Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-Based Healthcare

Mehedi Masud, *Senior Member, IEEE*, Gurjot Singh Gaba, *Member, IEEE*, Karanjeet Choudhary, *Member, IEEE*, M. Shamim Hossain, *Senior Member, IEEE*, Mohammed F. Alhamid, *Member, IEEE*, and Ghulam Muhammad, *Senior Member, IEEE*

***Abstract*—Internet of Things (IoT) produces massive heterogeneous data from various applications, including digital health, smart hospitals, automated pathology labs, and so forth. IoT sensor nodes are integrated with the medical equipment to enable the health workers to monitor the patients' health condition and appliances in real time. However, due to security vulnerabilities, an unauthorized user can access health-related information or control the IoT nodes attached to the patient's body resulting in unprecedented outcomes. Due to wireless channels as a medium of communication, IoT poses several threats such as a denial of service attack, man-in-the-middle attack, and modification attack to the IoT networks' security and privacy. The proposed research presents a lightweight and anonymity-preserving user authentication protocol to counter these security threats. The given scheme establishes a secure session for the legitimate user and prohibits unauthorized users from gaining access to the IoT sensor nodes. The proposed protocol uses only lightweight cryptography primitives (hash) to alleviate the node's tiny processor burden. The proposed protocol is efficient and superior because it has low computational and communication costs than conventional protocols. The proposed scheme uses password protection to let only the legitimate user access the IoT sensor nodes to obtain the patient's real-time health report.**

***Index Terms*—COVID-19, digital technology, healthcare, Internet of Things (IoT), key agreement, user authentication.**

I. Introduction

THE Internet of Things (IoT) and digital technology applications are opening up enormous considerable insight into secure data analytics and providing efficient, high-quality health care. The IoT in healthcare defines the communication between medical appliances and users via Internet [1]. IoT empowers the healthcare institutions with new abilities and prospects for business modernization; however, it encounters new obstacles and security threats [2]. IoT is the backbone of the digital healthcare ecosystem. This ecosystem comprises patients and healthcare professionals, clinical devices and robots, smart equipment, and limitless wireless sensors—all these can share sensitive data.

In the last few years, the healthcare industry has witnessed significant growth in the wireless medical sensor networks (WMSNs) for IoT. The sensors in WMSN are an essential component for the healthcare applications that allow a better quality of patient care without compromising the comfort, and health [3], [4]. Connecting body sensor networks to the Internet has also improved patients' monitoring in real time [5]. The monitoring system's primary services are observing key health measurements like the ECG pattern, blood pressure, pulse rate, and respiration rate. As small wearable sensors have come into the picture, combining them with wireless communication technologies has made monitoring even more effective. The advantages of wireless sensor networks include easy access to the patient's medical records and patient mobility, which is highly beneficial. Like any other wireless network, WMSNs are at high risk from eavesdropping, tampering, and impersonation attacks. The information exchanged in the healthcare applications is critical; a little malicious activity by an adversary could endanger the patient's life. The security of the data transmitted through open public channels is the main issue that needs to be addressed [6].

The recent COVID-19 pandemic [7], [8] has uplifted the functional paradigm of the hospitals. Telemedicine and monitoring of patients are remotely carried out while ensuring confidentiality, anonymity, etc. The IoT-enabled sensor nodes used in WMSN have low memory, less battery power, reduced bandwidth, and lower computation abilities [9]. The market for wireless LAN technologies is rapidly growing as they have enabled seamless real-time monitoring of the patients through integration and miniaturization of physical sensors and micro-fabrication.

This article is organized as follows: Section II discusses the related work. Section III demonstrates the system model, the adversary model, and the security goals. This article unfolds the assumptions, the mutual authentication process, and the key agreement phase in Section IV. Section V covers

Manuscript received January 27, 2021; revised March 12, 2021 and April 8, 2021; accepted May 3, 2021. Date of publication May 14, 2021; date of current version February 4, 2022. This work was supported by the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia, through Research Group Project no RGP-228. *(Corresponding author: M. Shamim Hossain)*

Mehedi Masud is with the Department of Computer Science, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia (e-mail: mmasud@tu.edu.sa).

Gurjot Singh Gaba and Karanjeet Choudhary are with the School of Electronics and Electrical Engineering, Lovely Professional University, Phagwara 144411, India (e-mail: gurjot.17023@lpu.co.in; karanchoudhary 8399@gmail.com).

M. Shamim Hossain and Mohammed F. Alhamid are with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia (e-mail: mshossain@ksu.edu.sa; mohalhamid@ksu.edu.sa).

Ghulam Muhammad is with the Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia (e-mail: ghulam@ksu.edu.sa).

Digital Object Identifier 10.1109/JIOT.2021.3080461

formal and informal security analysis, and Section VI presents performance and comparative analysis. This article concludes in Section VII and highlights the future scope.

II. Related Study

Chen *et al.* [10] suggested a scheme designed for telecare medicine information systems (TMISs) that performed dynamic ID-based authentication to preserve the anonymity of the user. However, Cao and Zhai [11] discovered certain disadvantages of the scheme, like being prone to the dictionary attack. The authentication protocol for TMIS by Wu *et al.* [12] is also prone to masquerade attacks [13]. Debiao *et al.* [13] devised a new authentication scheme for preventing the identified attacks. Later, Wei *et al.* [14] proved that the mechanism demonstrated by Debiao *et al.* [13] is also unsafe against the brute force attack of the password.

Challa *et al.* [15] presented a scheme relied on an ECC-based user authentication protocol; however, Jia *et al.* [16] found the scheme [15] unsafe against impersonation attacks. Moreover, the computation and communication cost of [15] is also huge. Zhou *et al.* [17] proposed a scheme that depends on IoT-based cloud architectures' authentication. However; the approach is vulnerable against privileged-insider attack, MITM, replay, and impersonation attacks [18].

