A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care

Mehedi Masud, *Senior Member, IEEE*, Gurjot Singh Gaba, *Member, IEEE*, Salman Alqahtani, Ghulam Muhammad, *Senior Member, IEEE*, B. B. Gupta, *Senior Member, IEEE*, Pardeep Kumar, *Member, IEEE*, and Ahmed Ghoneim, *Member, IEEE*

***Abstract*—Due to the outbreak of COVID-19, the Internet of Medical Things (IoMT) has enabled the doctors to remotely diagnose the patients, control the medical equipment, and monitor the quarantined patients through their digital devices. Security is a major concern in IoMT because the Internet of Things (IoT) nodes exchange sensitive information between virtual medical facilities over the vulnerable wireless medium. Hence, the virtual facilities must be protected from adversarial threats through secure sessions. This article proposes a lightweight and physically secure mutual authentication and secret key establishment protocol that uses physical unclonable functions (PUFs) to enable the network devices to verify the doctor's legitimacy (user) and sensor node before establishing a session key. PUF also protects the sensor nodes deployed in an unattended and hostile environment from tampering, cloning, and side-channel attacks. The proposed protocol exhibits all the necessary security properties required to protect the IoMT networks, like authentication, confidentiality, integrity, and anonymity. The formal AVISPA and informal security analysis demonstrate its robustness against attacks like impersonation, replay, a man in the middle, etc. The proposed protocol also consumes fewer resources to operate and is safe from physical attacks, making it more suitable for IoT-enabled medical network applications.**

***Index Terms*—COVID-19, cyber–physical system, Internet of Medical Things (IoMT), key management, security.**

Manuscript received December 16, 2020; accepted December 22, 2020. Date of publication December 28, 2020; date of current version October 22, 2021. This work was supported by the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia, through the Vice Deanship of Scientific Research Chairs: Chair of Pervasive and Mobile Computing. *(Corresponding authors: Ghulam Muhammad; B. B. Gupta.)*

Mehedi Masud is with the Department of Computer Science, College of Computers and Information Technology, Taif University, Taif 21974, Saudi Arabia (e-mail: mmasud@tu.edu.sa).

Gurjot Singh Gaba is with the Department of Electronics and Electrical Engineering, Lovely Professional University, Phagwara 144411, India (e-mail: gurjot.17023@lpu.co.in).

Salman Alqahtani is with the Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia (e-mail: salmanq@ksu.edu.sa).

Ghulam Muhammad is with the Chair of Pervasive and Mobile Computing and also 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).

B. B. Gupta is with the Department of Computer Engineering, National Institute of Technology Kurukshetra, Haryana 136119, India, and also with the Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan (e-mail: bbgupta@nitkkr.ac.in).

Pardeep Kumar is with the Department of Computer Science, Swansea University, Swansea SA1 8EN, U.K. (e-mail: pardeep.kumar@swansea.ac.uk).

Ahmed Ghoneim is with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 51178, Saudi Arabia, and is also with the Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt (e-mail: ghoneim@ksu.edu.sa).

Digital Object Identifier 10.1109/JIOT.2020.3047662

I. Introduction

INTERNET of Medical Things (IoMT) has evolved from the Internet of Things (IoT), where the doctors can use the wireless media to communicate with IoT enabled sensor nodes, such as smart thermometers, smart ventilators, and so on [1]. The IoT enables sensor nodes to gather, analyze, and disseminate the health-related information of the patients in real-time to the doctors [2] and enable them to diagnose, treat, and monitor patients remotely. Since the outbreak of COVID-19, hospitals are now leveraging the remote monitoring framework using IoMT to transform healthcare professionals' physical medical practices to telemedical practices to perform their duty safely. However, there are many challenges in utilizing IoMT networks and the issues concerning patients' security and privacy and healthcare institutions' sensitive information. The possible adversarial threats are eavesdropping, data breach, and Denial of Service (DoS) [3], [4]. The situation becomes more adverse in IoMT since medical users and vendors have limited awareness of security threats [5] and possible remedies. The adversary likes to breach the data that mainly includes patients' medical records, home health data, bank details, insurance information, etc., [6]–[8].

The adversaries exploit the systems and networks' vulnerabilities to conduct cyberattacks and achieve their evil desires. The absence of robust mutual authentication and key establishment scheme is the key factor attracting the adversaries toward IoMT networks [9]. The existing mutual authentication schemes are not directly applicable to IoMT networks as they are computation and communication expensive and can drain the precious energy reserves of IoT sensor nodes [10]. Moreover, most of the schemes do not consider the hostile environment of deployment of sensor nodes and become vulnerable to physical, cloning, and side-channel attacks [11]. Therefore, IoMT networks need practical mutual authentication and a secret key establishment approach to provide

robust security in all environments while being lightweight in computation and communication.

Due to the communicable nature of COVID-19, doctors prefer to diagnose and monitor the COVID-19 patients remotely with IoT-enabled sensor nodes. Security and privacy are major concerns in IoMT since the sensitive information is exchanged over the unguarded wireless channel that is used in IoMT. The attacker can exploit this vulnerability and control medical equipment that may cause damage to the medical equipment, resulting in fatalities and infrastructure damage. To prevent adversarial threats, the doctors and the IoT sensor nodes need to register with the network and prove their legitimacy to the gateway before establishing the secret session key at the time of access. Designing such an approach, particularly in the IoMT network, is challenging due to resource limitations and the likelihood of physical capturing of IoT sensor nodes deployed in a hostile environment.

This article proposes a lightweight, robust, and physically secure mutual authentication and secret key (MASK) establishment protocol for securing the sensitive health information of the patients. The proposed protocol uses lightweight cryptography primitives, such as one-way hash function, nonce, physical unclonable function (PUF), and bitwise XOR operations. The reliability is verified using formal and informal security analysis. The protocol also prevents the physical loss of a device and side-channel attacks. The protocol also consumes fewer resources to operate and is safe from physical attacks, making it more suitable for IoT-enabled medical network applications.

This article is structured as follows. Section II discusses related work. Section III presents the system model, adversary model, security and other goals, and PUF. Section IV demonstrates how the MASK protocol works. Section V provides formal and informal security analysis. Section VI discusses performance and comparative analysis. Section VII concludes and highlights future scope.

