Computer Communications 196 (2022) 45–54

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

A user-centric privacy-preserving authentication protocol for IoT-AmI environments

Mehedi Masud [a,1], Gurjot Singh Gaba [b,*,1], Pardeep Kumar [c], Andrei Gurtov [b]

[a] Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia
[b] Department of Computer and Information Science (IDA), Linköping University (LiU), Linköping 58183, Sweden
[c] Department of Computer Science, Swansea University, Swansea SA1 8EN, UK

ARTICLE INFO

Keywords:
Ambient intelligence
Blockchain
Fog computing
Healthcare
Internet of Things (IoT)

ABSTRACT

Ambient Intelligence (AmI) in Internet of Things (IoT) has empowered healthcare professionals to monitor, diagnose, and treat patients remotely. Besides, the AmI-IoT has improved patient engagement and gratification as doctors' interactions have become more comfortable and efficient. However, the benefits of the AmI-IoT-based healthcare applications are not availed entirely due to the adversarial threats. IoT networks are prone to cyber attacks due to vulnerable wireless mediums and the absentia of lightweight and robust security protocols. This paper introduces computationally-inexpensive privacy-assuring authentication protocol for AmI-IoT healthcare applications. The use of blockchain & fog computing in the protocol guarantees unforgeability, non-repudiation, transparency, low latency, and efficient bandwidth utilization. The protocol uses physically unclonable functions (PUF), biometrics, and Ethereum powered smart contracts to prevent replay, impersonation, and cloning attacks. Results prove the resource efficiency of the protocol as the smart contract incurs very minimal gas and transaction fees. The Scyther results validate the robustness of the proposed protocol against cyber-attacks. The protocol applies lightweight cryptography primitives (Hash, PUF) instead of conventional public-key cryptography and scalar multiplications. Consequently, the proposed protocol is better than centralized infrastructure-based authentication approaches.

1. Introduction

The Healthcare industry is being revolutionized with the tremendous progress in digital technologies, along with the IoT [1,2]. The healthcare industry is being transformed to the advanced level when people, apps, sensors, and medical devices communicate when delivering healthcare solutions [3,4]. IoT-driven drones, smart wearable devices, and health monitoring systems are considered to advance the healthcare industry's development [5]. The requirement to acquire, preserve and study patient information has advanced the healthcare industry to consider numerous trending digital technologies. The increasing acceptance of AmI-IoT in healthcare and health domains has evolved the latest systems, i.e., the Internet of Medical Things (IoMT) [6]. It decreases human mistakes and eradicates many decision-making delays. Some of the significant benefits of accepting IoT in the ambient Healthcare environments are real-time monitoring, improved patient experience, and cost minimization. Leveraging IoT-based systems and medical devices permits the clinician to monitor the patient remotely with real-time data that expedites the diagnosis and treatment and provides advantages, such as persistent communication, travel expenses, and diminishes hospital resources.

In the healthcare industry, the AmI-IoT is considered for interrelated healthcare entities/devices like patients' observing systems, sensor-based equipment, and sensor devices that acquire real-time health data. In *healthcare* 1.0, the doctors diagnosed the patients in person and maintained records on papers, whereas in *healthcare* 2.0, the doctors processed the patient's information as *electronic health records* (EHR). *Healthcare* 3.0 transformed the paradigm of medical diagnosis by introducing internet-enabled wearable devices, telemedicine, etc. *Healthcare* 4.0 uses a range of technologies like the IoT, UAVs, augmented reality (AR), artificial intelligence (AI), deep learning (DL), and natural language processing (NLP) to optimize and automate medical procedures [7,8].

IoT is a world of connected objects [9]. It is predicted that by the year 2030, the total number of connected devices would be around 24 billion [10]. IoT nodes are tiny in size and have limited storage, less power, and limited computation capabilities. Fig. 1 illustrates the smart

* Corresponding author.
E-mail addresses: mmasud@tu.edu.sa (M. Masud), gurjot.singh@liu.se (G.S. Gaba), pardeep.kumar@swansea.ac.uk (P. Kumar), andrei.gurtov@liu.se (A. Gurtov).
[1] These authors contributed equally to this work.

https://doi.org/10.1016/j.comcom.2022.09.021
Received 27 June 2022; Received in revised form 3 September 2022; Accepted 19 September 2022
Available online 28 September 2022

Fig. 1. Smart healthcare using IoT and aerial networks.

healthcare system using IoT, where objects are controlled and monitored in real-time through the internet, *e.g.*, automatic gate opening for ambulances, UAVs delivering human organs, and remote ordering of medicines and meals from pharmacy and pantry, respectively. Besides, the IoMT helps doctors and other authorized caretakers control the pressure of the ventilator, rate, and rhythm of the pacemaker remotely and generate the faulty medical equipment's alerts. In the recent COVID-19 situation, lockdowns and social distancing are the prime factors behind the rapid adoption of IoT by healthcare institutions.

1.1. Literature review

This section elaborates on the various authentication schemes developed to protect the AmI-IoMT networks. A mutual authentication approach for sensor networks was developed by Deebak [11], which was later found vulnerable [12]. Inspired by Deebak, Chen et al. [13] extended Deebak's approach [11]; however, Xu et al. discovered that the scheme was prone to replay and impersonation attacks [14]. Wang [15] constructed elliptic curve cryptography (ECC) based mutual authentication approach to counter password guessing and verifier attacks. Odelu et al. did cryptanalysis on Wang's approach and found it susceptible to cyber-threats [16]. Similarly, Turkanovic et al. [17] designed a user authentication and key establishment scheme for a resource-constrained ecosystem. However, both Farash [18], and Chang [19] found Turkanovic et al.'s scheme as insecure. Chang et al. [19] also attempted to devise privacy-preserving authentication and key agreement protocol, but Gope et al. [20] found it resource expensive and susceptible to traceability. Das et al. suggested a fuzzy extractor and smart card-based user authentication approach, whereas Li et al. introduced a biometric and password-based user legitimacy verification method; however, both the schemes have never been tested in hostile circumstances and are computationally expensive.

1.2. Research gap and motivation

The integration of AmI-IoMT has significantly transformed healthcare. The new paradigm enables the patient to communicate remotely with the doctor, hence saving resources and reducing strain on healthcare facilities. Despite the fact that IoMT is advantageous, cyber analysts believe that it could put patients' and medical specialists' lives in danger [21]. Based on the literature, IoMT networks are susceptible to attacks due to: (*i*) use of an insecure wireless medium, (*ii*) absentia of strong cryptography solutions due to *limited power*, memory, and processing capability [22], and (iii) the lack of cyber knowledge to end-users (medical practitioners), hence falling prey to attackers. Health-related information is sensitive, thus requires privacy [23]. Besides, integrity is also a very important aspect because a minor alteration by the attacker in the diagnosis report could result in a patient's different medication. As many medical technologies support automation, any malicious activity could trigger a detrimental action resulting in unprecedented outcomes.

Cybersecurity specialists presented a variety of methods to mitigate vulnerabilities and threats, including public key and lattice-based encryption, digital signatures, and so on. However, most recommended approaches have been found vulnerable to attacks in addition to being resource intensive. Despite the existence of conventional approaches, medical institutions and stakeholders got affected severely; 41.2 million records were compromised, whereas 2013 breaches were recorded from 86 countries in 2019. Moreover, the existing security solutions are more or less centralized that may not work well for a geographically vast and large IoT ecosystem [24]. Furthermore, centralized solutions have a single point of failure, decreased efficiency for larger networks, and notable delay [25,26]. Blockchain is coined as a solution by security practitioners because it works on *decentralized* and *geographically distributed* technology with attributes such as immutability, transparency, and fault tolerance [27]. In summary, security and privacy in AmI-IoT networks can be ensured by implementing robust authentication and key exchange mechanisms using blockchain [28,29].

1.3. Research contributions

The following are our contributions:

- We identify vulnerabilities and research gaps in the AmI-IoT healthcare ecosystem.
- We propose a decentralized and lightweight authentication framework based on Ethereum smart contracts, fog computing, PUF, and biometrics.
- We investigate the robustness of the proposed framework in hostile situations to demonstrate its applicability to sensitive medical applications.
- We calculate the transaction costs of smart contracts to evaluate the framework's appropriateness for resource-constrained environments.