Farash *et al.* [19] presented a user authentication and key establishment protocol for diverse WSN and IoT networks. However, Amin *et al.* [20] discovered various drawbacks in this protocol and identified vulnerability against user impersonation and offline password guessing attacks. Meanwhile, Sharma and Kalra [21] proposed a lightweight user authentication protocol; however, Canetti and Krawczyk [22] proved the approach presented in [21] as insecure against privileged inside attack. Turkanović *et al.* [23] proposed another new scheme for user authentication and key establishment. This scheme was found vulnerable against some attacks, like offline password guessing, user impersonation, and sensor node impersonation attacks [24]. Wazid *et al.* [25] presented a lightweight authentication scheme with key management suitable for IoT applications. This scheme uses a one-way cryptographic hash function and bitwise XOR to provide a lightweight and secure communication.

The relevant schemes discussed in literature review are summarized in Table I. It is evident from Table I that traditional schemes are prone to multiple attacks, such as impersonation, MITM, and replay; most of these schemes do not address the security's untraceability and anonymity concerns. Consequently, inadequate security and expensive characteristics of existing schemes make them unsuitable for resource-constrained applications of IoT-based digital health.

TABLE I
State of the Art: Threats and Complexities

S	T	NASP	CTC	CMC	EC	FA	Y
[15]	2	I	L	M	H	A, B	2017
[17]	1, 2, 3, 4	II	H	H	M	P	2019
[19]	1, 2, 5	III	H	M	M	A, B	2016
[21]	1, 5	III	M	H	L	A	2019
[23]	1, 2, 5	I	M	M	L	*	2014
[25]	2	III	H	L	M	A	2019

Acronyms: *S*: Scheme, *T*: Threats, *NASP*: Non-accomplished security properties, *CTC*: Computation cost, *CMC*: Communication cost, *EC*: Execution cost, *FA*: Formal analysis, *Y*: Year, *1*: Privileged insider, *2*: Impersonation, *3*: Replay, *4*: Man-in-the-middle, *5*: Offline password guessing, *I*: Untraceability, *II*: Mutual authentication, III: *Anonymity*, (*): Not performed

A. Motivation

COVID-19 pandemic has revolutionized the working process of frontline workers, especially health workers. Instead of in-person patient monitoring and record maintaining, IoT-enabled telemedicine practices, and digital registers have made their inception. However, due to rapid evolution, the IT administrators did not get ample time to review the security vulnerabilities' deployed in IoT networks. Also, IoT networks are more susceptible to cyber-attacks due to the use of vulnerable wireless mediums for communication, lack of robust security protocols for the resource-constrained environment, and inadequate cyber intelligence amongst the medical fraternity. The cyber threats to these networks can damage hospital property or endanger the lives of the patients. Therefore, IoT networks' security and privacy have the utmost importance. The administrator registers doctors and sensor nodes to ensure security. Doctor (user) and IoT sensor node mutually verify each other before initiating every new session, followed by the exchange of secret keys. Although this process is robust and well known, it becomes a challenge to invoke robust cryptography protocols in IoT networks due to resource-constrained nodes.

B. Our Contribution

1) This article proposes a lightweight and anonymous user authentication scheme for IoT-based healthcare applications. The scheme is computationally efficient since it uses one-way hash functions and XOR operations.
2) The proposed protocol is safe against various attacks, like impersonation, replay, man-in-the-middle (MITM), denial of service, and exhibits most of the essential security properties, such as anonymity and privacy, and untraceability.
3) The proposed scheme only permits the registered and verified users to access the medical networks through secure sessions.

III. Preliminaries

A. System Model

Fig. 1 shows the system model to illustrate the communication among different entities (doctor (user), gateway, and IoT sensor node) in an IoT healthcare environment.

1) *User:* The doctor has to prove his legitimacy at the network gateway before communicating with the sensor node to access patients' reports. We assume that the device used by the doctor is resource-constrained.

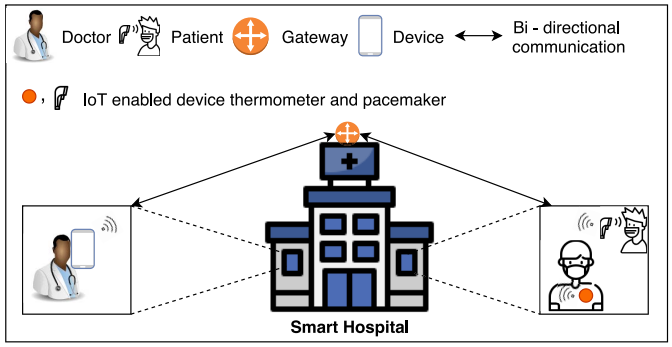

Fig. 1. System Model depicting the communication in a smart hospital.

2) *Gateway:* Gateway acts as a hub between the doctor and the sensor node. It is worth noting that the gateway is not a resource-deprived entity.
3) *IoT Sensor Node:* IoT enabled sensor nodes collect and transmit the real-time data of the patients'. The sensor nodes have a wireless connection to the doctor's devices through a gateway. IoT nodes are low-power devices with limited computation abilities.

B. Adversary Model

The proposed protocol considers the Dolev–Yao (DY) model to determine the protocol's performance under different compromised conditions [26]. Consider a healthcare IoT network [27], [28] that deploys an IoT-enabled pacemaker at the patient's chest. Considering the adversary model [29], the attacker can change the frequency rate for controlling the patient's heartbeat. The attacker can also flood the doctor's device by spamming it with meaningless data. For instance, the intruder can try to eavesdrop on the conversation to gain access to confidential data. The attacker can also replay the messages and obtain access to the doctor's device or IoT node. The cyberattacks can result in mild to severe consequences, including patient's death, financial, reputation loss of healthcare institutions, and in other industrial systems [30].

C. Security and Other Goals

The suggested scheme exhibits prominent security properties. We adopt the security properties from [31].

1) *Mutual Authentication and Key Establishment:* The hospital network is known to be very sensitive because several nodes are connected to the hospital machines (e.g., ventilator). The user device and sensor nodes must perform mutual authentication and key agreement for their secure communication.
2) *Data Privacy:* Hospital network carries very sensitive information through itself (e.g., User ID, password, secret key, etc.). If any of the information gets leaked, it may jeopardize patients' lives and harm the hospital's reputation. Therefore, the information must be exchanged confidentially.
3) *Freshness and Message Integrity:* If the real data is tampered with, nonpermissible parties can cause significant damage. Therefore, the protocols used in e-Healthcare must preserve the integrity and freshness of the transferred data.
4) *Anonymity of Identity:* Intruders are always looking for loopholes and important data like passwords, user id, etc. Intruders can use these identities for conducting MITM and impersonation attacks. Therefore, it is imperative to keep the identities of the network devices anonymous while exchanging messages.
5) *Lightweightness:* IoT nodes are resource-constrained, i.e., the nodes can execute only limited computations. Therefore, the security protocols must be constructed with lightweight cryptography primitives (e.g., hash and bitwise XOR) to extend devices' active lifetime.

