Eng.) degree in electrical and computer engineering from the National Technical University of Athens in 2014, and the M.S. and Ph.D. degrees in computer science from the University of California at Los Angeles in 2017 and 2019, respectively. He is an Assistant Professor of Computer Science with the University of Nebraska at Omaha. His research interests include network systems and protocols, Internet architectures, IoT and edge computing, and security.

Muhammad Adil (Graduate Student Member, IEEE) received the Associate Engineering degree in electronics, the B.S. degree in computer science, and the M.S. (CS) degree with specialization in computer networks from the Virtual University of Pakistan, Lahore, in 2016 and 2019, respectively, where he is currently pursuing the Ph.D. degree. He has CCNA and CCNP certification. His research area includes different routing protocols, security, and load balancing in WSN and IoT networks. He is also interested in dynamic wireless charging of electric vehicles connected in network topological infrastructure with machine learning techniques. He has many publications in prestigious journals, such as IEEE INTERNET OF THINGS, IEEE ACCESS, *Computer Networks* (Elsevier), *Sensors* (MDPI), and *CMC-Computers, Materials & Continua*. He is an Honorary Member of London Journals (Press London Journal of Research in Computer Science and Technology (LJRCST)) and European Alliance for Innovation. He is reviewing for prestigious journals, such as IEEE ACCESS, IEEE SENSORS, IEEE SYSTEMS, IEEE INTERNET OF THINGS, *Sensors* (MDPI), and *Computer Networks* (Elsevier).

Aamir Akbar (Member, IEEE) received the M.Sc. degree from Oxford Brooks University, U.K., in 2012, and the Ph.D. degree in computer science from Aston University, U.K., in 2019. He is currently a Lecturer with the Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan. His research interests include, but not limited to, AI techniques for IoT, SDN, and energy-efficient fog/edge computing. His work leverages multiobjective optimization, evolutionary computation, self-adaptivity, and self-awareness to tackle problems. He has published his work in prestigious IEEE journals and transactions.

Nicholas Stergiou is the Distinguished Community Research Chair of Biomechanics and the Professor and the Director of the Biomechanics Research Building and the Center for Research in Human Movement Variability with the University of Nebraska at Omaha. He was also appointed as the Assistant Dean and the Director of the Division of Biomechanics and Research Development. He is the Founding Chair of the first ever academic Department of Biomechanics that graduates students with a B.S. in Biomechanics. His research focuses on understanding variability inherent in human movement and he is an international authority in the study of Nonlinear Dynamics. He has published more than 200 peer-reviewed papers and have been inducted to the National Academy of Kinesiology. He is a Fellow of the American Institute for Medical and Biological Engineering and the American Society of Biomechanics. He is currently serving as the President of the American Society of Biomechanics.