1.4. Paper organization

The remaining structure of the paper is as follows: Section 2 discusses the preliminaries required for the proposed protocol. Section 3 explains the working scenario of the proposed protocol. Section 4

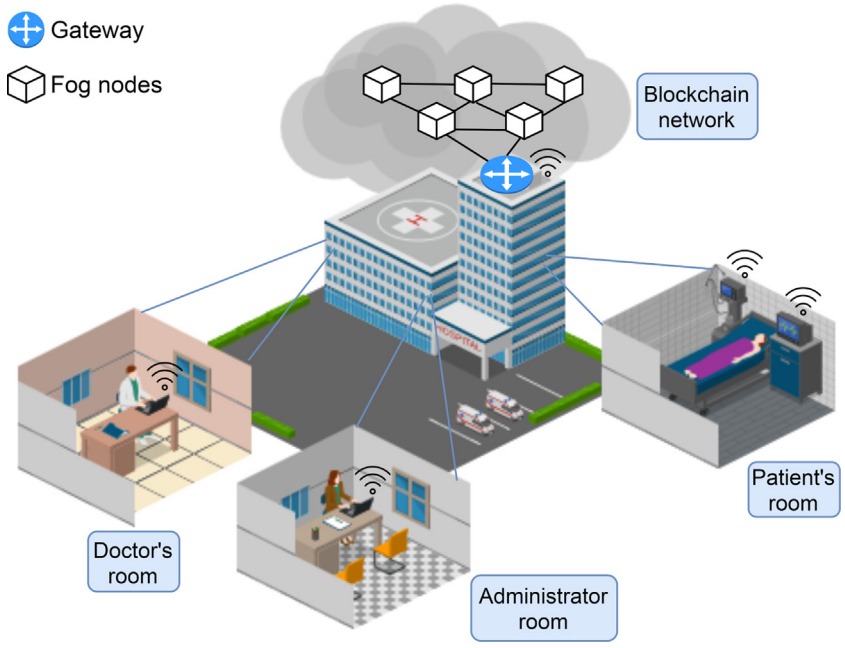

Fig. 2. System model depicting the communication between user, administrator, IoT sensor node, gateway, and the blockchain fog nodes.

justifies the robustness of the protocol through formal security analysis. Section 5 shows the results and discusses comparison analysis. Section 6 concludes the paper and highlights the future scope.

2. Preliminaries

2.1. System model

Fig. 2 illustrates the scenario of a *smart healthcare institution* where *stakeholders* (doctor, administrator, etc.) use digital *gadgets* (laptop, etc.) to access the internet-enabled wireless sensor nodes embedded on the medical appliances and patients' body (e.g., pacemaker) [30]. The *administrator* has the responsibility to register the legitimate staff members and the IoT sensor nodes (e.g., drones) in the blockchain network. A *user* can be any staff member of the healthcare institution with interest to access the medical reports and appliances [31]. On the contrary, the *IoT sensor nodes* (e.g., Zigbee-IEEE 802.15.4) are tiny in size and have limited computation abilities but powerful enough to sense the physical environment and relay the information to the user through the gateway [32]. The healthcare institution has deployed a resource-abundant *network gateway* (supports IEEE 802.3 and IEEE 802.11) with the prime responsibility to facilitate communications between user, administrator, IoT sensor node, and blockchain network. To reduce the computation burden, *blockchain fog nodes* (BFN) are deployed to provide a decentralized authenticity verification framework [33].

2.2. Adversary model

The *adversary model* aka *attacker model* describes the various possible threats and the resulting risks that arise due to cyber attacks [34]. According to the *Dolev–Yao* (DY) model, a cyber adversary is capable of eavesdropping, replaying, cloning, intercepting, injecting, phishing, modifications, malware, impersonation, privilege escalation, and man-in-the-middle attacks. The implications of cyber-threats in the IoMT environment depends on the attack duration and application sensitivity. Most often, the organization and affected parties incur financial losses, reputational harm, legal ramifications, and intellectual property theft. These threats could result in benign (temporary shutdown of medical services) to severe (endangering patients lives) impact on medical IoT networks.

2.3. Goals

This section discusses the goals of the proposed security protocol. The protocol must prohibit unauthorized access and prevents cloning. Besides, the protocol must be robust to resist notable cyberattacks, e.g., man-in-the-middle, replay, impersonation, etc. [35]. The protocol should only permit legitimate entities to initiate the session, and establish session keys to attain confidentiality. Most importantly, the authentication framework should not rely on a single server. Instead, it should be decentralized to prevent physical and denial of service attacks. These security goals must be tied to an efficiency goal, i.e., computations and communications required to achieve the security goals must not be enormous [36].

2.4. Physical unclonable function (puf)

The traditional authentication protocols are computationally expensive due to the use of public-key cryptography. Besides, these protocols also demand storage space in tiny user and IoT devices [19]. As the IoT nodes and user devices are subjected to physical capturing, it is necessary to protect them from cloning attacks. PUF provides a robust and resource economical solution to resist hardware threats. PUF enables the devices to prove their legitimacy without complex computations and storage requirements. A *nanoscale variation* during manufacturing makes every PUF of the integrated circuit (IC) unique. Mathematically, PUF can be defined as, $R = P(C)$. It is apparent from the expression that the output *response* of the PUF depends upon the input *challenge* and the device executing it. It is noteworthy that any physical tampering with the PUF would destroy its original attributes [37].

2.5. Blockchain

It is a technology proposed by *Satoshi Nakamoto* (pseudonym) for enabling peer-to-peer (decentralized) secure transactions [38,39]. The blockchain information is stored in the form of transactions that are further contained in blocks [40]. The block consists of various elements, to name a few, timestamp, transaction details, gas consumed, current hash, parent hash, and nonce, etc. whereas, each transaction comprises transaction hash, timestamp, transaction fee, nonce, and input data, etc. The nodes of the network follow the *consensus* (e.g., proof of work

Table 1
Notations and descriptions.

Notation	Description	Notation	Description
UR_{req}	Registration request by user	U_{ide}, S_{CU}	Real identity of user, smart contract for users
M_{XY}	Message exchange between X and Y	SN_{ID}^{IoT}, SC_{SN}	Real identity of sensor node, smart contract for sensor nodes
U, G, A	User, gateway, administrator	B, S, M_A	Blockchain network, sensor node, miner address
N_U, N_G, N_{SN}	Nonce generated by, U, G, S	PI_U, PI_{SN}	Pseudo-identity of user and sensor node
S_1, S_2	Extracted and helper string	α, γ, θ Φ, β, ω, Δ	Greek characters as variable
B_{adm}^{pub}	BC address of A alias public key	ψ, η, δ, μ, B_{adm}^{pri}	Greek characters are variable, BC private key of A
$\|$, $\equiv$	Concatenation & comparison operator	T_H, T_S, B_L, C_C	Transaction hash, timestamp, block, contract creator
h, $\oplus$	Hash function & bitwise XOR operator	C_A, T_F, T_G	Contract address, transaction fee, gas used in transaction
C_N, P_N, R_N	Challenge, Response, PUF: Device 'N'	AS, CT	Authentication successful, connection termination
Gen(Bio), *Rep*(Bio)	Generate and reproduce biometric	Res_C, SK, G_S	Response code, secret session key, gateway secrets

(PoW), proof of stake (PoS)) to decide the acceptance or rejection of the transactions. Each new transaction includes the hash of the previous block, establishing a relationship between transactions (chain). Few properties that make the blockchain robust and the most reliable are unforgeability, non-repudiation, resilience, and transparency [41].

2.6. Smart contract

The smart contract is a concept similar to physical contracts but in digital form. Smart contracts establish a binding between untrusted and unknown parties; smart contracts are scripted and stored in the blockchain network as transactions [42,43]. Unlike centralized approaches, smart contracts do not require a mediator for binding and execution, which eliminates third-party expenses and facilitates dispute-free transactions. It has several benefits over conventional physical contracts, like immutability, speedy execution, real-time access, inexpensive, immense precision, etc. This concept is originally introduced by *ethereum* (ETH) to use the decentralized characteristics of blockchain for purposes other than cryptocurrencies. The cost to deploy the smart contract is measured in terms of *gas* (units, wei) wherein *wei* is *one quintillionth* of an *ether* (1 wei = 10^{-18} ether).