TABLE II
NOTATIONS AND DESCRIPTIONS

Notation	Description
D_{ID}, S_{ID}	Doctor identity, Sensor node (SN) identity
PW_D	Device password set by doctor
R_{req}	Registration request
R_{SG}, R_{SN}	Random secret generated by gateway & SN
h(.), $\|$	Hash function, concatenation operator
$\oplus$, SK	Bit wise XOR operation, Session key
S_{TID}, D_{TID}	Temporary identity of sensor node and doctor
N_D, N_G, N_S	Nonce generated by device, gateway, sensor node

IV. Proposed Scheme

Table II defines the notations used to explain the protocol's working. Greek symbols represent variables and have no mathematical significance.

A. Assumptions

We make the following assumptions.

1) Doctor device, gateway, and IoT sensor node are capable of computing similar cryptography operations.
2) Doctor device and the IoT sensor node are resource-constrained, whereas the gateway is connected to the main power supply and has no computational or storage constraints.
3) Gateway is a trustworthy entity and cannot be tampered.
4) Communication channel used during registration is secure, whereas a public (insecure) channel is used to relay the messages post-registration.

B. User Registration Phase

A doctor (user) must register his device with the gateway to obtain real-time patients' health information. Fig. 2 demonstrates the steps of the user registration phase.

Step 1: Doctor enters D_{ID}, PW_D, and generates the message, R_{req}. Then R_{req} is transmitted through the secure channel to the gateway.

Step 2: The gateway stores the user information D_{ID}, PW_D for future use. Afterwards, the gateway generates R_{SG}^1, and computes $\alpha = (D_{\text{ID}} \oplus R_{\text{SG}}^1) \oplus \text{PW}_D$. Now gateway generates the temporary id of user, D_{TID} and computes $R_{\text{SG}}^1 \oplus D_{\text{ID}}$. Thereafter, the gateway stores the values in itself R_{SG}^1, D_{TID} and send α to the user through the secure channel.

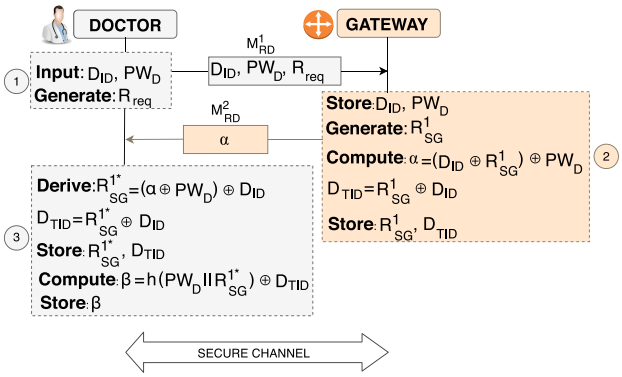

Fig. 2. User registration phase.

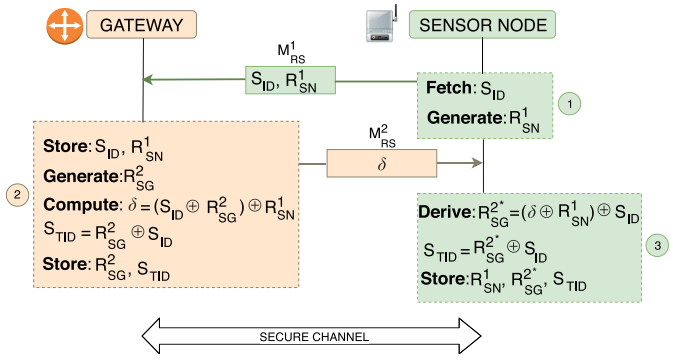

Fig. 3. Sensor node registration phase.

Step 3: The doctor receives the value α from the gateway and derives R^1_{SG} from $(\alpha \oplus PW_D) \oplus D_{ID}$. The temporary identity of user D_{TID} is derived from $R^1_{SG} \oplus D_{ID}$ and the values R^1_{SG}, D_{TID} are stored. Then the user computes and stores $\beta = (PW_D || R^{1*}_{SG}) \oplus D_{TID}$ for further use.

C. Sensor Node Registration Phase

The sensor node must register itself in the gateway before delivering real-time information of patients to the doctor. Fig. 3 illustrates the sensor node registration phase.

Step 1: Sensor node retrieves the identity detail S_{ID} from its processor, and generates the random secret value R^1_{SN}. Subsequently, the sensor node concatenates S_{ID}, R^1_{SN} and sends it to the gateway through the secure channel.

Step 2: Upon reception, gateway stores the S_{ID}, R^1_{SN}. Thereafter, gateway generates the new random secret value R^2_{SG}. Next, gateway computes $\delta = (S_{ID} \oplus R^2_{SG}) \oplus R^1_{SN}$ temporary identity, $S_{TID} = R^2_{SG} \oplus S_{ID}$ followed by storing the R^2_{SG}, S_{TID} in its memory. Finally, gateway sends δ to the sensor node through secure channel.

Step 3: The sensor node receives message from the gateway and computes $R^{2*}_{SG} = (\delta \oplus R^1_{SN}) \oplus S_{ID}$. Lastly, sensor node derives its temporary identity from $R^{2*}_{SG} \oplus S_{ID}$ and stores the values R^1_{SN}, R^2_{SG}, and S_{TID}.

D. Mutual Authentication and Key Agreement Phase

Consider a doctor who intends to observe instantaneous information of a particular IoT sensor node embedded on the medical appliance. But before the exchange of information, the doctor and sensor node verify the authenticity of each other. Fig. 4 shows the complete process of mutual authentication and key agreement.