II. Related Work

El-Latif *et al.* [12] proposed a quantum steganography protocol using hash function verify security. However, Tseng *et al.* [13] asserted that the [12] approach is only applicable to secure message in cloud-based IoT platform. To overcome the deficits, Das independently constructed a 2-factor user authentication protocol for wireless sensor networks (WSNs) [14]. But as per the cryptanalysis [15], the approach of Das [14] is found susceptible to impersonation attacks. Likewise, Chang *et al.* [16] examined the approach of Turkanović *et al.* [17] for user authentication and key agreement and found it vulnerable to impersonation attacks. Similarly, Gope *et al.* [18] introduced a novel real-time authentication and key agreement protocol. However, the protocol did not ascertain the anonymity of sensor nodes. Yeh *et al.* [19] introduced an asymmetric cryptography-based authentication protocol. Still, the scheme did not accomplish mutual authentication and is computationally expensive due to public-key cryptography. Hossain *et al.* [20] propose two-factor authentication schemes for end-to-end secured IoT environment using biometric traits, which are subjected to masquerade and replay

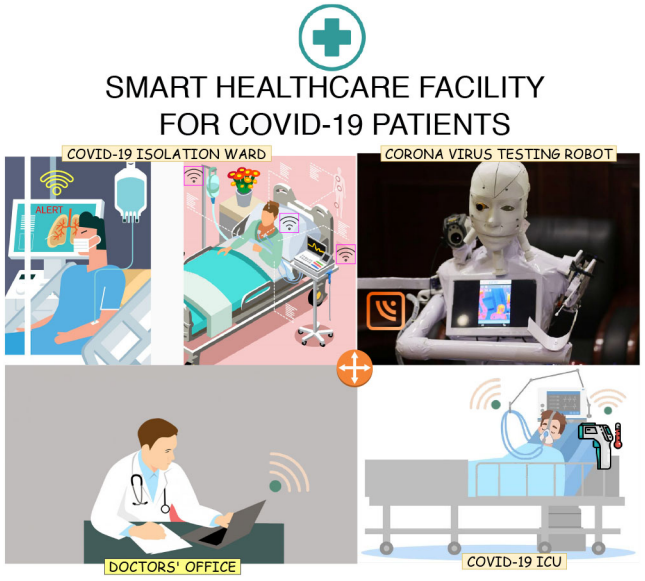

Fig. 1. System model for mutual authentication and key exchange between IoT devices in smart healthcare facility.

attacks. Das *et al.* [21] developed an IoT specific authentication approach using biometric and smart card to address the shortcomings. Likewise, Li *et al.* [22] designed a robust but resource expensive 3-factor user authentication scheme based on user identity, password, and biometrics. To reduce the computation expenditure, Esfahani *et al.* [23] introduced a lightweight scheme that uses a one-way hash function and bitwise XOR operations. Independently, Paliwal [24] tried to address the security issues of [25] by developing hash based mutual authentication and key agreement scheme. In summary, most of the protocols are insecure against significant adversarial threats, fail to exhibit essential security properties to keep the communication secure, and are computationally and communication expensive.

III. Preliminaries

System Model: Fig. 1 depicts the scenario of a smart healthcare facility where COVID-19 affected patients are diagnosed. Hossain *et al.* [26] and Abdulsalam and Hossain [27] framework consists of sensor nodes, a gateway, and the user (e.g., doctor). The sensor nodes are integrated with the medical equipment to monitor the patients' health, etc. Gateway is used to relay the information between the doctor, and IoT enabled sensor nodes in Healthcare-IoT [28]. The user (e.g., doctor) is interested in receiving real-time information from sensor nodes [e.g., ZigBee (IEEE 802.15.4), Z-Wave (e.g., *ZW*0500)]) to take decisive actions regarding the patients' treatment.

Adversary Model: In a smart healthcare facility, IoT sensor nodes relay real-time patient diagnosis reports. According to the Dolev–Yao (DY) adversary model [18], an adversary may disrupt the IoMT network's operation through malicious actions eavesdropping on the information related to the drug formula of the COVID-19 vaccine. The adversary can replay the eavesdropped message to get privileged access and intercept the messages to retrieve security credentials that can be

used later for generating keys to compromise subsequent communications. Besides, the adversary can delete or alter the patient medicine prescription. IoT sensors are deployed openly in smart healthcare facilities; therefore, they are subjected to cloning, side channel, and physical attacks.

Security and Other Goals: The "robust" and "efficient" [10], [18] goals of a security protocol are 1) performs MASK establishment; 2) protects against prominent attacks, such as MITM, replay, modification, impersonation, DoS, etc.; 3) keep data privacy property, i.e., a security protocol must implement a robust procedure considering eavesdropping by an adversary; 4) identity anonymity and untraceability, i.e., security protocol must exhibit identity anonymity and untraceability to prevent MITM and DoS attacks; 5) a security protocol must introduce a mechanism to protect the IoT devices when deployed in a hostile environment from physical tampering, cloning, and side-channel attacks; and 6) must use lightweight cryptography operations to utilize the resources efficiently.

Physically Unclonable Function: PUF is recommended as a solution to secure the hardware from adversarial threats. PUF neither stores any keys on edge devices nor uses public-key cryptography for performing authentication between devices. Besides, it cannot be cloned since the PUF is formed by making nanoscale variations during the integrated chip's manufacturing process (IC). All these attributes make the above a good choice for authentication of lightweight devices in IoHT [29]. An ideal PUF should exhibit the property of uniqueness, reliability, and unpredictability. Mathematically, PUF can be expressed as $R = P(C)$, wherein R denotes output response, P denotes PUF, and C denotes the input challenge. Since the output of the PUF depends upon the intrinsic physical variations in the IC, any tampering to the PUF would destroy the unique characteristics of the device [11].

TABLE I
SYMBOLS, ABBREVIATIONS, AND OPERATORS DESCRIPTION

Notation	Definition
C_E^N, R_E^N	C: Challenge, R: Response, N: Number, E: Entity
P_D, P_{SN}	Physically Unclonable Function
D_{ID}^H	Unique identity of doctor issued by Hospital
D_{LN}^{MCC}	Unique license no. issued by Medical Council
SN_{IEI}	International equipment identity of Sensor Node
TID_U, TID_{SN}	Temporary identity of User and Sensor Node
PW_U, F	User password, Strong cryptography function
N_U, N_G, N_{SN}	Nonce
SK_U, SK_{SN}	Session Key
h(.)	one way cryptography hash function
$\oplus$, $\|$	Bit-wise XOR and concatenation operator
$A \equiv^? B$	Is A identical to B?

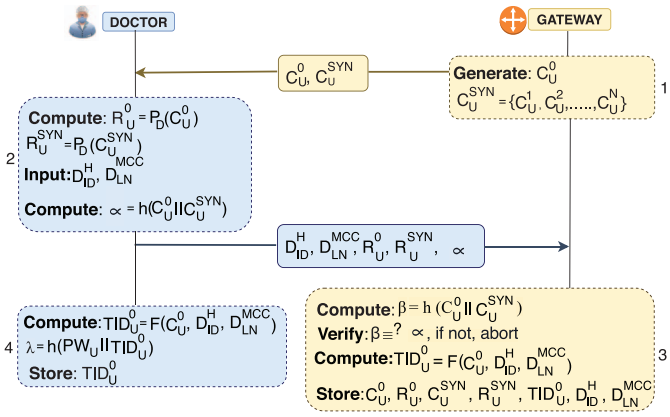

Fig. 2. User registration phase.

IV. Proposed Security Framework

The proposed protocol is executed in three phases, namely, *user registration*, *device registration*, and *MASK establishment*. Table I provides the notations that are used throughout this article. The following assumptions are considered in designing the protocol.