2.7. Fog computing

Conventionally, centralized infrastructure is used to validate the authenticity of communicating entities. But it is encountered that vulnerability in a centralized server could compromise the entire network. Therefore, decentralized blockchain technology is introduced as the potential solution to the problem. However, certain challenges like *time delay* and *computation requirements* became a hurdle for its deployment in IoT and aerial networks. To overcome the hurdle, *fog computing* is proposed. Fog computing is a decentralized infrastructure deployed near the network location to perform the computations on behalf of resource-deprived nodes [44]. The other few benefits of fog computing are *low latency* and*efficient bandwidth utilization*.

3. Proposed scheme

This section proposes a mutual authentication and secret key establishment process to ensure the security and privacy of the AmI-IoMT networks. The notations used in this paper to describe the protocol's working are listed in Table 1.

3.1. Assumptions

- The micro-controller of the user device and the IoT sensor node is connected to the PUF; it is infeasible to tamper the connection between micro-controller and PUF [20].
- IoT nodes, user-, and network-devices can administer cryptography processes.
- The user device and IoT sensor node are resource-constrained, unlike resource-abundant gateway and BFN.
- The gateway is a tamper-proof and trusted network device; likewise, BFN is trusted and genuine.
- Due to antagonistic conditions, IoT sensor nodes, and user devices are subjected to physical capturing.
- The administrator is honest, and his activities are lawful.

3.2. User registration phase

A user (doctor, nurse, etc.) interested in accessing the IoT medical network has to register himself at the healthcare organization. The entire registration method is described in Fig. 3 and disclosed as follows:

Step 1: The user device (UD) prepares the message M_{UA}^1 ($= UR_{req} \| U_{ide}$) comprising of registration request (UR_{req}) and institute provided unique identity (U_{ide}) and delivers it to admin. It is worth noting that the user and admin communicate through a secure channel [6] during the registration process.

Step 2: The admin receives the request and store the U_{ide} into its device memory (DM). Subsequently, the admin prompts a challenge (C_U) to the PUF of the UD.

Step 3: UD generates the response, $R_U = P_U(C_U)$ for a given challenge. Subsequently, the biometric credentials of the user {Gen(Bio) = (S_1, S_2)} are generated and stored. Further, UD computes $\alpha = h(S_1 \| U_{ide})$ and send $\alpha \| R_U$ to the admin.

Step 4: Upon receipt of M_{UA}^3, admin stores α, C_U, R_U into its DM and develop a smart contract (SC) as shown in Fig. 4, SC_U^1 to register users on the blockchain network (BN). Admin also prepares a message digest (MD) of R_U for later use. Admin applies its digital signature, Z = E(B_{adm}^{pri}, SC_U^1), to counter forgery while deploying SC into the BN. Remarkably, the admin and BN exchange information via a public (insecure) channel [6] during the registration process.

Step 5: Miners in the BN decrypts D(B_{adm}^{pub}, Z) and deploys the SC, SC_U^1. Upon successful deployment (transaction), miner reverts to the admin with these details $T_H^1, T_S^1, B_L^1, C_C^1, C_A^1, T_F^1, T_G^1, M_A^1$.

Step 6: Admin verifies M_{AB}^2 and stores the transaction hash (T_H^1), and contract address (C_A^1) into its DM. Admin constructs a message $E(B_{adm}^{pri}, \alpha \| t \| C_A^1)$ to add credentials of user and its device into the SC.

Step 7: Miners decrypt the message D(B_{adm}^{pub}, V) and adds the user (α) and device (t) credentials into the SC_U^1 with address C_A^1. Blockchain nodes verify the identity of user from the existing legitimate list in SC_U^1, in case of coherence, blockchain nodes returns an error, otherwise it is stored as transaction. Upon transaction, blockchain nodes send these details $\{T_H^2, T_S^2, B_L^2, M_A^2, T_F^2, T_G^2, C_A^1, C_C^1\}$ to the admin.

Step 8: Admin retrieves the transaction details from M_{AB}^4 and stores T_H^2 into its DM. Finally, the admin generates the pseudo-identity (PI_U^1) for anonymity and gateway secret (G_S^1) for mutual authentication and send it to the user as M_{UA}^4.

Step 9: User stores the T_H^2, C_A^1, PI_U^1, G_S^1 for future use.

3.3. IoT sensor node registration phase

The admin enrolls the IoT sensor nodes (ISN) to declare them *authentic*. The registration helps the gateway to allow only authorized ISN to interact with the user. The whole manner is depicted in Fig. 5 and demonstrated as follows:

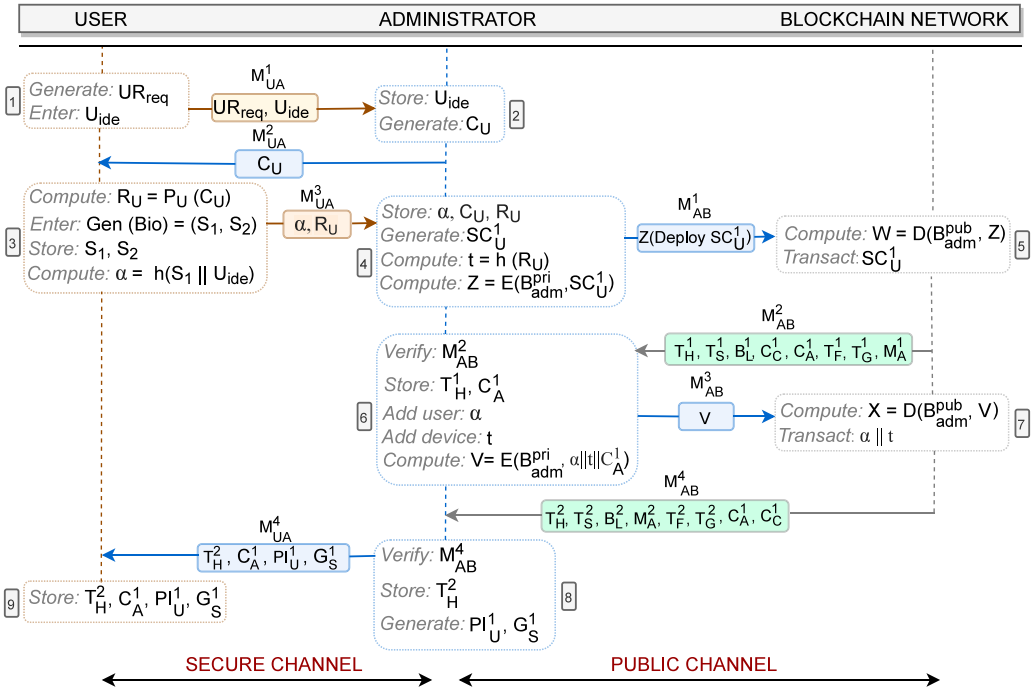

Fig. 3. User registration process.

```
pragma solidity   ^0.5.1;
contract IoTHealtcare {
        uint public alpha;   //message digest of biometric and identity {h(S1,Uide)}
        uint public t;   //message digest of PUF response {h(RU)}
        string status = "duplicate entry";  //UnD:User and device
    function addUnD(uint _alpha, uint _t) public returns(string memory result) {
        if (_alpha == alpha  && _t == t) {
    return status;   //returns an error if the user and device are already registered
    }   else {alpha = _alpha;   //otherwise, successful registration
              t = _t;
    }}
    function inspectUnD(uint _alpha, uint _t) public view returns(uint32 result) {
        if (_alpha == alpha
        &&  _t == t) {
           return 1;   //returns 1 if user and device are legitimate else returns 2
        } else {return 2;
}}}
```

Fig. 4. Smart contract for users.

Step 1: Admin prompts the challenge C_{SN} to ISN. The ISN and admin communicate through a secure channel during the registration process.

Step 2: The ISN inputs the C_{SN} to generate PUF response, $R_{SN} = P_{SN}(C_{SN})$ & delivers $SN_{ID}^{IoT} \parallel R_{SN}$ to admin.