Step 1: Doctor enters the password PW_D in the device and computes $Q = h(PW_D || R^1_{SG}) \oplus D_{TID}$. Now the doctor's device verifies Q with respect to β which is stored in device during registration phase. If the values of both Q and β are equal, then the device continue the process else it is aborted. Afterwards, the doctor's device generates the nonce N^1_D, then computes $N^{1*}_D = N^1_D \oplus PW_D$. The device further computes $R^1_{SG} || PW_D$ to form λ. Lastly, the user device sends the following information N^{1*}_D, D_{TID}, and λ, S_{TID} to the gateway.

Step 2: When the gateway receives information from the user, first it extracts the value N^1_D from $N^{1*}_D \oplus PW_D$. The gateway checks the freshness of the nonce N^1_D. If found fresh, the procedure continues; else, it aborts. Further gateway locates the D_{TID} and S_{TID} in the database and compares it with the received ones; if values are identical, the process continues else aborted. The gateway then computes the hash of $(R^1_{SG} || PW_D)$ to form λ^*. Now the gateway extracts the λ from its database and compares it with the computed λ^*. Identicalness results in successful authentication of the user at the gateway. The gateway generates the nonce N^1_G, computes the XOR of S_{TID} and N^1_G, and stores it in G^1_W. Then, the gateway calculates $h(R^1_{SN} || R^2_{SG})$ to form G^2_W. Further, gateway generates the session key (SK) for the sensor node and enlcose secretly within $SK_S = (SK \oplus R^1_{SN}) \oplus N^1_G$. Gateway computes and stores the $G^3_W = R^3_{SG} \oplus R^1_{SN}$.

Now gateway sends the information G^1_W, G^2_W, D_{TID}, SK_S, and G^3_W through public channel to the sensor node.

Step 3: Upon reception, the sensor node extracts the nonce N^1_G from $G^1_W \oplus S_{TID}$, and verifies the freshness. The process continues if the nonce is found fresh, else terminates. The gateway then computes hash $(R^1_{SN} || R^2_{SG})$ and forms the S^1_N. The gateway verifies if S^1_N is the same as G^2_W, similar values indicate the successful authentication of the gateway at the sensor node. The sensor node retrieves SK from $(SK_S \oplus N^1_G) \oplus R^1_{SN}$. The sensor node generates the nonce N^1_S, and computes $N^1_S \oplus S_{TID}$ to form S^2_N. Now sensor node computes the hash of $(R^{2*}_{SG} || R^1_{SN} || SK)$ and stores it in S^3_N, whereas $R^2_{SG} \oplus R^2_{SN}$ is stored as S^4_N. The sensor node also retrieves the R^2_{SG} from $G^3_W \oplus R^1_{SN}$ and derives the new temporary id of sensor node $S^{new}_{TID} = R^3_{SG} \oplus S_{ID}$ and store the information R^2_{SN}, R^2_{SG}, S^{new}_{TID}. Finally, the sensor node sends S^2_N, S^3_N, and S^4_N to the gateway.

Step 4: Gateway extracts the nonce N^1_S from $S^2_N \oplus S_{TID}$ after receiving the message from sensor node. Subsequently, the freshness of the nonce is verified. The gateway further computes the hash of $(R^2_{SG} || R^1_{SN} || SK)$. The gateway verifies both the values G^4_W and S^3_N, the identicalness indicates the accomplishment of mutual authentication process between sensor node gateway. Additionally, it specifies that the sensor node has derived the correct SK successfully. Gateway retrieves the value R^2_{SN} from the $S^4_N \oplus R^2_{SG}$ and computes $R^3_{SG} \oplus S_{ID}$ to form S^{new}_{TID}. The gateway stores the information R^2_{SN}, R^3_{SG}, and S^{new}_{TID} with itself. In the next step, gateway generates nonce N^2_G and computes $D_{ID} \oplus N^2_G$ to form μ. Afterwards,