1) The IoT sensor node is integrated into medical equipment consist of a micro-controller (μC) attached to a PUF.
2) User device, gateway, and sensor nodes compute identical cryptography operations.
3) User devices and sensor nodes have some resource constraints (i.e., limited compute power and memory, etc.). But the gateway has no restrictions on computing and storage.
4) Sensor nodes are vulnerable to physical.

Now we present different phases of the protocol.

User Registration Phase: Fig. 2 illustrates the process of how a user("doctor") needs to register its trusted device in the gateway to obtain real-time health information of the patients.

Step 1: The gateway first generates a random challenge C_U^0 for the current registration process along with another set of challenges $C_U^{SYN} = \{C_U^1, C_U^2, \ldots, C_U^N\}$. C_U^{SYN} consists of many random challenges used by the gateway in the future to verify the user device. The gateway forms the message $\{C_U^0, C_U^{SYN}\}$ and sends it to the doctor's device.

Step 2: Upon receiving, $\{C_U^0, C_U^{SYN}\}$, doctor's device triggers the PUF to generate the response, R_U^0 and R_U^{SYN}. R_U^{SYN} comprises of responses to many random challenges $(= R_U^1, R_U^2, \ldots, R_U^N)$ that will be used by the gateway to authenticate the doctor's device in future correspondences. Afterwards, doctor inputs his/her unique identity details, D_{ID}^H, and D_{LN}^{MCC}. Thereafter, doctor's device compute $\alpha = h(C_U^0 \| C_U^{SYN})$ to enable the gateway to verify the association between received responses (R_U^0, R_U^{SYN}) and sent challenges (C_U^0, C_U^{SYN}). Lastly, the doctor's device compose a message, including D_{ID}^H, D_{LN}^{MCC}, R_U^0, R_U^{SYN}, α and sends it to gateway for requesting authorization to communicate with sensor nodes.

Step 3: After reception, gateway computes $\beta = h(C_U^0 \| C_U^{SYN})$ and verifies the identicalness between β and α; the gateway terminates the session if result is distinct, otherwise computes $TID_U^0 = F(C_U^0, D_{ID}^H, D_{LN}^{MCC})$. At the end of the registration,

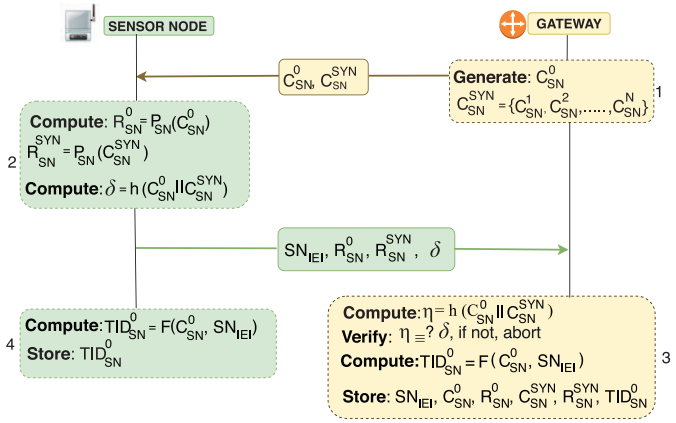

Fig. 3. Sensor node registration phase.

gateway stores the C^0_U, R^0_U, C^{SYN}_U, R^{SYN}_U, TID^0_U, D^H_{ID}, D^{MCC}_{LN} for future communication with user.

Step 4: Likewise, doctor's device also computes and stores $TID^0_U = F(C^0_U, D^H_{ID} D^{MCC}_{LN})$ and λ.

Remark 1: It is worth noting that TID^0_U is a function of C^0_U, D^H_{ID}, and D^{MCC}_{LN}. The use of new challenge C^N_U for every session assures distinct temporal identity TID^N_U for every session, thus achieving untraceability. Moreover, instead of real identity of user $\{D^H_{ID}, D^{MCC}_{LN}\}$, temporary identity TID^0_U is used to preserve user anonymity during message exchanges. λ is a function of TID^0_U and updates every session to protect the device from adversarial threats.

Device Registration Phase: The IoT node at the healthcare institution is first registered with the gateway. Fig. 3 illustrates registration process.

Step 1: The gateway generates a challenge for sensor node registration C^0_{SN} followed by another set of challenges C^{SYN}_{SN} $\{C^1_{SN}, C^2_{SN}, \ldots, C^N_{SN}\}$. The composed message $\{C^0_{SN}, C^{SYN}_{SN}\}$ is sent to the sensor node through a secure channel.

Step 2: Upon reception $\{C^0_{SN}, C^{SYN}_{SN}\}$, sensor node begins to prepare the responses $R^0_{SN} = P_{SN}(C^0_{SN})$, $R^{SYN}_{SN} = P_{SN}(C^{SYN}_{SN})$ to the received challenges (C^0_{SN}, C^{SYN}_{SN}). The sensor node computes $\delta = h(C^0_{SN} \| C^{SYN}_{SN})$ to enable the gateway in verifying the association between response and challenges. Finally, $\{SN_{IEI}, R^0_{SN}, R^{SYN}_{SN}, \delta\}$ is delivered.

Step 3: Gateway at first computes $\eta = h(C^0_{SN} \| C^{SYN}_{SN})$ followed by a comparison of $\eta \equiv^? \delta$ to verify the relationship between responses and challenges. Subsequently, the gateway derives the temporary identity of the sensor node $TID^0_{SN}\{= F(C^0_{SN}, SN_{IEI})\}$. After the computations and retrieval, the gateway stores the SN_{IEI}, C^0_{SN}, R^0_{SN}, C^{SYN}_{SN}, R^{SYN}_{SN}, and TID^0_{SN}.

Step 4: The sensor node computes and stores the temporary identity $TID^0_{SN}\{= F(C^0_{SN}, SN_{IEI})\}$. TID^0_{SN} enables the sensor node to accomplish anonymity and untraceability.

Remark 2: Gateway records the real identity of the sensor node SN_{IEI} during registration. It is noteworthy that TID^0_{SN} is a function of C^0_{SN}, and SN_{IEI}. The use of new challenge C^N_U for every session assures distinct short-term identity of sensor node TID^N_{SN} for every session, therefore accomplishing untraceability. Moreover, TID^0_{SN} does not disclose the real identity of the sensor node during message exchanges, thus preserving sensor node identity anonymity.

Mutual Authentication and Secret Key Establishment Phase: Fig. 4 illustrates the process of MASK establishment and explained as follows.

Step 1: Initially, the doctor has to prove his/her identity by entering his password PW_U. The doctor's device then calculates $\lambda^* = h(PW_U \| TID^0_U)$ and verifies the user's authenticity, $\lambda^* \equiv^? \lambda$. After successful verification the device generates a nonce N^1_U, and computes $N^{1*}_U = N^1_U \oplus D^H_{ID}$ to protect the nonce privacy. The doctor's device creates a pseudo-identity $TID^{0*}_U = TID^0_U \oplus D^{MCC}_{LN}$ from the temporary identity TID^0_U to add a second layer of identity anonymity and untraceability protection. Finally, the doctor's device sends the message $\{N^{1*}_U, TID^{0*}_U\}$ to the gateway.