Step 3: Upon M_{AS}^{2} arrival, admin stores C_{SN}, R_{SN}, and SN_{ID}^{IoT} into its DM. Subsequently, admin develops a smart contract SC_{SN}^{1} to register ISN on the BN. Due to space limitations and relative similarity with SC_{U}^{1}, SC_{SN}^{1} is not presented. Afterwards, the admin computes message digest, $g = h(SN_{ID}^{IoT} \parallel R_{SN})$ and digital signature, $\delta = E(B_{adm}^{pri}, SC_{SN}^{1})$ to preserve integrity and prevent non-repudiation. Remarkably, the admin and BN exchange information via a public (insecure) channel during the registration process.

Step 4: The BN miners decrypts $D(B_{adm}^{pub}, \delta)$ and deploys the SC_{SN}^{1} into the BN. Upon successful deployment, the miner returns $T_H^3, T_S^3, B_L^3, C_C^1, C_A^2, T_F^3, T_G^3, M_A^3$ to the admin.

Step 5: Admin analyze the M_{AB}^{2} and stores the transaction hash (T_H^3), and contract address (C_A^2) into its DM. Besides, admin computes Φ {= $E(B_{adm}^{pri}, g)$} and corresponds to BN for the addition of ISN (Φ) into the list of authorized nodes.

Step 6: Miner decrypts $D(B_{adm}^{pub}, \Phi)$ and retrieves $h(SN_{ID}^{IoT} \parallel R_{SN})$. Blockchain nodes verify the identity of ISN from the existing legitimate list in SC_{SN}^{1}, in case of coherence, blockchain nodes returns an error, otherwise it is stored in SC_{SN}^{1}. Upon successful transaction, blockchain nodes send these details $T_H^4, T_S^4, B_L^4, M_A^4, T_F^4, T_G^4, C_A^2, C_C^1$ to the admin.

Step 7: The admin verifies M_{AB}^{4} and stores the transaction hash T_H^4 into its DM. Finally, admin generates pseudo-identity of ISN (PI_{SN}^{1}) for anonymity and gateway secret (G_S^2) for mutual authentication and send it to ISN as M_{AS}^{3}.

Step 8: ISN stores the T_H^4, C_A^2, PI_{SN}^{1}, G_S^2 for future use.

3.4. Mutual authentication and key agreement phase

It is imperative to investigate users' and ISN's legitimacy before permitting them to converse with each other. The introduced protocol

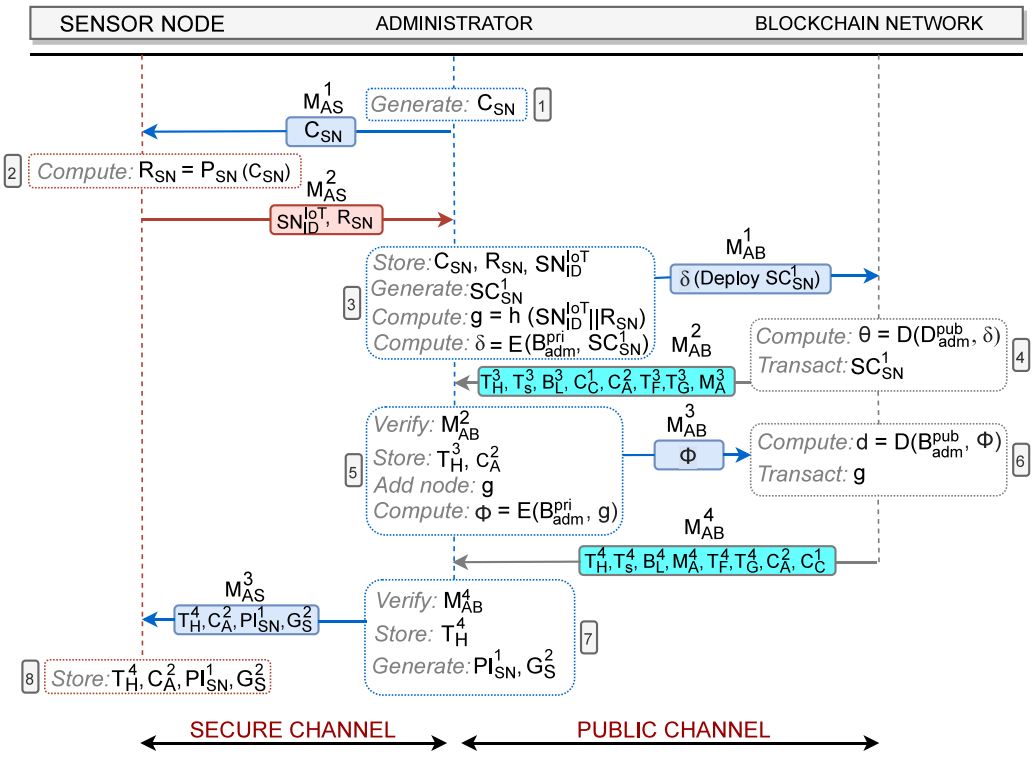

Fig. 5. IoT sensor node registration process.

guarantees mutual authentication and secure key establishment. The complete approach is illustrated in Fig. 6 and explained as follows:

Step 1: The UD generates N_U^1 and transmits $N_U^1 \parallel PI_U^1$ towards gateway (G_W). Communication between all entities occurs over insecure public channels.

Step 2: The G_W inspects N_U^1 and begins to locate PI_U^1. Upon success, the G_W chooses the corresponding C_U, R_U pair and generates nonce, N_G^1. To ensure safe relaying of the challenge (C_U), G_W computes $\beta = C_U \oplus G_S^1$. Additionally, G_W computes $j = h(G_S^1 \parallel R_U)$ to help UD in verifying the authenticity of G_W. Subsequently, N_G^1, β, j are sent to UD.

Step 3: The UD confirms the freshness of N_G^1 and derives $C_U = G_S^1 \oplus \beta$. Afterwards, UD inputs the challenge to PUF and retrieves the response, $R_U = P_U(C_U)$. Besides, the UD computes $\omega = h(G_S^1 \parallel R_U)$ and finds the equivalency between $\omega \equiv^? j$. The identicalness ($\omega \equiv j$) indicates successful authentication of G_W at UD, whereas non-equivalency ($\omega \not\equiv j$) results in connection termination. Further, UD prompts the user to enter biometrics, Rep $(Bio', S_2) = S_1$. UD generates N_U^2 and computes $\Delta = h(S_1 \parallel U_{ide}) \oplus G_S^1$, $\mu = G_S^1 \oplus R_U^1$ to prove its authenticity at G_W. At last, UD constructs M_{UG}^3 $\{= N_U^2, \Delta, \mu, PI_{SN}^1, T_H^2, C_A^1\}$ and send it to G_W.

Step 4: The G_W verifies N_U^2 and derives $h(S_1 \parallel U_{ide}) = \Delta \oplus G_S^1$. G_W retrieves $R_U = \mu \oplus G_S^1$ and prepares $G_1 = h(S_1 \parallel U_{ide}) \parallel h(R_U)$. Finally, G_W send T_H^2, C_A^1, and G_1 to BFN.

Step 5: BFN identifies the smart contract with C_A^1 address, and locates the transaction hash, T_H^2. Subsequently, BFN examines the authenticity of user and device by comparing the received information $h(S_1 \| U_{ide}) \| h(R_U)$ with the already transacted information, $\alpha \parallel t$. BFN prepares the response code, Res_C and deliver it to G_W as M_{BG}^2. Res_C discloses the success or failure of authentication. The authenticity verification mechanism using smart contracts is presented in Fig. 4.

Step 6: G_W evaluates Res_C, wherein $Res_C = 1$ approves the genuineness of user and its device, and $Res_C = 2$ indicates an adversarial attempt. G_W terminates the connection in case of a malicious attempt. Otherwise, it continues. Upon authentication, G_W initiates the process to connect UD with the PI_{SN}^1. G_W fetches the C_{SN}, R_{SN} pair from its DM. Further, G_W generates the nonce, N_G^2 and computes $\gamma = G_S^2 \oplus C_{SN}$ to send the challenge (C_{SN}) safely to the PI_{SN}^1. Besides, G_W calculates $\eta = h(G_S^2 \parallel R_{SN})$ to help ISN in verifying the authenticity of G_W. Subsequently, $M_{GS}^1 = N_G^2 \| \gamma \| \eta$ is composed and sent to PI_{SN}^1 (a pseudonym of SN_{ID}^{IoT}).