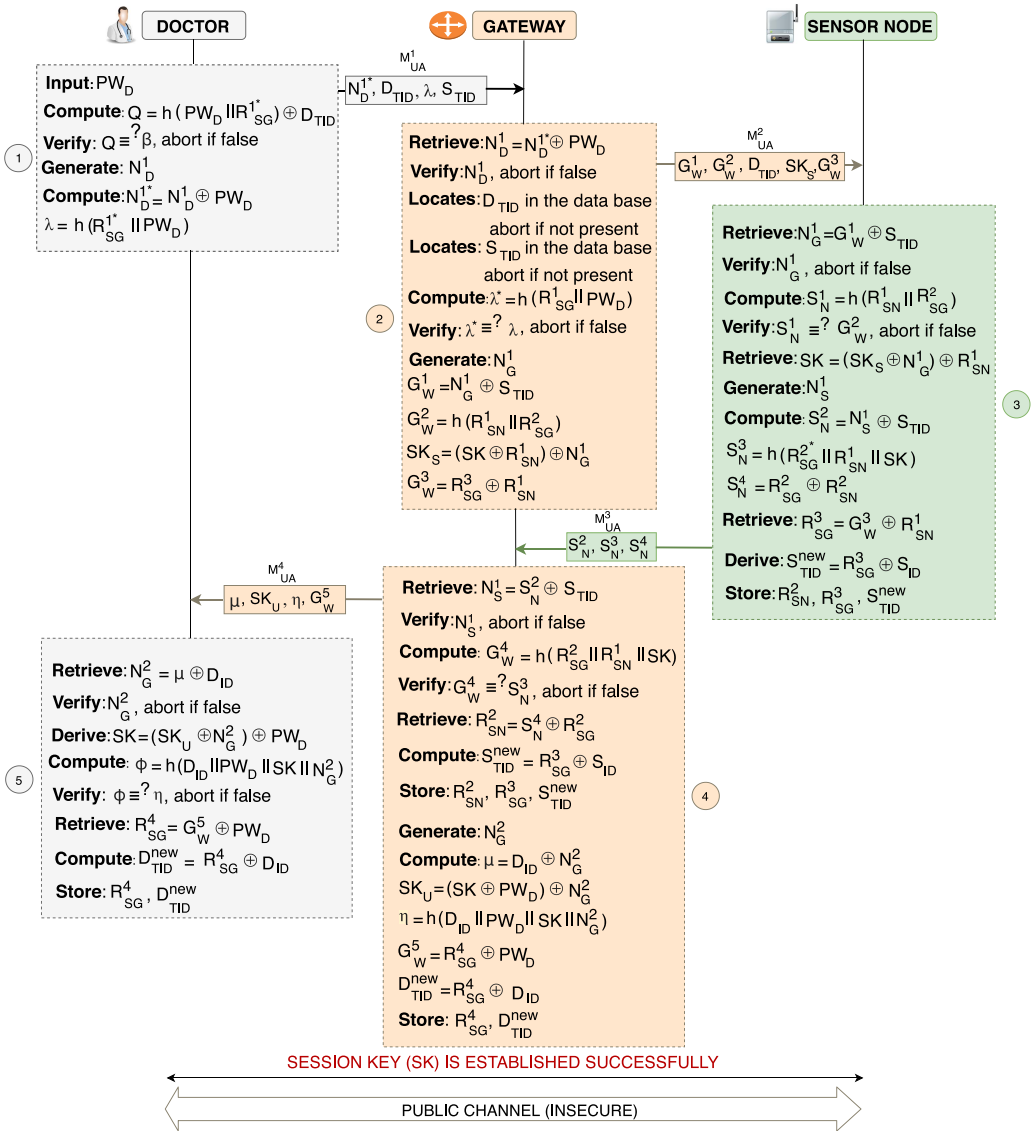

Fig. 4. Mutual authentication and key agreement phase.

gateway generates the SK for the user and enclose it secretly within $\text{SK}_U = (\text{SK} \oplus \text{PW}_D) \oplus N_G^2$. Now gateway calculates $\text{h}(D_{\text{ID}} \,||\, \text{PW}_D \,||\, \text{SK} \,||\, N_G^2)$ to get η whereas $R_{\text{SG}}^4 \oplus \text{PW}_D$ is stored in G_W^5. The gateway generates the new temporary identity of user device, $D_{\text{TID}}^{\text{new}} = R_{\text{SG}}^4 \oplus D_{\text{ID}}$. Gateway stores R_{SG}^4, $D_{\text{TID}}^{\text{new}}$, and send the following information to the user device, μ, SK_U, η, and G_W^5 through insecure public channel.

Step 5: The user (doctor) device extracts the nonce N_G^2 from $\mu \oplus D_{\text{ID}}$ and verifies the freshness; if found fresh, then operation is continued else it discontinues. Next, the user device derives the value SK from $(\text{SK}_U \oplus N_G^2) \oplus \text{PW}_D$. Subsequently, gateway calculates $\text{h}(D_{\text{ID}} \,||\, \text{PW}_D \,||\, \text{SK} \,||\, N_G^2)$ and stores the result in ϕ. Then, ϕ and η are compared with each other; homogeneous values indicate the accomplishment of mutual authentication between gateway and user. Also, it indicates the generation of the correct SK by the user device. The device then retrieves R_{SG}^4 from $G_W^5 \oplus \text{PW}_D$ and computes new temporary identity of device $D_{\text{TID}}^{\text{new}}$ from $R_{\text{SG}}^4 \oplus D_{\text{ID}}$ and store the value R_{SG}^4 and $D_{\text{TID}}^{\text{new}}$ in its memory.

In the end, the secret SK is generated effectively between the sensor node and the user device.

V. Security Analysis

A. Formal

For verifying the goals of security, we employed a broadly trusted tool called the "automated validation of Internet security protocols and applications (AVISPAs)" [32]. There are chiefly four backends in AVISPA, particularly "on-the-fly mode-checker (OFMC)," "constraint-logic-based attack searcher (CL-AtSe)," "SAT (Boolean satisfiability problem)-based model checker (SATMC)," and "tree automata based on automatic approximations for the analysis of security protocols (TA4SPs)." AVISPA takes the input in "high-level protocol specification language (HLPSL)" and converts it into the "intermediate format (IF)" with the HLPSl2IF. IF is fed into one backend out of four to generate the "output format

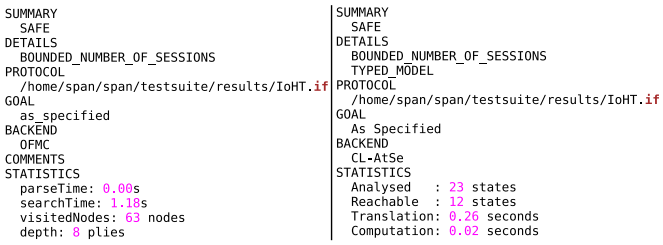

Fig. 5. Simulation results from OFMC and CL-AtSe backends of AVISPA.

(OF)." The OF produces any of the three outcomes, in particular, i.e., "safe," "unsafe," or "inconclusive." The "basic" functions of the communicating objects are described first, followed by "session" and "environment" roles. The description of basic roles of the agents also include the security goal predicates (secret and witness) to limit the boundaries of evaluation. The environment role specifies the global constants, knowledge of the intruder based on the adversary model (*DY*), and the details of the probable communication sessions between authentic and unauthentic communicating entities. The proposed scheme provides three roles of entities: 1) user device; 2) gateway; and 3) sensor node. The present evaluation covers only two backends, i.e., OFMC and CL-AtSe, because the remaining two (i.e., SATMC and TA4SP) do not include bitwise XOR operations while generating the output. Fig. 5 illustrates the simulation results of OFMC and CL-AtSe backend. It is apparent from the simulation results that the OFMC backend visited 63 nodes with a depth of 8 plies in 1.18 s to conclude the protocol safe from cyber threats. Likewise, the CL-AtSe backend analyzed 23 states in 0.26 s to declare the protocol safe. Therefore, the proposed authentication protocol can be used as a better alternative to the existing authentication protocols with limited protection.

B. Informal

Theorem 1: Resilient against replay attacks.

