future internet

MDPI

Article

Lightweight Privacy-Preserving Remote User Authentication and Key Agreement Protocol for Next-Generation IoT-Based Smart Healthcare

Zeeshan Ashraf [1,*], Zahid Mahmood [2] and Muddesar Iqbal [3,*]

[1] Department of Computer Science, The University of Chenab, Gujrat 50700, Pakistan
[2] Department of Computer Science & IT, University of Kotli Azad Jammu & Kashmir, Azad Jammu and Kashmir, Kotli 11100, Pakistan; zahidmahmood575@uokajk.edu.pk
[3] Renewable Energy Lab, College of Engineering, Prince Sultan University, Riyadh 11586, Saudi Arabia
* Correspondence: zeeshan@cs.uchenab.edu.pk (Z.A.); m.iqbal@lsbu.ac.uk (M.I.)

Abstract: The advancement and innovations in wireless communication technologies including the Internet of Things have massively changed the paradigms of health-based services. In particular, during the COVID-19 pandemic, the trends of working from home have been promoted. Wireless body area network technology frameworks help sufferers in remotely obtaining scientific remedies from physicians through the Internet without paying a visit to the clinics. IoT sensor nodes are incorporated into the clinical device to allow health workers to consult the patients' fitness conditions in real time. Insecure wireless communication channels make unauthorized access to fitness-related records and manipulation of IoT sensor nodes attached to the patient's bodies possible, as a result of security flaws. As a result, IoT-enabled devices are threatened by a number of well-known attacks, including impersonation, replay, man-in-the-middle, and denial-of-service assaults. Modern authentication schemes do solve these issues, but they frequently involve challenging mathematical concepts that raise processing and transmission costs. In this paper, we propose a lightweight, secure, and efficient symmetric key exchange algorithm and remote user authentication scheme. Our research proposal presents a successful privacy-protecting method for remote users and provides protection against known attacks. When compared to conventional options, this technique significantly reduces calculation costs by up to 37.68% and transmission costs by up to 32.55%.

Keywords: authentication; healthcare; IoT; key agreement; next-generation network; security

check for updates

Citation: Ashraf, Z.; Mahmood, Z.; Iqbal, M. Lightweight Privacy-Preserving Remote User Authentication and Key Agreement Protocol for Next-Generation IoT-Based Smart Healthcare. *Future Internet* **2023**, *15*, 386. https://doi.org/10.3390/fi15120386

Academic Editor: Gianluigi Ferrari

Received: 18 September 2023
Revised: 29 October 2023
Accepted: 26 November 2023
Published: 29 November 2023

1. Introduction

The use of 5G and the Internet of Things (IoT) have revolutionary changed and created innovation in different sectors [1]. IoT applications are already being deployed extensively, in various domains such as wearables, smart homes, smart cities, agriculture, industrial automation, and healthcare. The main challenges for IoT in different sectors include ensuring security and privacy, managing power consumption, developing scalable architecture, integrating with existing systems, selecting appropriate components, and testing smart devices for reliability [2]. Remote user verification and data privacy challenges are a top priority in IoT-based applications in different sectors [3]. The IoT is the backbone of the smart healthcare ecosystems [4]. The healthcare ecosystem is a complex network of organizations, individuals, and resources involved in delivering healthcare services [5]. It includes healthcare providers such as hospitals, clinics, and physicians, as well as insurance companies, government agencies, pharmaceutical companies, medical device manufacturers, and patients [6]. The healthcare ecosystem is constantly evolving and adapting to changes in technology, healthcare policies, and patient needs [7]. IoT-based smart healthcare systems have become popular in recent years. IoT-based healthcare enables the remote monitoring, real-time tracking of patient data, and improves the communication between patients and healthcare providers [8]. Effective healthcare ecosystems require collaboration and coordination between all the different entities such as patients, healthcare professionals, clinical devices, smart equipment, and limitless wireless sensors [9]. This includes sharing information, resources, and best practices to mitigate the affected person's consequences and decrease costs [10]. Some common characteristics such as equity, comprehensive services, adequate workforce, information systems, and infrastructure are crucial for healthcare ecosystems [11]. The goal of the healthcare ecosystem is to provide accessible, high-quality care to patients while also promoting innovation and efficiency [12]. IoT-based healthcare has the ability to enhance the affected person's results, lessen healthcare expenses, and improve the care quality [13]. However, it is essential to ensure that patient data are safe and healthcare providers have the necessary infrastructure and training to use the IoT effectively.