Step 7: ISN verifies N_G^2 and derives the challenge, $C_{SN} = \gamma \oplus G_S^2$. Afterwards, ISN calculates the response, $R_{SN} = P_{SN}(C_{SN})$ and use it to compute $\psi = h(G_S^2 \parallel R_{SN})$. ISN evaluates the identicalness, $\psi \equiv^? \eta$; equivalency proves the authenticity of G_W at ISN, whereas non-equivalency results in connection termination. Upon authentication of G_W, ISN generates N_{SN}^1 and computes $op_1 = G_S^2 \oplus R_{SN}$, $op_2 = G_S^2 \oplus SN_{ID}^{IoT}$ to prove its legitimacy at G_W. Finally, the ISN drafts $M_{GS}^2 = N_{SN}^1, op_1, op_2, T_H^4, C_A^2$ and send it to G_W.

Step 8: G_W examines the freshness of N_{SN}^1 and retrieves the response, $R_{SN} = op_1 \oplus G_S^2$ and real identity of ISN, $SN_{ID}^{IoT} = op_2 \oplus G_S^2$. Subsequently, G_W computes $G_2 = h(SN_{ID}^{IoT} \parallel R_{SN})$ and delivers $M_{BG}^3 = T_H^4 \| C_A^2 \| G_2$ to BFN for authenticity verification of ISN.

Step 9: BFN identifies the smart contract with C_A^2 address, and locates the transaction hash, T_H^4. BFN examines the authenticity of ISN by comparing the received information $h(SN_{ID}^{IoT} \parallel R_{SN})$ with the already transacted information, g. BFN prepares the response code, Res_C and delivers it to G_W as M_{BG}^4. Res_C discloses the success/failure of authentication.

Step 10: G_W evaluates Res_C, wherein $Res_C = 1$ approves the genuineness of ISN, and $Res_C = 2$ indicates an adversarial attempt. G_W terminates the connection in case of adversarial attempt, otherwise continues. Furthermore, G_W generates the N_G^3 and N_G^4, calculates the new pseudo-identities of UD ($PI_U^{2*} = G_S^1 \oplus PI_U^2$) and ISN ($PI_{SN}^{2\#} = G_S^2 \oplus PI_{SN}^2$). Finally, G_W computes the secret session key for user ($SK^* = G_S^1 \oplus$ SK) and ISN ($SK^\# = G_S^2 \oplus$ SK). The G_W composes $M_{UG}^4 = N_G^3 \| SK^* \| PI_U^{2*}$ and $M_{GS}^3 = N_G^4 \| SK^\# \| PI_{SN}^{2\#}$ and send M_{UG}^4, M_{GS}^3 to UD and ISN, respectively. It is noteworthy that neither secret key nor pseudo-identity are shared in interpretable form.

Step 11: UD verifies the freshness of N_G^3, and derives the SK $(= SK^* \oplus G_S^1)$ and PI_U^2 $(= PI_U^{2*} \oplus G_S^1)$. The SK is used to secure the current session whereas PI_U^{2*} is stored in UD memory for ensuring anonymity in the subsequent session.

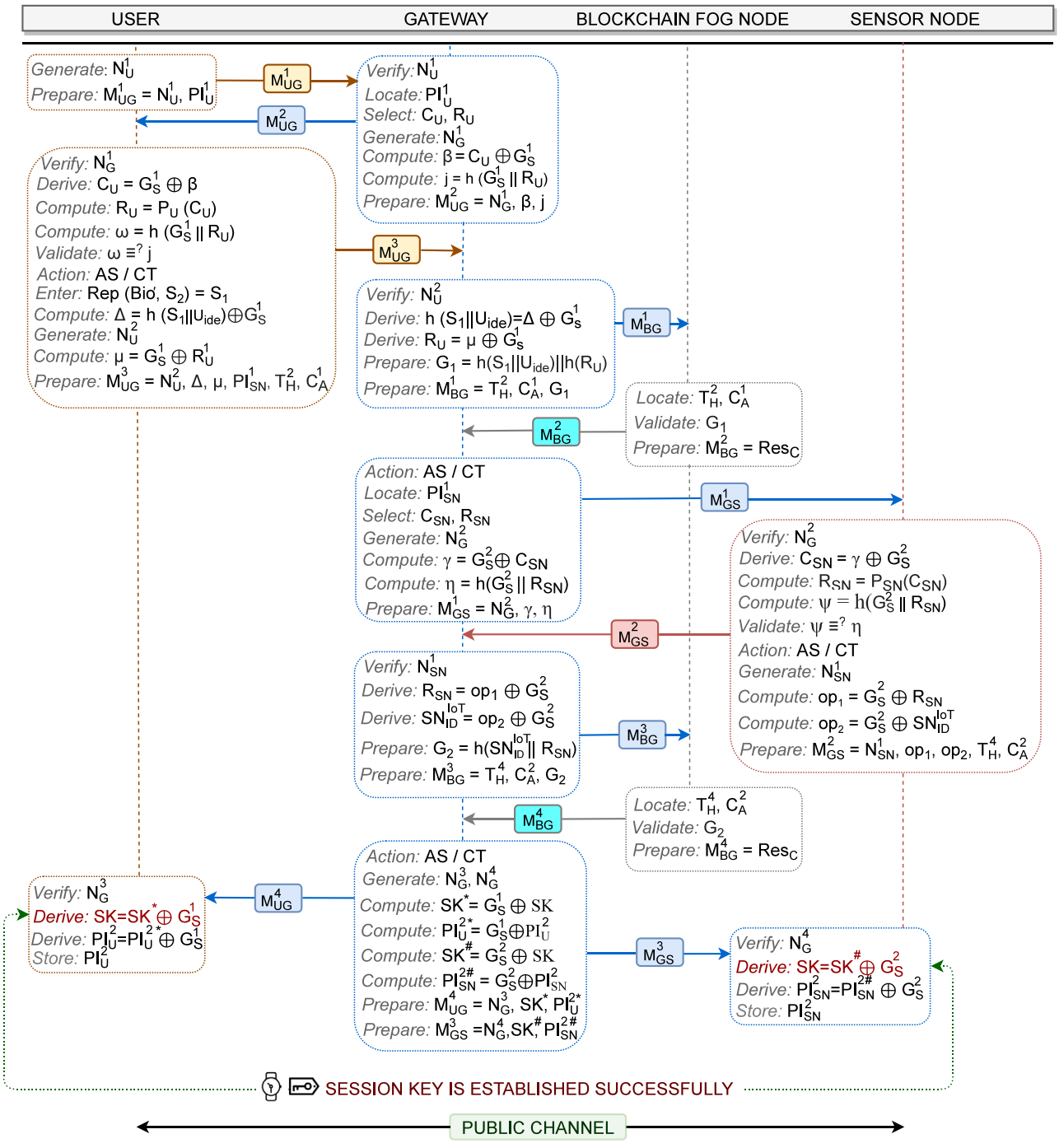

Fig. 6. Mutual authentication and key establishment process.

Step 12: Upon receipt of M_{GS}^3, ISN verifies N_G^4, and calculates the SK ($= SK^\# \oplus G_S^2$) and PI_{SN}^2 ($= PI_{SN}^{2\#} \oplus G_S^2$). The SK is used to secure the current session whereas PI_{SN}^2 is stored for ensuring anonymity in the subsequent session.