Step 2: After receiving $\{N^{1*}_U, TID^{0*}_U\}$, the gateway extracts the real nonce, $N^1_U = N^{1*}_U \oplus D^H_{ID}$. The gateway then verifies the freshness of the N^1_U. Subsequently, the gateway derives the temporary identity from pseudo-identity, $TID^0_U = TID^{0*}_U \oplus D^{MCC}_{LN}$ and matches with the database. Once TID^0_U is located, the gateway selects the corresponding challenge (C^0_U) and response (R^0_U). To meet the privacy requirements, the gateway encloses the real C^0_U, N^1_G within the G_1 $(= D^H_{ID} \oplus C^0_U)$ and G_2 $(= D^{MCC}_{LN} \oplus N^1_G)$. Finally, the gateway computes $G_3 = h(C^0_U \| N^1_G \| R^0_U)$; G_3 helps the doctor's device to verify the authenticity of the gateway. The gateway sends the challenge C^0_U, nonce N^1_G, and authentication message enclosed in G_1, G_2, and G_3, respectively to the doctor's device.

Step 3: Upon receiving the G_1, G_2, and G_3 from the gateway, the doctor's device begins extracting the challenge $C^{0*}_U = G_1 \oplus D^H_{ID}$, and nonce $N^{1*}_G = G_2 \oplus D^{MCC}_{LN}$. After examining the freshness of N^{1*}_G, doctor's device extracts response from PUF, $R^{0*}_U = P_D(C^{0*}_U)$. Subsequently, the doctor's device calculates $U_1 = h(C^{0*}_U \| N^{1*}_G \| R^{0*}_U)$ and compares with $G_3\{= h(C^0_U \| N^1_G \| R^0_U)\}$. After proving the authenticity, the user device prepares the pseudo-identity of the sensor node $SN^*_{IEI} = h(D^H_{ID} \| D^{MCC}_{LN} \| R^{0*}_U \| N^{1*}_G) \oplus SN_{IEI}$. Thereafter, the doctor device prepares device authentication value, $U_2 = h(C^{0*}_U \| N^{1*}_G \| R^{0*}_U \| TID^0_U)$. N^2_U is also shared secretly with gateway. Finally, $\{U_2, U_3, SN^*_{IEI}\}$ is sent to the gateway.

Step 4: Initially, the gateway derives the $N^2_U = U_3 \oplus D^{MCC}_{LN}$ and evaluates the freshness. If fresh, gateway begins the computation of $G_4 = h(C^0_U \| N^1_G \| R^0_U \| TID^0_U$ and examines the identicalness between U_2 and G_4. The mutual authentication between doctor and gateway gets accomplished if

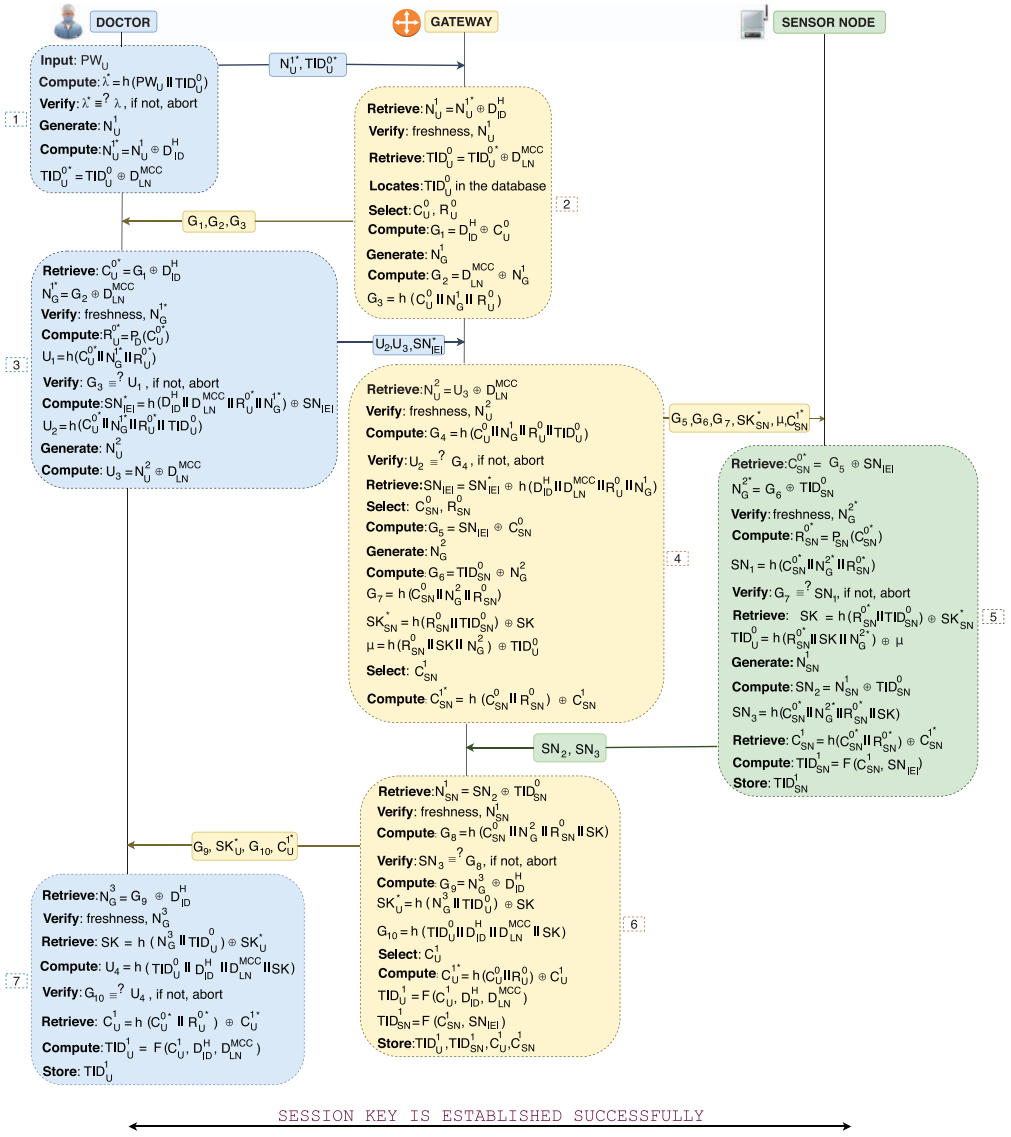

Fig. 4. Lightweight and physically protected MASK establishment protocol for real time data access in IoMT networks.