Proof: Let's consider an example, the attacker captured the message, $M_{\text{UA}}^1 = N_D^{1*}$, D_{TID}, λ, S_{TID} and later replayed to the gateway. Upon reception, gateway examines the freshness of nonce $N_D^{1*} = N_D^1 \oplus \text{PW}_D$. The replayed message contains an old nonce; hence the session is terminated by the gateway. The identical process is followed for other messages (M_{UA}^2, M_{UA}^3, M_{UA}^4) as well. Moreover, it is not possible for the adversary to modify the nonce N_D^1 since it is enclosed secretly $N_D^{1*} = N_D^1 \oplus \text{PW}_D$. Similarly, the nonce in all the messages, M_{UA}^2, M_{UA}^3, and M_{UA}^4 are protected from modifications. Hence, the proposed protocol is safe from replay attacks. ■

Theorem 2: Resistant to MITM attack.

Proof: Let's assume that an attacker conducts the MITM attack between the user device and gateway. The attacker captured the message $M_{\text{UA}}^1 = N_D^{1*}$, D_{TID}, λ, S_{TID} and try to modify it for fooling other involved entities. However, adversary cannot modify $\lambda = h(R_{\text{SG}}^{1*} || \text{PW}_D)$ because hash functions have collision-resistant property. Therefore, the attacker fails to modify the information of M_{UA}^1. Similarly, M_{UA}^2, M_{UA}^3, and M_{UA}^4 are also protected from alterations. ■

Theorem 3: Protection from impersonation attacks.

Proof: The presented protocol is safe from impersonation attacks because the adversary has no secret information about the entities to misuse and impersonate. Let's assume that attacker captured the message $M_{\text{UA}}^2 = G_W^1$, G_W^2, D_{TID}, SK_S, G_W^3 and try to retrieve the secret credentials of user and sensor node. However, the attacker fails because the $G_W^1 = N_G^1 \oplus S_{\text{TID}}$ is not accessible as plain text, $G_W^2 = h(R_{\text{SN}}^1 \mid |R_{\text{SG}}^2)$ is available as message digest, D_{TID} is temporary identity of user device, whereas SK_S and G_w^3 are also computed through XOR operation. Therefore, as per the hash functions' collision-resistant property, the attacker cannot retrieve the original information from the message. Hence, attackers and malicious nodes do not have any identity or even secret information to prove legitimate users and sensor nodes, respectively. Therefore, impersonation is not possible in the proposed protocol. Even other messages exchanged M_{UA}^1, M_{UA}^3, and M_{UA}^4 are nonvulnerable. ■

Theorem 4: Attains identity anonymity and untraceability.

Proof: Consider an attacker seizes the message $M_{\text{UA}}^1 = N_D^{1*}$, D_{TID}, λ, S_{TID}. Despite capturing, attacker could not retrieve the identity information because temporary identities (D_{TID} and S_{TID}) are used instead of real identities (D_{ID} and S_{ID}). Therefore, the communication remains anonymous. Moreover, temporary identities changes every session ($D_{\text{TID}}^{\text{new}}$, $S_{\text{TID}}^{\text{new}}$). Hence, the attacker fails to trace the message journey. ■

Theorem 5: SK agreement and its security.

Proof: The proposed scheme enables the user and the IoT node to exchange the session keys in real-time to secure the communications. The gateway acts as an intermediary and helps them in exchanging the keys. For instance, the gateway in Fig. 4 generates the keys for both the parties after the successful examination of their legitimacy. The gateway enclose the secret key of sensor node (SK) within $\text{SK}_S = (\text{SK} \oplus R_{\text{SN}}^1) \oplus N_G^1$ and send it to sensor node in message M_{UA}^2. Afterwards, gateway enclose the user key (SK) within $\text{SK}_U = (\text{SK} \oplus \text{PW}_D) \oplus N_G^2$ and send it to user in message M_{UA}^4. Both parties can use this key for securing their communications. It is noteworthy that the attacker cannot steal the keys despite shared through insecure public channels as the keys are not sent in plain-text. Since adversary do not know R_{SN}^1, N_G^1, PW_D, and N_G^2, therefore the adversary cannot retrieve the keys from messages M_{UA}^2 and M_{UA}^4. ■

Theorem 6: Proposed protocol ensures data privacy.

Proof: Let us assume that the adversary captured the message, $M_{\text{UA}}^3 = S_N^2 \| S_N^3 \| S_N^4$ wherein $S_N^2 = N_S^1 \oplus S_{\text{TID}}$, $S_N^3 = R_{\text{SG}}^{2*} \,||\, R_{\text{SN}}^1 \,||\, \text{SK}$, and $S_N^4 = R_{\text{SG}}^2 \oplus R_{\text{SN}}^2$. The adversary cannot determine the real information from the message M_{UA}^3 because none of the message components (S_N^2, S_N^3, S_N^4) carry the information in plaintext; they are either in message digest form or have undergone bitwise XOR computations. It is well proven that retrieving information from the hash is not possible due to collision-resistant property. Therefore, an adversary cannot read any information from the messages exchanged by the protocol. Hence, data privacy is ensured. ■

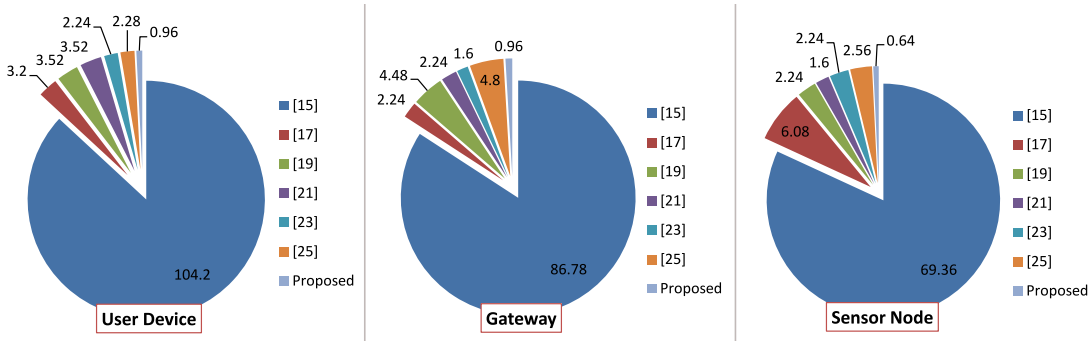

Fig. 6. Execution Cost (*ms*) comparison of proposed versus conventional protocols.