4. Security analysis

Scyther facilitates the security protocol developers to test the strength of their devised protocol against attacks. It offers simplicity in modeling cryptosystems, and also supports the DY model [45]. To operate Scyther, we have installed Scyther 1.1.3, Graphviz 2.46, Python 2.7, and wxPython 2.8, in the computing system that has Ubuntu OS (Linux, 64-bit). We have used the default settings of Scyther; *typed matching* and *pruning method* is used with a maximum no. of runs as 5 and maximum number of patterns per claim as 10, respectively. The protocol is scripted in *Security Protocol Description Language* and begins with global constants and functions declaration succeeded by roles of individual entities that comprise *computations*, *communications*, and *claims*. The results obtained from the Scyther are presented in Fig. 7; it proves the robustness of the proposed protocol against MITM, and replay attacks, etc. The claims 'secret' verified the confidentiality of the message elements, whereas 'Nisynch', 'Niagree', 'Alive', and

Claim				Status	Comments
IoT_Healthcare	user	IoT_Healthcare,u1	Secret s1	Ok	No attacks within bounds.
		IoT_Healthcare,u2	Nisynch	Ok	No attacks within bounds.
		IoT_Healthcare,u3	Niagree	Ok	No attacks within bounds.
		IoT_Healthcare,u4	Alive	Ok	No attacks within bounds.
		IoT_Healthcare,u5	Weakagree	Ok	No attacks within bounds.
	gateway	IoT_Healthcare,g1	Secret gs2	Ok	No attacks within bounds.
		IoT_Healthcare,g2	Nisynch	Ok	No attacks within bounds.
		IoT_Healthcare,g3	Niagree	Ok	No attacks within bounds.
		IoT_Healthcare,g4	Alive	Ok	No attacks within bounds.
		IoT_Healthcare,g5	Weakagree	Ok	No attacks within bounds.
	iot_node	IoT_Healthcare,i1	Secret rsn	Ok	No attacks within bounds.
		IoT_Healthcare,i2	Nisynch	Ok	No attacks within bounds.
		IoT_Healthcare,i3	Niagree	Ok	No attacks within bounds.
		IoT_Healthcare,i4	Alive	Ok	No attacks within bounds.
		IoT_Healthcare,i5	Weakagree	Ok	No attacks within bounds.

Fig. 7. Simulation results from Scyther.

Table 2
Smart contract transaction costs.

Environment	Deployment		Registration		Registration (Duplicate entry)	
	Transaction fee (*Ether*)	Gas	Transaction fee (*Ether*)	Gas	Transaction fee (*Ether*)	Gas
JavaScript VM	0.00064322091955602	449 028	0.00006347292138915	44 310	0.00004534353088811	31 654
Injected Web3	0.00033556562114504	234 256	0.000089774575860515	62 671	0.000037735661659995	26 343

Gas price (Gwei): 1.432473965, *Transaction fee*: Gas price × Gas used by transaction, *Injected Web3*: Metamask (Ropsten Test Network).

'Weakagree' verified the authenticity of the entities. Consequently, Scyther ascertained that the proposed protocol is secure to use for IoT healthcare networks.

5. Performance and comparative analysis

The smart contract (SC) employed by the proposed protocol is realized in the *Remix Integrated Development Environment* (IDE) using *Solidity* programming language [46]. The SC is deployed and tested on two distinct platforms (JavaScript VM (JVM), Injected Web3 (IW3)) for consistency check. *Metamask* supported IW3 *Ropsten Test Network* is used to execute smart contracts while *etherscan* is used to access transaction logs [47]. Table 2 presents the *gas* and the *transaction fee* spent for deploying and registering the nodes on the decentralized blockchain network. It is worth noting that SC does not levy any transaction costs while verifying the authenticity of nodes. Based on the calculations, the deployment, registration, and duplicacy prevention in the JVM and IW3 environment would cost around $1.15, $0.11, $0.081, and $0.60, $0.16, and $0.0681, respectively. The costs may vary because the crypto-currencies are very volatile. The aforementioned calculations are based on this relationship, 1 ETH = $1765.88.

It is evident from Table 3 that the proposed protocol attained the security properties such as data privacy, message integrity, freshness, anonymity, untraceability, and biometric security. The accomplishment of security properties strengthened the proposed security protocol to withstand attacks like replay, impersonation, modification, DoS, MITM, and cloning, etc. Besides, the proposed protocol uses decentralized blockchain-powered Ethereum SC to overcome the demerits of centralized infrastructure. It is apparent from Table 3 that existing schemes [19,20,36,48–52] are not able to resist all prominent attacks. Further, it is exposed that none of the traditional schemes [19,20,36, 48–52] adopted a decentralized approach, thus resulting in decreased efficiency.

Table 3
Comparison of Proposed scheme vs. Traditional schemes.

$\mathcal{G}$	$\mathcal{S}_1$	$\mathcal{S}_2$	$\mathcal{S}_3$	$\mathcal{S}_4$	$\mathcal{S}_5$	$\mathcal{S}_6$	$\mathcal{S}_7$	$\mathcal{S}_8$	$\mathcal{H}$
$\mathcal{G}_1$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{G}_2$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{G}_3$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{G}_4$	✓	×	×	✓	×	×	✓	×	✓
$\mathcal{G}_5$	✓	×	✓	✓	×	✓	✓	×	✓
$\mathcal{G}_6$	✓	✓	✓	×	×	✓	✓	✓	✓
$\mathcal{G}_7$	×	×	✓	×	×	×	×	×	✓
$\mathcal{G}_8$	×	×	✓	×	×	×	×	×	✓
$\mathcal{G}_9$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{G}_{10}$	✓	×	×	✓	×	×	×	×	✓
$\mathcal{G}_{11}$	✓	✓	✓	✓	×	×	✓	✓	✓
$\mathcal{G}_{12}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{G}_{13}$	✓	✓	✓	✓	✓	✓	✓	×	✓
$\mathcal{G}_{14}$	*	✓	✓	✓	✓	*	✓	✓	✓
$\mathcal{G}_{15}$	✓	×	✓	×	×	✓	×	×	✓
$\mathcal{G}_{16}$	*	×	✓	✓	✓	*	✓	✓	✓
$\mathcal{G}_{17}$	×	×	✓	×	×	×	×	×	✓
$\mathcal{G}_{18}$	✓	×	✓	✓	×	×	✓	✓	✓
$\mathcal{G}_{19}$	×	×	✓	✓	✓	×	✓	✓	✓
$\mathcal{G}_{20}$	×	×	×	×	×	×	×	×	✓

$\mathcal{G}$: Security goals, $\mathcal{H}$: Proposed healthcare protocol, '✓': goal accomplished, '×': goal unaccomplished, '*': Not applicable, $\mathcal{G}_1$: Replay, $\mathcal{G}_2$: Impersonation, $\mathcal{G}_3$: Modification, $\mathcal{G}_4$: DoS, $\mathcal{G}_5$: MITM, $\mathcal{G}_6$: Known key, $\mathcal{G}_7$: Cloning, $\mathcal{G}_8$: Side-channel, $\mathcal{G}_9$: Mutual authentication, $\mathcal{G}_{10}$: Data privacy, $\mathcal{G}_{11}$: Session key security, $\mathcal{G}_{12}$: Message integrity, $\mathcal{G}_{13}$: Message freshness, $\mathcal{G}_{14}$: User identity anonymity, $\mathcal{G}_{15}$: Sensor node identity anonymity, $\mathcal{G}_{16}$: User untraceability, $\mathcal{G}_{17}$: Sensor node untraceability, $\mathcal{G}_{18}$: Formal security analysis, $\mathcal{G}_{19}$: Biometric security, $\mathcal{G}_{20}$: Smart contract, $\mathcal{S}_n$: Schemes in comparison, $\mathcal{S}_1$: [36], $\mathcal{S}_2$: [19], $\mathcal{S}_3$: [20], $\mathcal{S}_4$: [48], $\mathcal{S}_5$: [49], $\mathcal{S}_6$: [50], $\mathcal{S}_7$: [51], $\mathcal{S}_8$: [52].

Table 4
Computation cost comparison of proposed scheme vs. Traditional schemes.