$U_2 \equiv G_4$, else fails. The gateway afterward extracts the real identity of the sensor node for accomplishing mutual authentication, $SN_{IEI} = SN^*_{IEI} \oplus h(D^H_{ID}\|D^{MCC}_{LN}\|R^0_U\|N^1_G)$. After retrieving SN_{IEI}, the gateway then selects the corresponding C^0_{SN}, R^0_{SN} pair and generates the N^2_G. To ensure privacy, the challenge C^0_{SN} and the nonce N^2_G is secretly enclosed within G_5 and G_6, respectively. Gateway also prepares $G_7 = h(C^0_{SN}\|N^2_G\|R^0_{SN})$ to prove its identity to the sensor node. The gateway calculates SK for the sensor node and enclose it secretly within SK^*_{SN} $(= h(R^0_{SN}\|TID^0_{SN}) \oplus SK)$. Correspondingly, gateway also encloses the TID^0_U within μ $(= h(R^0_{SN}\|SK\|N^2_G) \oplus TID^0_U)$. Finally, gateway selects a random new challenge C^1_{SN} from the set of challenges C^{SYN}_{SN} generated at the time of registration and computes $C^{1*}_{SN} = h(C^0_{SN}\|R^0_{SN}) \oplus C^1_{SN}$. The gateway compose a message consisting of G_5, G_6, G_7, SK^*_{SN}, μ, C^{1*}_{SN} and send it to the sensor node.

Step 5: After receiving $\{G_5, G_6, G_7, SK^*_{SN}, \mu, C^{1*}_{SN}\}$ from gateway, the sensor node retrieves $C^{0*}_{SN} = G_5 \oplus SN_{IEI}$. Then the sensor node calculates $N^{2*}_G = G_6 \oplus TID^0_{SN}$ and examines the freshness of N^{2*}_G. The sensor node extracts the response from the PUF, $R^{0*}_{SN} = P_{SN}(C^{0*}_{SN})$. The sensor node derives $SN_1 = h(C^{0*}_{SN}\|N^{2*}_G\|R^{0*}_{SN})$ and compares $G_7 \equiv^? SN_1$; If authentication is successful, the sensor node determines its session key by calculating $SK = h(R^{0*}_{SN}\|TID^{0*}_{SN}) \oplus SK^*_{SN}$. Likewise, sensor node extracts the $TID^0_U = h(R^{0*}_{SN}\|SK\|N^{2*}_G) \oplus \mu$. Afterward, the sensor node generates the nonce N^1_{SN} and encloses it within SN_2 $(= N^1_{SN} \oplus TID^0_{SN})$. Besides, the sensor node computes $SN_3 = h(C^{0*}_{SN}\|N^{2*}_G\|R^{0*}_{SN}\|SK)$ to accomplish mutual authentication with gateway and also to assure the gateway of correct SK generation. The sensor node retrieves the new challenge $C^1_{SN} = h(C^{0*}_{SN}\|R^{0*}_{SN}) \oplus C^{1*}_{SN}$ provided by the gateway to generate new temporary identity

TID^1_{SN} required for next future session. Once new challenge C^1_{SN} is extracted, the sensor node calculates the $TID^1_{SN} = F(C^1_{SN}, SN_{IEI})$ and stores the new temporary identity for future communication with gateway. At last, the sensor node composes a message $\{SN_2, SN_3\}$ and send it to gateway.

Step 6: Upon receiving SN_2 and SN_3, the gateway starts the retrieval of N^1_{SN} $(= SN_2 \oplus TID^0_{SN})$ and verifies the freshness of N^1_{SN}. After the nonce verification, the gateway computes, $G_8 = h(C^0_{SN} \| N^2_G \| R^0_{SN} \| SK)$ and compares, $SN_3 \equiv^? G_8$. Succeeding verification, the gateway calculates $G_9 = N^3_G \oplus D^H_{ID}$. Thereafter, gateway encloses the session key of the user within $SK^*_U = h(N^3_G \| TID^0_U) \oplus SK$. Then the gateway calculates $G_{10} = h(TID^0_U \| D^H_{ID} \| D^{MCC}_{LN} \| SK)$ to let the user node verify the correct key generation. Post G_{10} computation, the gateway selects a random new challenge C^1_U from the list of challenges C^{SYN}_U constructed during registration. Hence, the gateway encloses the new challenge within C^{1*}_U $(= h(C^0_U \| R^0_U) \oplus C^1_U)$ to ensure confidentiality. Finally, the gateway calculates the fresh $TID^1_U = F(C^1_U, D^H_{ID}, D^{MCC}_{LN})$ and $TID^1_{SN} = F(C^1_{SN}, SN_{IEI})$. The gateway stores the $TID^1_U, TID^1_{SN}, C^1_U, C^1_{SN}$ into the database. The gateway compose a message $\{G_9, SK^*_U, G_{10}, C^{1*}_U\}$ and sends it to doctor's device.

Step 7: The doctor's device receives $\{G_9, SK^*_U, G_{10}, C^{1*}_U\}$ from the gateway and retrieves the nonce $N^3_G = G_9 \oplus D^H_{ID}$ and examines its freshness. Then the device extract session key, $SK = h(N^3_G \| TID^0_U) \oplus SK^*_U$. Upon successful extraction, the device computes $U_4 = h(TID^0_U \| D^H_{ID} \| D^{MCC}_{LN} \| SK)$ and verifies the identicalness between U_4 and G_{10}. Successful verification assures the doctor's device of correct key generation. Finally, the device extracts the new challenge $C^1_U = h(C^{0*}_U \| R^{0*}_U) \oplus C^{1*}_U$ and computes the fresh $TID^1_U = F(C^1_U, D^H_{ID}, D^{MCC}_{LN})$. The doctor's device stores the TID^1_U for future communication with the gateway.

Remark 3: The gateway verifies the TID_U and TID_{SN} and permits only legitimate devices to communicate. To accomplish identity anonymity and untraceability temporary identities TID^0_U and TID^0_{SN} are used. Neither the challenge $\{C^0_U, C^0_{SN}\}$ nor the nonce $\{N^1_U, N^2_U, N^1_G, N^2_G, N^3_G\}$ are disclosed on the public channel, therefore only authorized entities are entitled to retrieve this information. The message (U_2) is sent as a message digest, hence not allows the attacker to interpret and modify despite eavesdropping the G_1, G_3, and TID^{0*}_U. Moreover, the attacker cannot prepare U_2 because he does not know C^{0*}_U, N^{1*}_G, R^{0*}_U, and TID^0_U. The parameter μ creates an association between session key (SK) and (TID^0_U). Identities $\{TID^0_U, TID^0_{SN}\}$ and key (SK) in the proposed protocol are reproduced after the expiry of every session.

```
% OFMC
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/
              results/IoMT.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 1.37s
  visitedNodes: 88 nodes
  depth: 11 plies
```

```
% CL-AtSe
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/
              results/IoMT.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 15 states
  Reachable  : 7 states
  Translation: 0.19 seconds
  Computation: 0.03 seconds
```

Fig. 5. Results obtained from AVISPA using OFMC and CL-AtSe backend.