TABLE III
COMPUTATIONAL COST OF THE PROPOSED PROTOCOL

Phase	User device	Gateway	Sensor node	Total
P_1	CC_h	-	-	CC_h
P_2	-	-	-	-
P_3	$3 * CC_h$	$3 * CC_h$	$2 * CC_h$	$8 * CC_h$
Total	$4 * CC_h$	$3 * CC_h$	$2 * CC_h$	$9 * CC_h$

Acronyms: CC_h: Computational Cost Hash, P_1: User Registration, P_2: Sensor Node Registration, P_3: Mutual Authentication and Key Agreement.

TABLE IV
COMPARISON OF COMPUTATION COSTS

Scheme	User device	Gateway	Sensor Node	Total cost
[15]	$5 * CC_h$	$4 * CC_h$	$3 * CC_h$	$12 * CC_h$
[17]	$10 * CC_h$	$7 * CC_7$	$19 * CC_h$	$36 * CC_h$
[19]	$11 * CC_h$	$14 * CC_h$	$7 * CC_h$	$32 * CC_h$
[21]	$11 * CC_h$	$7 * CC_h$	$5 * CC_h$	$23 * CC_h$
[23]	$7 * CC_h$	$5 * CC_h$	$7 * CC_h$	$19 * CC_h$
[25]	$9 * CC_h$	$15 * CC_h$	$8 * CC_h$	$32 * CC_h$
P_S	$3 * CC_h$	$3 * CC_h$	$2 * CC_h$	$8 * CC_h$

Acronyms: CC_h: Computation Cost Hash, P_S: Proposed Scheme.

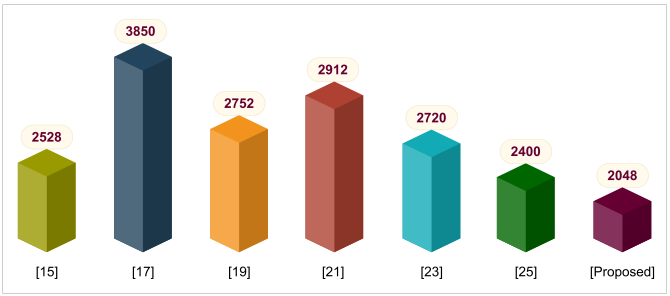

Fig. 7. Communication cost (*bits*) comparison of the proposed versus conventional protocols.

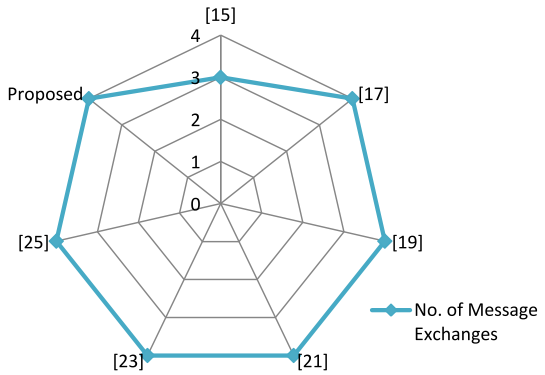

Fig. 8. Number of messages exchanged by the proposed and conventional protocols during key establishment phase.

TABLE V
ANALYSIS AND COMPARISON OF THE PROPOSED PROTOCOL BASED ON PROTECTION AGAINST ATTACKS AND SECURITY GOALS

ASP	[15]	[17]	[19]	[21]	[23]	[25]	P_S
ASP_1	✓	✓	×	×	✓	✓	✓
ASP_2	✓	✓	×	×	✓	✓	✓
ASP_3	✓	×	×	×	×	✓	✓
ASP_4	✓	✓	×	×	×	✓	✓
ASP_5	✓	✓	✓	✓	✓	✓	✓
ASP_6	✓	×	×	✓	×	×	✓
ASP_7	✓	×	✓	✓	✓	✓	✓
ASP_8	✓	×	✓	✓	✓	✓	✓
ASP_9	✓	×	✓	✓	✓	✓	✓
ASP_{10}	✓	✓	✓	✓	✓	✓	✓
ASP_{11}	×	✓	✓	✓	×	✓	✓
ASP_{12}	×	×	✓	✓	✓	✓	✓
ASP_{13}	✓	✓	✓	✓	×	✓	✓

Acronyms: ✓: Protected/Compliance; ×: Vulnerable/non compliance; P_S: Proposed Scheme; ASP: Attack and Security properties; ASP_1: Identity anonymity of user device; ASP_2: Identity anonymity of IoT sensor node; ASP_3: privileged-insider attack; ASP_4: off-line password guessing attack; ASP_5: denial-of-service attack; ASP_6: user impersonation attack; ASP_7: replay attack; ASP_8: man-in-the middle attack; ASP_9: mutual authentication; ASP_{10}: session key agreement; ASP_{11}: untraceability; ASP_{12}: IoT sensor node impersonation attack; ASP_{13}: Formal security verification.

VI. PERFORMANCE AND COMPARATIVE ANALYSIS

The computation cost spent by the user device, sensor node, and gateway for all phases of the protocol (user registration, sensor node registration, mutual authentication, and key agreement) are presented in Table III. The IoT network's resource-constrained nodes are computing few crypto operations in each phase, hence exhibiting computation efficiency. Table IV shows that the proposed scheme executes the hash function just eight times, far less than the other schemes. Fig. 6 signifies the difference of execution cost (*ms*) between the proposed scheme and the conventional protocols. From Table V, it is evident that the proposed scheme can resist most

of the significant attacks and is also more secure than the old schemes. Fig. 7 indicates that the number of bits exchanged by the proposed scheme is 2048 bits far less than the conventional protocols. Fig. 8 demonstrates the number of messages exchanged among the different entities in the mutual authentication and the key agreement phase. The proposed scheme exchanges an equivalent number of messages as the other schemes.

VII. Conclusion and Future Directions

This research presents a lightweight and anonymity-preserving user authentication scheme for resource-constrained IoT-based digital health networks. The protocol is implemented using computation efficient cryptography primitives, such as one-way hash function, bit-wise XOR, and the nonce to accomplish the user authentication process. The scheme is safe from major types of attacks like replay, MITM, DoS, etc. Further, we demonstrate that the scheme has low computational and communication costs compared to the state-of-the-art approaches. With its broad applicability in healthcare applications, this scheme is expected to be deployed more than traditional ones. In the future, the zero-knowledge proof concept and PUF will be integrated into the proposed protocol to extend the security and privacy of the information exchanged in IoT networks.