$\mathcal{S}$	Computation cost
S_1	$AE_{1t} + AD_{3t} + H_{2t} + M_{2t} + XOR_{2t}$
S_2	$H_{18t} + XOR_{9t} + R_{2t}$
S_3	$H_{22t} + PUF_{5t} + XOR_{16t} + R_{3t} + B_{1t}$
S_4	$H_{37t} + XOR_{16t} + R_{2t} + B_{1t}$
S_5	$SE_{4t} + SD_{4t} + H_{19t} + XOR_{14t} + R_{4t} + B_{1t} + SM_{3t}$
S_6	$H_{15t} + XOR_{10t} + R_{2t}$
S_7	$H_{25t} + XOR_{20t} + R_{3t} + MOD_{9t}$
S_8	$H_{18t} + XOR_{9t} + R_{3t} + B_{1t} + SM_{6t}$
$\mathcal{H}$	$H_{7t} + PUF_{2t} + XOR_{20t} + R_{7t} + B_{1t}$

$\mathcal{S}$ - Scheme, S_1: [36], S_2: [19], S_3: [20], S_4: [48], S_5: [49], S_6: [50], S_7: [51], S_8: [52], $\mathcal{H}$ - Proposed healthcare protocol, AE - Asymmetric encryption, AD - Asymmetric decryption, H - Hash, SE - Symmetric encryption, SD - Symmetric decryption, M - Hash based MAC, R - Random number, PUF - Physically Unclonable Function, B - Bio-metric, MOD - Modulus, XOR - Bit-wise XOR, SM - Scalar Multiplication, Nt - number of times.

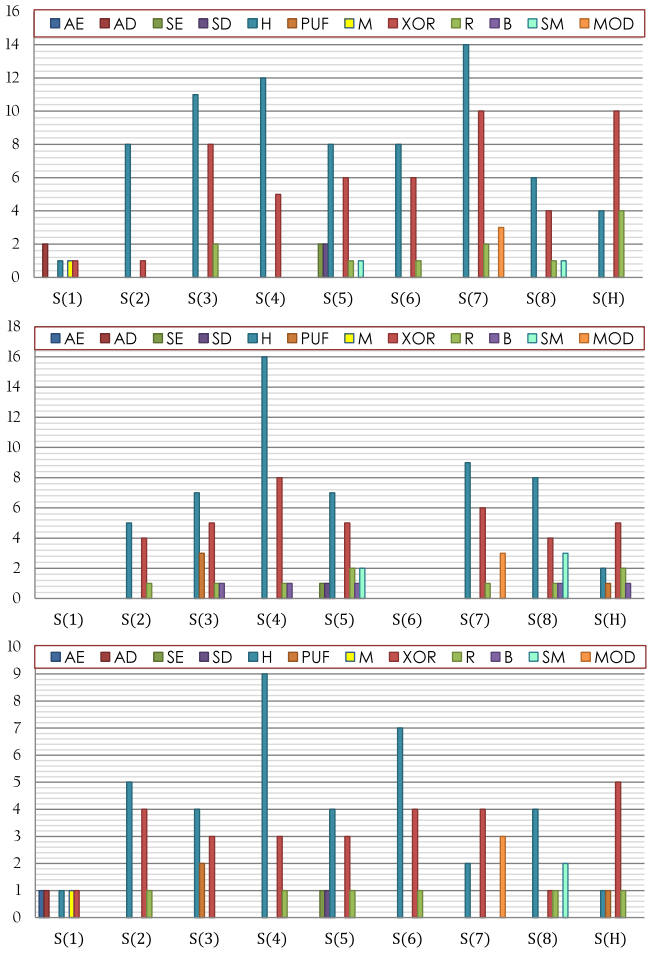

Fig. 8. Computation Cost of Gateway (topmost), User (middle-most), and IoT sensor node (bottom-most) of proposed scheme vs. traditional schemes; S(n): schemes in comparison, S(1): [36], S(2): [19], S(3): [20], S(4): [48], S(5): [49], S(6): [50], S(7): [51], S(8): [52], S(H): Proposed protocol.

The computation cost calculations for the registration phase is omitted because it incurs only once during initialization. As evident from Table 4, the proposed protocol is computationally economical because it uses lightweight cryptography primitives (hash, XOR, and PUF) instead of computing expensive cryptography primitives (public-key cryptography, scalar multiplications). Fig. 8 demonstrates that the entities in the proposed scheme (user device, gateway, IoT sensor node) executes the cryptographic operations fewer times than the entities in the conventional schemes [19,20,36,48–52], indicating that it is computationally inexpensive. As apparent from Table 4 and Fig. 8, a few traditional schemes [19,50] have the reasonable computation, but those schemes [19,50] do not guarantee the complete security of the IoT networks. Therefore, the proposed protocol can be the best alternative to the existing compute expensive protocols.

6. Conclusions and future scope

Healthcare 4.0 in AmI environments is a technology-driven and patient-centric paradigm where IoT sensor nodes automatically operate, collect the information from medical equipment, and export it to the cloud. To protect sensitive health information from adversarial threats, authentication approaches were developed in the past. However, those schemes were infrastructure-centric, computationally expensive, and prone to adversarial threats. Therefore, we have employed PUF, blockchain-powered SC, and fog nodes in our proposed authentication protocol to circumvent SPOF, prevent cyber-attacks, and enhance efficiency. The ethereum SC is developed in Remix IDE using solidity, executed on metamask RTN, and used to verify the authenticity of network entities at minimal cost. We have verified the resiliency of the protocol against attacks using Scyther. Due to nominal computation cost, the proposed scheme finds its applicability in resource-constrained IoT based healthcare networks. Zero-Knowledge Proofs (ZKPs) and homomorphic encryption will be applied to perform confidentiality-preserving authentication and processing of information, hence extending the security and privacy of the IoT-enabled healthcare applications.

CRediT authorship contribution statement

Mehedi Masud: Conceptualization, Methodology, Software, Validation, Formal analysis, Data curation, Writing – original draft, Writing – review & editing, Project administration. **Gurjot Singh Gaba:** Conceptualization, Methodology, Software, Validation, Formal analysis, Data curation, Writing – original draft, Writing – review & editing. **Pardeep Kumar:** Methodology, Formal analysis, Writing – original draft, Writing – review & editing, Supervision. **Andrei Gurtov:** Methodology, Resources, Writing – original draft, Writing – review & editing, Supervision, Project administration, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgment

The research is supported by Taif University Researchers Supporting Project Number (TURSP-2020/10), Taif University, Taif, Saudi Arabia, CENIIT Project 17.01, and the Excellence Center at Linköping-Lund in IT (ELLIIT) Project A4.

References

[1] S. Banerjee, B. Bera, A.K. Das, S. Chattopadhyay, M.K. Khan, J.J. Rodrigues, Private blockchain-envisioned multi-authority CP-ABE-based user access control scheme in IIoT, Comput. Commun. 169 (2021) 99–113.
[2] P. Nerurkar, D. Patel, Y. Busnel, R. Ludinard, S. Kumari, M.K. Khan, Dissecting bitcoin blockchain: Empirical analysis of bitcoin network (2009–2020), J. Netw. Comput. Appl. 177 (2021) 102940.
[3] E.K. Wang, Z. Liang, C.-M. Chen, S. Kumari, M.K. Khan, PoRX: A reputation incentive scheme for blockchain consensus of IIoT, Future Gener. Comput. Syst. 102 (2020) 140–151.

[4] C. Lin, D. He, X. Huang, M.K. Khan, K.-K.R. Choo, DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain, IEEE Trans. Inf. Forensics Secur. 15 (2020) 2440–2452.

[5] P. Gope, Y. Gheraibia, S. Kabir, B. Sikdar, A secure IoT-based modern healthcare system with fault-tolerant decision making process, IEEE J. Biomed. Health Inf. (2020).

[6] M. Masud, G.S. Gaba, S. Alqahtani, G. Muhammad, B. Gupta, P. Kumar, A. Ghoneim, A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care, IEEE Internet Things J. (2020).

[7] H. Qiu, M. Qiu, M. Liu, G. Memmi, Secure health data sharing for medical cyber-physical systems for the healthcare 4.0, IEEE J. Biomed. Health Inf. 24 (9) (2020) 2499–2505.

[8] M. Masud, M. Alazab, K. Choudhary, G.S. Gaba, 3P-SAKE: privacy-preserving and physically secured authenticated key establishment protocol for wireless industrial networks, Comput. Commun. 175 (2021) 82–90.

[9] Z. Shao, S. Yuan, Y. Wang, Adaptive online learning for IoT botnet detection, Inform. Sci. 574 (2021) 84–95.

[10] M. Hatton, The IoT in 2030: 24 billion connected things generating $1.5 trillion, 2020, https://iotbusinessnews.com/2020/05/20/03177-the-iot-in-2030-24-billion-connected-things-generating-1-5-trillion/. Online; accessed February 9, 2021.