V. Security Analysis

A. Formal Analysis

We considered the AVISPA tool [21] to examine the strength of the proposed MASK protocol. The protocol is written with the AVISPA-HLPSL script. AVISPA supports four backends, namely, "on-the-fly model-checker (OFMC)," "Constraint-Logic-based Attack Searcher (CL-AtSe)," "SAT-based model-checker (SATMC)," and "Tree Automata tool based on Automatic Approximations for the Analysis of Security Protocols (TA4SPs)." The MASK-HLPSL script contains the description of 3 primary roles, "user," "gateway," and "IoT node." Besides, the environment role defines the various sessions and intruder knowledge. The goals declared in the environment role of MASK protocol are data privacy, freshness, and authentication, etc. As illustrated in Fig. 5, the OFMC backend produced the result as "safe" after visiting 88 nodes with a depth of 11 plies. Likewise, simulation of CL-AtSe took 0.19 s to declare the protocol as safe. The MASK-HLPSL-IF script has been fed to other 2 backends (SATMC and TA4SP) as well, but resulted inconclusive because these backends do not support bitwise XOR operations. Therefore, the results of OFMC and CL-AtSe backends show that MASK protocol is safe from all prominent attacks, including, replay and MITM.

B. Informal Analysis

Theorem 1: Secured from impersonation attacks.

Proof: Consider a scenario where an attacker intercepted the message $G_5, G_6, G_7, SK^*_{SN}, \mu$, and C^{1*}_{SN}. The message contains the identity of user, TID^0_U and secret key, SK but enclosed secretly within $\mu\{= h(R^0_{SN} \| SK \| N^2_G) \oplus TID^0_U\}$ and SK^*_{SN} $\{= h(R^0_{SN} \| TID^0_{SN}) \oplus SK\}$. It is computationally infeasible for the attacker to retrieve TID^0_{SN} and SK from μ and SK^*_{SN} due to collision-resistant property of hash functions [11]. Moreover, every device employing MASK protocol is integrated with unique PUF. The attacker neither know responses generated by the PUF (R^0_U, R^0_{SN}) nor can predict [18]; therefore, the attacker cannot duplicate the identity of the user and sensor node. Hence, the protocol is protected from impersonation attacks. ■

Theorem 2: Resistant to MITM attacks.

Proof: Assuming that adversary has captured the message $\{U_2, U_3, SN^*_{IEI}\}$. Now, the adversary can try to modify the message to execute MITM but will be unsuccessful to make any modifications since the information in the messages $U_2 = h(C^{0*}_U \| N^{1*}_G \| R^{0*}_U \| TID^0_U)$, $U_2 = N^2_U \oplus D^{MCC}_{LN}$, and $SN^*_{IEI} = h(D^H_{ID} \| D^{MCC}_{LN} \| R^{0*}_U \| N^{1*}_G) \oplus SN_{IEI}$ are processed through one-way hash function and bitwise XOR operation. The collision resistant property of hash functions [11] restrict the attacker to either predict or revive the challenge (C^{0*}_U), response (R^{0*}_U), identity ($TID^0_U, D^{MCC}_{LN}, D^H_{ID}, SN_{IEI}$), and nonce ($N^{1*}_G, N^2_U$) values. Hence, the messages of the MASK protocol are safe from MITM attacks. ■

Theorem 3: Protection against physical attacks.

Proof: Assume that an attacker has physically captured the sensor node. The attacker aims to prepare a clone or steal information from the chip of the sensor node. The MASK protocol integrates the user device and sensor node with the PUF. Since the output of the PUF $\{R^0_U = P_D(C^0_U), R^0_{SN} = P_{SN}(C^0_{SN})\}$ depends upon the intrinsic physical variations in the IC, hence any attempt to tamper with the PUF would destroy the unique characteristics of the device and render the PUF useless [11]. Consequently, the protocol is safe against cloning and side-channel attacks. ■

Theorem 4: Exhibits data privacy.

Proof: Assume an adversary has captured the message $G_9, SK^*_U, G_{10}, C^{1*}_U$ to extract the useful information. G_9 is composed of (N^3_G) and (D^H_{ID}); the attacker will not be able to retrieve the real nonce (N^3_G) as (D^H_{ID}) is never disclosed openly. Similarly $G_{10} = h(TID^0_U \| D^H_{ID} \| D^{MCC}_{LN} \| SK)$, $SK^*_U = h(N^3_G \| TID^0_U) \oplus SK$, and C^{1*}_U ($= h(C^0_U \| R^0_U) \oplus C^1_U$) are computed using secret values and one way hash function. Therefore, the information in the message remains confidential. ■

Theorem 5: Attainment of user and sensor node identity anonymity and untraceability.

Proof: Imagine an adversary has captured the message $\{N^{1*}_U, TID^{0*}_U\}$ to extract the identity details (D^H_{ID}, D^{MCC}_{LN}) of the user. Despite successful capturing, the adversary can not reveal (D^H_{ID}, D^{MCC}_{LN}) since it is never used during mutual authentication and key agreement phase. During the registration phase, the gateway generates the temporary identity of the sensor node TID^0_{SN} and user device TID^0_U for future correspondence. Moreover, the temporary identity is further transformed into pseudo-identity during the mutual authentication for enhanced security. The user device sends the pseudo-identity of sensor node $SN^*_{IEI} = h(D^H_{ID} \| D^{MCC}_{LN} \| R^{0*}_U \| N^{1*}_G) \oplus SN_{IEI}$ and itself $TID^{0*}_U = TID^0_U \oplus D^{MCC}_{LN}$ while communicating with the gateway. Hence, the real identities of the sensor node and user device are never disclosed, thus keeping the communication anonymous. Moreover, the temporary identities $TID^0_U = F(C^0_U, D^H_{ID} D^{MCC}_{LN})$, $TID^0_{SN} = F(C^0_{SN}, SN_{IEI})$ changes every session due to change in input challenge ($C^1_U, C^2_U, \ldots, C^N_U; C^1_{SN}, C^2_{SN}, \ldots, C^N_{SN}$), thus ensuring untraceability of user device and sensor node. ■

VI. Performance and Comparative Analysis

The MASK protocol has been tested considering CM5000 TelosB mote with specifications as TI MSP430F1611 micro-controller, CC2420 RF chip, memory 1 MB, and a power source of $3V$ ($2 \times AA$ battery) [30]. The results shows that MASK protocol uses only 0.0008% of total memory space available in CM5000 TelosB mote (1 MB), whereas the schemes [10], [23], [24] require 0.036%, 0.027%, and 0.015% of the storage space, respectively. Hence, the MASK protocol needs very little storage space than the conventional protocols [10], [23], [24].