References

[1] M. S. Hossain, and G. Muhammad, "Cloud-assisted Industrial Internet of Things (IIoT)–Enabled framework for health monitoring," *Comput. Netw.*, vol. 101, pp.192–202, Jun. 2016.

[2] M. Almulhim and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications," in *Proc. IEEE 20th Int. Conf. Adv. Commun. Technol. (ICACT)*, Chuncheon, South Korea, Feb. 2018, pp. 481–487.

[3] P. Kumar, S.-G. Lee, and H.-J. Lee, "E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks," *Sensors*, vol. 12, no. 2, pp. 1625–1647, 2012.

[4] M. S. Hossain, "Cloud-supported cyber–physical localization framework for patients monitoring," *IEEE Syst. J.*, vol. 11, no. 1, pp. 118–127, Mar. 2017.

[5] R. K. Pathinarupothi, P. Durga, and E. S. Rangan, "IoT-based smart edge for global health: Remote monitoring with severity detection and alerts transmission," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2449–2462, Apr. 2019.

[6] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and provenance enhanced Internet of health things framework: A blockchain managed federated learning approach," *IEEE Access*, vol. 8, pp. 205071–205087, 2020.

[7] M. S. Hossain, G. Muhammad, and N. Guizani, "Explainable AI and mass surveillance system-based healthcare framework to combat COVID-I9 like pandemics," *IEEE Netw.*, vol. 34, no. 4, pp. 126–132, Jul./Aug. 2020.

[8] Y. Abdulsalam and M. S. Hossain, "COVID-19 networking demand: An auction-based mechanism for automated selection of edge computing services," *IEEE Trans. Netw. Sci. Eng.*, early access, Sep. 24, 2020, doi: 10.1109/TNSE.2020.3026637.

[9] M. S. Hossain and G. Muhammad, "Emotion-aware connected healthcare big data towards 5G," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2399–2406, Aug. 2018.

[10] H.-M. Chen, J.-W. Lo, and C.-K. Yeh, "An efficient and secure dynamic ID-based authentication scheme for telecare medical information systems," *J. Med. Syst.*, vol. 36, no. 6, pp. 3907–3915, 2012.

[11] T. Cao and J. Zhai, "Improved dynamic ID-based authentication scheme for telecare medical information systems," *J. Med. Syst.*, vol. 37, no. 2, p. 9912, 2013.

[12] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, and Y. Chung, "A secure authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 3, pp. 1529–1535, 2012.

[13] H. Debiao, C. Jianhua, and Z. Rui, "A more secure authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 3, pp. 1989–1995, 2012.

[14] J. Wei, X. Hu, and W. Liu, "An improved authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 6, pp. 3597–3604, 2012.

[15] S. Challa *et al.*, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[16] X. Jia, D. He, L. Li, and K.-K. R. Choo, "Signature-based three-factor authenticated key exchange for Internet of Things applications," *Multimedia Tools Appl.*, vol. 77, no. 14, pp. 18355–18382, 2018.

[17] L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance," *Future Gener. Comput. Syst.*, vol. 91, pp. 244–251, Feb. 2019.

[18] M. Masud *et al.*, "A lightweight and robust secure key establishment protocol for Internet of medical things in COVID-19 patients care," *IEEE Internet Things J.*, early access, Dec. 28, 2020, doi: 10.1109/JIOT.2020.3047662.

[19] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Netw.*, vol. 36, pp. 152–176, Jan. 2016.

[20] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, L. Leng, and N. Kumar, "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks," *Comput. Netw.*, vol. 101, pp. 42–62, Jun. 2016.

[21] G. Sharma and S. Kalra, "A lightweight user authentication scheme for cloud-IoT based healthcare services," *Iran. J. Sci. Technol. Trans. Elect. Eng.*, vol. 43, no. 1, pp. 619–636, 2019.

[22] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Adv. Cryptol. (EUROCRYPT)*, 2002, pp. 337–351.

[23] 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.

[24] R. Amin and G. P. 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.

[25] M. Wazid, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "LDAKM-EIoT: Lightweight device authentication and key management mechanism for edge-based IoT deployment," *Sensors*, vol. 19, no. 24, p. 5539, 2019.

[26] G. S. Gaba, G. Kumar, H. Monga, T.-H. Kim, and P. Kumar, "Robust and lightweight mutual authentication scheme in distributed smart environments," *IEEE Access*, vol. 8, pp. 69722–69733, 2020.

[27] L. Hu, M. Qiu, J. Song, M. S. Hossain, and A. Ghoneim, "Software defined healthcare networks," *IEEE Wireless Commun.*, vol. 22, no. 6, pp. 67–75, Dec. 2015.

[28] S. U. Amin, M. Alsulaiman, G. Muhammad, M. A. Mekhtiche, and M. S. Hossain, "Deep learning for EEG motor imagery classification based on multi-layer CNNs feature fusion," *Future Gener. Comput. Syst.*, vol. 101, pp. 542–554, Dec. 2019.

[29] A. Rahman, M. S. Hossain, N. A. Alrajeh, and F. Alsolami, "Adversarial examples—Security threats to COVID-19 deep learning systems in medical IoT devices," *IEEE Internet Things J.*, early access, Aug. 3, 2020, doi: 10.1109/JIOT.2020.3013710.

[30] A. K. Sangaiah, D. V. Medhane, G.-B. Bian, A. Ghoneim, M. Alrashoud, and M. S. Hossain, "Energy-aware green adversary model for cyberphysical security in industrial system," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3322–3329, May 2020.

[31] G. S. Gaba, G. Kumar, H. Monga, T.-H. Kim, M. Liyanage, and P. Kumar, "Robust and lightweight key exchange (LKE) protocol for industry 4.0," *IEEE Access*, vol. 8, pp. 132808–132824, 2020.

[32] A. Armando *et al.*, "The AVISPA tool for the automated validation of Internet security protocols and applications," in *Proc. Int. Conf. Comput.-Aided Verification*, 2005, pp. 281–285.