[11] B.D. Deebak, Secure and efficient mutual adaptive user authentication scheme for heterogeneous wireless sensor networks using multimedia client–server systems, Wirel. Pers. Commun. 87 (3) (2016) 1013–1035.

[12] Y.K. Ever, Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks, IEEE Syst. J. 13 (1) (2018) 456–467.

[13] T.-H. Chen, W.-K. Shih, A robust mutual authentication protocol for wireless sensor networks, ETRI J. 32 (5) (2010) 704–712.

[14] L. Xu, F. Wu, Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care, J. Med. Syst. 39 (2) (2015) 1–9.

[15] L. Wang, Analysis and enhancement of a password authentication and update scheme based on elliptic curve cryptography, J. Appl. Math. 2014 (2014).

[16] V. Odelu, A.K. Das, A. Goswami, An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card, J. Inf. Secur. Appl. 21 (2015) 1–19.

[17] M. Turkanović, B. Brumen, 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. 20 (2014) 96–112.

[18] M.S. Farash, M. Turkanović, S. Kumari, 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. 36 (2016) 152–176.

[19] C.-C. Chang, H.-D. Le, A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks, IEEE Trans. Wireless Commun. 15 (1) (2015) 357–366.

[20] P. Gope, A.K. Das, N. Kumar, Y. Cheng, Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks, IEEE Trans. Ind. Inf. 15 (9) (2019) 4957–4968.

[21] P. Kumar, A. Gurtov, M. Sain, A. Martin, P.H. Ha, Lightweight authentication and key agreement for smart metering in smart energy networks, IEEE Trans. Smart Grid 10 (4) (2018) 4349–4359.

[22] A. Fayad, B. Hammi, R. Khatoun, A. Serhrouchni, A blockchain-based lightweight authentication solution for IoT, in: 2019 3rd Cyber Security in Networking Conference (CSNet), IEEE, 2019, pp. 28–34.

[23] T. Wu, G. Yang, L. Zhu, Y. Wu, Privacy-preserving voluntary-tallying leader election for internet of things, Inform. Sci. 574 (2021) 461–472.

[24] S. Athanere, R. Thakur, Blockchain based hierarchical semi-decentralized approach using ipfs for secure and efficient data sharing, J. King Saud Univ Comput Inf Sci 34 (4) (2022) 1523–1534.

[25] I. Widi Widayat, M. Köppen, Blockchain simulation environment on multi-image encryption for smart farming application, in: International Conference on Intelligent Networking and Collaborative Systems, Springer, 2021, pp. 316–326.

[26] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, P.H. Ha, Anonymous secure framework in connected smart home environments, IEEE Trans. Inf. Forensics Secur. 12 (4) (2017) 968–979.

[27] Y. Zhan, B. Wang, R. Lu, Y. Yu, DRBFT: Delegated randomization Byzantine fault tolerance consensus protocol for blockchains, Inform. Sci. 559 (2021) 8–21.

[28] B. Deebak, F.H. Memon, X. Cheng, K. Dev, J. Hu, S.A. Khowaja, N.M.F. Qureshi, K.H. Choi, Seamless privacy-preservation and authentication framework for IoT-enabled smart ehealth systems, Sustainable Cities Soc. (2022) 103661.

[29] R.L. Kumar, Q.-V. Pham, F. Khan, M.J. Piran, K. Dev, Blockchain for securing aerial communications: Potentials, solutions, and research directions, Phys. Commun. 47 (2021) 101390.

[30] M. Tahir, M. Sardaraz, S. Muhammad, M. Saud Khan, A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics, Sustainability 12 (17) (2020) 6960.

[31] P. Singh, G.S. Gaba, A. Kaur, M. Hedabou, A. Gurtov, Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT, IEEE J. Biomed. Health Inf. (2022).

[32] G.S. Gaba, G. Kumar, T.-H. Kim, H. Monga, P. Kumar, Secure device-to-device communications for 5g enabled internet of things applications, Comput. Commun. 169 (2021) 114–128.

[33] A. Yazdinejad, G. Srivastava, R.M. Parizi, A. Dehghantanha, K.-K.R. Choo, M. Aledhari, Decentralized authentication of distributed patients in hospital networks using blockchain, IEEE J. Biomed. Health Inf. 24 (8) (2020) 2146–2156.

[34] G.S. Gaba, M. Hedabou, P. Kumar, A. Braeken, M. Liyanage, M. Alazab, Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare, Sustainable Cities Soc. 80 (2022) 103766.

[35] Y. Pourasad, R. Ranjbarzadeh, A. Mardani, A new algorithm for digital image encryption based on chaos theory, Entropy 23 (3) (2021) 341.

[36] G. Kumar, H. Monga, T.-H. Kim, M. Liyanage, Robust and lightweight key exchange (LKE) protocol for industry 4.0, IEEE Access 8 (2020) 132808–132824.

[37] Y. Zheng, Y. Cao, C.-H. Chang, UDhashing: Physical unclonable function-based user-device hash for endpoint authentication, IEEE Trans. Ind. Electron. 66 (12) (2019) 9559–9570.

[38] C. Wu, L. Ke, Y. Du, Quantum resistant key-exposure free chameleon hash and applications in redactable blockchain, Inform. Sci. 548 (2021) 438–449.

[39] D. Mathivathanan, K. Mathiyazhagan, N.P. Rana, S. Khorana, Y.K. Dwivedi, Barriers to the adoption of blockchain technology in business supply chains: a total interpretive structural modelling (TISM) approach, Int. J. Prod. Res. 59 (11) (2021) 3338–3359.

[40] M. Yavari, M. Safkhani, S. Kumari, S. Kumar, C.-M. Chen, An improved blockchain-based authentication protocol for IoT network management, Secur. Commun. Netw. 2020 (2020).

[41] G. Büyüközkan, G. Tüfekçi, A decision-making framework for evaluating appropriate business blockchain platforms using multiple preference formats and VIKOR, Inform. Sci. 571 (2021) 337–357.

[42] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, Y. Zhang, A smart contract based access control framework for cloud smart healthcare system, IEEE Internet Things J. (2020).

[43] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, H. Lu, Towards secure and privacy-preserving data sharing for covid-19 medical records: A blockchain-empowered approach, IEEE Trans. Netw. Sci. Eng. (2021).

[44] K. Lei, M. Du, J. Huang, T. Jin, Groupchain: Towards a scalable public blockchain in fog computing of IoT services computing, IEEE Trans. Serv. Comput. 13 (2) (2020) 252–262.

[45] J. Zhang, G. Qu, Physical unclonable function-based key sharing via machine learning for IoT security, IEEE Trans. Ind. Electron. 67 (8) (2019) 7025–7033.

[46] L. Zhang, H. Zhang, J. Yu, H. Xian, Blockchain-based two-party fair contract signing scheme, Inform. Sci. 535 (2020) 142–155.

[47] A. Lisi, A. De Salve, P. Mori, L. Ricci, S. Fabrizi, Rewarding reviews with tokens: An ethereum-based approach, Future Gener. Comput. Syst. 120 (2021) 36–54.

[48] A.K. Das, M. Wazid, N. Kumar, A.V. Vasilakos, J.J. Rodrigues, Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment, IEEE Internet Things J. 5 (6) (2018) 4900–4913.

[49] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, K.-K.R. Choo, A robust and energy efficient authentication protocol for industrial internet of things, IEEE Internet Things J. 5 (3) (2018) 1606–1615.

[50] A. Esfahani, G. Mantas, R. Matischek, F.B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M.G. Tauber, C. Schmittner, J. Bastos, A lightweight authentication mechanism for M2M communications in industrial IoT environment, IEEE Internet Things J. 6 (1) (2019) 288–296.

[51] S. Paliwal, Hash-based conditional privacy preserving authentication and key exchange protocol suitable for industrial internet of things, IEEE Access 7 (2019) 136073–136093.

[52] X. Li, J. Niu, M.Z.A. Bhuiyan, F. Wu, M. Karuppiah, S. Kumari, A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things, IEEE Trans. Ind. Inf. 14 (8) (2018) 3599–3609.