Table II shows that MASK protocol ensures data privacy, identity anonymity, untraceability, integrity, freshness, and session key security. The MASK protocol also is guarded against impersonation, modification, MITM, replay, cloning, and side-channel attacks. Meanwhile, the conventional approaches [10], [16], [21]–[25] do not guarantee data privacy and untraceability. Moreover, these schemes are also vulnerable to side-channel and cloning attacks. Also, the

TABLE II
Comparison of MASK Protocol Versus Conventional Protocols

$\mathcal{S}_\mathcal{G}$	[10]	[16]	[18]	[21]	[22]	[23]	[24]	[25]	$\mathcal{M}$
$\mathcal{P}_1$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{P}_2$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{P}_3$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{P}_4$	✓	×	×	✓	×	×	✓	×	✓
$\mathcal{P}_5$	✓	×	✓	✓	×	✓	✓	×	✓
$\mathcal{P}_6$	✓	✓	✓	×	×	✓	✓	✓	✓
$\mathcal{P}_7$	×	×	✓	×	×	×	×	×	✓
$\mathcal{P}_8$	×	×	✓	×	×	×	×	×	✓
$\mathcal{P}_9$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{P}_{10}$	✓	×	×	✓	×	×	×	×	✓
$\mathcal{P}_{11}$	✓	✓	✓	✓	×	×	✓	✓	✓
$\mathcal{P}_{12}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{P}_{13}$	✓	✓	✓	✓	✓	✓	✓	×	✓
$\mathcal{P}_{14}$	*	✓	✓	✓	✓	*	✓	✓	✓
$\mathcal{P}_{15}$	✓	×	✓	×	×	✓	×	×	✓
$\mathcal{P}_{16}$	*	×	✓	✓	✓	*	✓	✓	✓
$\mathcal{P}_{17}$	×	×	✓	×	×	×	×	×	✓

Acronyms: $\mathcal{S}_\mathcal{G}$: Security goals, $\mathcal{M}$: MASK protocol, ✓: Secure against attack/preserves a security attribute, ×: Vulnerable/non accomplishment of security attribute, *: Not applicable, $\mathcal{P}_1$: Replay, $\mathcal{P}_2$: Impersonation, $\mathcal{P}_3$: Modification of messages, $\mathcal{P}_4$: DoS, $\mathcal{P}_5$: MITM, $\mathcal{P}_6$: Known key, $\mathcal{P}_7$: Cloning, $\mathcal{P}_8$: Side-channel, $\mathcal{P}_9$: Mutual authentication, $\mathcal{P}_{10}$: Data privacy, $\mathcal{P}_{11}$: Session key security, $\mathcal{P}_{12}$: Message integrity, $\mathcal{P}_{13}$: Message freshness, $\mathcal{P}_{14}$: User identity anonymity, $\mathcal{P}_{15}$: Sensor node identity anonymity, $\mathcal{P}_{16}$: User untraceability, $\mathcal{P}_{17}$: Sensor node untraceability

TABLE III
Communication Cost of Sensor Node

Scheme	Cost (bits)	Cost (μJ)
[10]	720	519
[16]	912	703
[18]	1792	1405
[21]	864	653
[22]	960	748
[23]	1024	772
[24]	912	738
[25]	960	733
MASK	832	656

TABLE IV
COMPUTATION COST OF MASK PROTOCOL

Phase	User Device	Gateway	Sensor Node	Total Cost
Registration	$2\ C_H + 2\ C_{PUF}$	$2\ C_H$	$C_H + 2\ C_{PUF}$	$5\ C_H + 4\ C_{PUF}$
Key Establishment	$7\ C_H + C_{PUF} + 9\ C_{XOR}$	$11\ C_H + 15\ C_{XOR}$	$5\ C_H + C_{PUF} + 6\ C_{XOR}$	$23\ C_H + 2\ C_{PUF} + 15\ C_{XOR}$
Total Cost	$9\ C_H + 3\ C_{PUF} + 9\ C_{XOR}$	$13\ C_H + 15\ C_{XOR}$	$6\ C_H + 3\ C_{PUF} + 6\ C_{XOR}$	$28\ C_H + 6\ C_{PUF} + 15\ C_{XOR}$

Acronyms: C - Computation, C_H - Computation of Hash, C_{PUF} - Computation of Physically Unclonable Function, C_{XOR} - Computation of Bit-wise XOR, *Integers* - defines the frequency of operation.

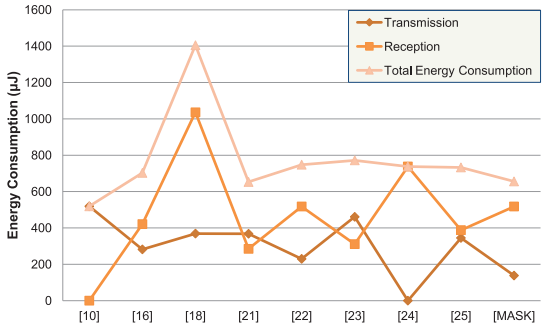

Fig. 6. Energy cost comparison.

scheme in [18] does not protect against DoS attacks. Hence, their deployment in a hostile environment can pose threats to the entire network.

The TelosB mote [30] consumes $0.72\,\mu J$ and $0.81\,\mu J$ of energy [3], [9], [10] while transmitting and receiving, respectively. Table III provides the number of bits (T_X/R_X) and the quantity of energy consumption (μJ) by a sensor node during the mutual authentication and key establishment phase. Note that the registration phase is excluded since it executes only once during network set-up. Table III shows that MASK protocol uses the resources of sensor node efficiently than the traditional approaches [16], [18], [22]–[25]. The schemes [10], [21] though they consume less energy than the proposed protocol, are insecure because these schemes neither prevent physical attacks nor ensure untraceability. Hence, the approaches [10], [16], [18], [21]–[25] in IoMT networks can result in unexpected adverse consequences. Fig. 6 depicts the amount of energy spent by a sensor node for transmission and reception during the mutual authentication and key establishment phase. It is noticeable that the MASK protocol's sensor node consumes the least energy during transmission and affordable energy while reception. Thus, the energy-efficient characteristics of the MASK protocol makes it superior in comparison to other existing protocols.

Table IV shows that the MASK protocol is computationally efficient. It employs only lightweight operations, such as hash, PUF, and XOR rather than bulky cryptography operations like asymmetric and symmetric ciphers, scalar multiplications, and fuzzy extractors. Table V compares the computation cost of the MASK and other conventional protocols during the mutual authentication and key agreement phase. The scheme proposed by Gope *et al.* [18] executed the PUF 5 times, whereas the MASK protocol only does it twice. Moreover, the scheme in [18] uses the fuzzy extractor to retrieve biometrics, whereas the MASK protocol does not use any biometrics. The

TABLE V
COMPUTATION COST COMPARISON OF MASK PROTOCOL VERSUS CONVENTIONAL PROTOCOLS

Scheme	Computation Cost
[10]	$C_{AE} + 3\ C_{AD} + 2\ C_H + 2\ C_M + 2\ C_{XOR}$
[16]	$18\ C_H + 9\ C_{XOR} + 2\ C_R$
[18]	$22\ C_H + 5\ C_{PUF} + 16\ C_{XOR} + 3\ C_R + C_B$
[21]	$37\ C_H + 16\ C_{XOR} + 2\ C_R + C_B$
[22]	$4\ C_{SE} + 4\ C_{SD} + 19\ C_H + 14\ C_{XOR} + 4\ C_R + C_B + 3\ C_{SM}$
[23]	$15\ C_H + 10\ C_{XOR} + 2\ C_R$
[24]	$25\ C_H + 20\ C_{XOR} + 3\ C_R + 9\ C_{MOD}$
[25]	$18\ C_H + 9\ C_{XOR} + 3\ C_R + C_B + 6\ C_{SM}$
MASK	$23\ C_H + 2\ C_{PUF} + 15\ C_{XOR} + 6\ C_R$

Acronyms: C - Computation, C_{AE} - Computation of asymmetric encryption, C_{AD} - Computation of asymmetric decryption, C_H - Computation of Hash, C_{SE} - Computation of symmetric encryption, C_{SD} - Computation of symmetric decryption, C_M - Computation of hash based MAC, C_R - Computation of random number, C_{PUF} - Computation of Physically Unclonable Function, C_B - Computation of bio-metric, C_{MOD} - Computation of modulus, C_{XOR} - Computation of Bit-wise XOR, C_{SM} - Computation of Scalar Multiplication, *Integers* - defines the frequency of operation.

approaches developed by Gaba *et al.* [10] and Li *et al.* [22] utilized asymmetric and symmetric ciphers that overburden the tiny processor of the sensor node. The other protocols designed by Das *et al.* [21], Li *et al.* [25], and Paliwal [24] are also computing expensive since they calculate biometrics, scalar multiplications, and modulus, respectively. Besides, the approaches in [21] and [24] also make excessive use of hash and XOR operations. The protocols [16], [23] have reasonable computation complexity. However, it is achieved at the cost of compromised security. The schemes in [16] and [23] are vulnerable to DoS, cloning, and side-channel attacks and fail to provide data privacy and sensor node untraceability. Additionally, the approaches [16], [23] are communication expensive as well. Fig. 7 demonstrates the computation cost spent by a user, gateway, and sensor node in MASK protocol and also compares it with other protocols. From Fig. 7, it is clear that the MASK protocol has attained all essential security properties with very reasonable communication and computation cost.

The vertical bars in Fig. 8 illustrates the total number of messages exchanged by the sensor node throughout the protocol. The diamond tag in the bar indicates the number of messages exchanged by the sensor node during the MASK establishment phase. The resource-constrained sensor node employing MASK protocol exchanges an equal number of messages as in other protocols. Hence, computation is

Fig. 7. Computation cost of user (topmost), gateway (middle), and sensor node (bottom-most) of MASK protocol versus conventional protocols.

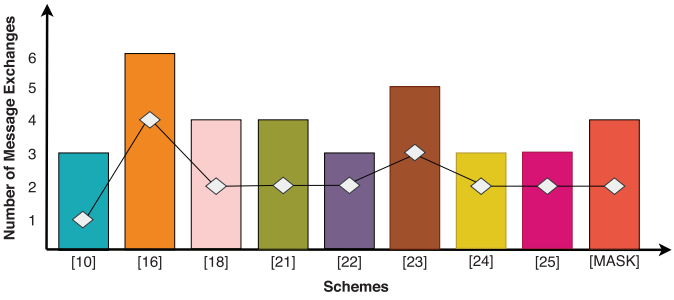

Fig. 8. Communication cost comparison.

inexpensive. The sensor nodes in the schemes [16] and [21] exchange 3 and 4 messages, respectively, which is more than the MASK protocol. The number of message exchanges is also a performance metric to select a particular application protocol because more messages lead to more delay, overhead, and energy exhaustion. Therefore, the MASK protocol is more robust and lightweight compared to the state-of-the-art protocols.

VII. Conclusion

This article has introduced a robust and lightweight security protocol to provide MASK establishment between doctor and sensor node. We evaluated the strength of the MASK protocol through formal and informal security analysis. The performance analysis has proven the capability of MASK protocol to protect the sensor node from physical and other prominent attacks. MASK protocol consumes only 656 μJ of energy and 0.0008% of tiny node memory. The comparison shows that the MASK protocol outperforms the other conventional protocols to prevent attacks, computation and communication efficiency, and so forth. In the future, the MASK protocol may be extended for those hostile environments where network devices like gateways are also subjected to physical attacks.

References

[1] H. Lin, S. Garg, J. Hu, X. Wang, Md. J. Piran, and M. S. Hossain "Privacy-enhanced data fusion for covid-19 applications in intelligent Internet of Medical Things," *IEEE Internet Things J.*, early access, Oct. 22, 2020, doi: 10.1109/JIOT.2020.3033129.

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

[3] 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.

[4] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and privacy for the Internet of Medical Things enabled healthcare systems: A survey," *IEEE Access*, vol. 7, pp. 183339–183355, 2019.

[5] 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.

[6] M. Masud, M. S. Hossain, and A. Alamri, "Data interoperability and multimedia content management in e-health systems," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1015–1023, Nov. 2012.

[7] G. Muhammad, M. S. Hossain, and N. Kumar, "EEG-based pathology detection for home health monitoring," *IEEE J. Sel. Areas Commun.*, early access, Aug. 31, 2020, doi: 10.1109/JSAC.2020.3020654.

[8] 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.

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

[10] 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.

[11] P. Gope, J. Lee, and T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2831–2843, Nov. 2018.

[12] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, and S. Elmougy, "Secure quantum steganography protocol for fog cloud Internet of Things," *IEEE Access*, vol. 6, pp. 10332–10340, 2018.

[13] H.-R. Tseng, R.-H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *Proc. IEEE GLOBECOM IEEE Global Telecommun. Conf.*, 2007, pp. 986–990.

[14] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009.

[15] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks,'" *Sensors*, vol. 10, no. 3, pp. 2450–2459, 2010.

[16] 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.

[17] 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.

[18] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 9, pp. 4957–4968, Sep. 2019.

[19] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011.

[20] M. S. Hossain, G. Muhammad, S. Md M. Rahman, W. Abdul, A. Alelaiwi, and A. Alamri, "Toward end-to-end biomet rics-based security for IoT infrastructure," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 44–51, Oct. 2016.

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

[22] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K.-K. R. Choo, "A robust and energy efficient authentication protocol for industrial Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1606–1615, Jun. 2018.

[23] A. Esfahani *et al.*, "A lightweight authentication mechanism for M2M communications in industrial IoT environment," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 288–296, Feb. 2019.

[24] S. Paliwal, "Hash-based conditional privacy preserving authentication and key exchange protocol suitable for industrial Internet of Things," *IEEE Access*, vol. 7, pp. 136073–136093, 2019.

[25] 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. Informat.*, vol. 14, no. 8, pp. 3599–3609, Aug. 2018.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] S. Fajarado. (2010). *CM5000 Datasheet*. Accessed: Feb. 15, 2020. [Online]. Available: http://www.epssilon.cl/files/EPS5000.pdf