A wireless sensor network (WSN) is a network of sensors that communicate wirelessly to perform various tasks such as monitoring, data collection, and control [14]. A sensor has low computing and communication powers that detect or measure a physical quantity such as temperature, pressure, or light intensity [15]. IoT-based wireless body area networks (WBANs) are a type of wireless network that involves using small, low-power sensors or devices placed on or inside a person's body to monitor various physiological and environmental parameters such as heart rate, temperature, blood pressure, and oxygen levels [16]. These devices communicate with a central hub or gateway that collects and analyzes the data and may also transmit the data to a remote location for further processing [17]. In healthcare, WBANs can be used to monitor patients' vital signs remotely, enabling doctors and caregivers to make real-time decisions about patient care [18]. One of the key challenges of WBANs is ensuring that the sensors are reliable and accurate, as well as ensuring that wireless communication is secure and private [19]. WBANs have a high chance of eavesdropping, man-in-the-middle (MITM), and impersonation attacks [20,21]. Critical information about the patients is exchanged in healthcare applications. The malicious interest by way of an adversary could endanger the patient's life. A patient's sensitive data are only to be accessible to valid users such as doctors and clinical staff [22]. So, it is necessary to allow access only to authorized remote users. The healthcare system needs to guarantee security services including privacy, facts' integrity, and confidentiality of a patient's fitness documents.

1.1. Motivation and Contribution

Work from home has been promoted during the COVID-19 pandemic. The IoT can help healthcare providers monitor patients remotely, which can enhance patient care and decrease healthcare costs [23,24]. Patients can use IoT devices to track their vital signs, including coronary heart rate, blood stress, and blood glucose range, and transmit these data to healthcare providers in real time. This can help healthcare providers detect health problems early and provide timely intervention. However, the sensitive clinical statistics of the patient are at high risk if the data are accessed remotely, due to the fact that the communication channels are insecure [25]. In this paper, the authentication issue is highlighted so that an authentic user can only monitor the health condition of the patient remotely over an insecure network. Authentication schemes stop unauthorized users from accessing network resources over vulnerable networks [26]. The available authentication schemes for IoT-based healthcare services cannot resist major network attacks. Moreover, existing schemes adopt complicated procedures that consume high computation and communication costs. So, such authentication schemes are not recommended for the resource-constrained environment that demands a lightweight scheme in terms of low computation and communication costs. Therefore, this paper introduces a lightweight remote user authentication scheme for IoT-based healthcare services by using a strong and simple symmetric session key exchange algorithm. The essential contributions of this research study are as follows:

1. An efficient, cost-effective, and simple IoT-based secure platform is proposed in this research.
2. The security model adopts a strong and simple symmetric session key exchange algorithm.
3. The effectiveness of the plan against several types of known attacks is demonstrated.
4. The proposed system model only allows the registered and verified users to be granted entry into the healthcare network.
5. A detailed comparison analysis of the proposed model is conducted with the existing models to compute the cost of the proposed model with respect to communication and computation costs.

1.2. Organization of the Paper

Section 2 delves into the related work, providing an overview of prior research in the field. Sections 3 and 4 focus on the system model and the secure authentication scheme, offering comprehensive explanations of these components. Section 5 is dedicated to the formal analysis, where rigorous examination and evaluation take place. Section 6 presents the findings derived from the analysis, offering insights and observations. Finally, in Section 7, this paper draws its conclusions, summarizing the key takeaways, and contributions.

2. Related Works

Authentication is a manner of verifying the legitimacy of a user or system before granting access to the required service [27]. The authentication process is an integral part of information security. Remote user authentication is necessary for IoT-based systems when the public network is vulnerable. In IoT-based remote patient healthcare monitoring systems, the sensitive data of the patients are collected through different sensors and accessed by healthcare professionals through the Internet. Multiple security services have been proposed in the existing research for healthcare and are discussed in this section.

In [28], Challa et al. proposed an ECC-based user authentication that is heavy with respect to computation and communication [29,30]. Moreover, Jia et al. [31] found that the scheme [28] does not provide security against impersonate attacks. Zhou et al. [32] introduced an authentication scheme for IoT-based cloud architectures. However, the scheme is vulnerable to privileged insider attacks, MITM attacks, replay attacks, and impersonation attacks [33]. Moreover, this scheme adopted a complicated mathematical procedure that increases the computation and communication costs.

Farash et al. [34] proposed a user authentication and key management protocol for IoT-based WSNs. However, Amin et al. [35] found numerous drawbacks of this protocol and diagnosed vulnerability against user impersonation and offline password-guessing attacks. In addition, this scheme adopted a complicated mathematical procedure that increases the computation and communication costs.

Sharma et al. [36] introduced a user authentication scheme for IoT-based cloud healthcare systems. However, the researchers in [37] proved that the scheme does not offer security services against insider attacks. In addition, the scheme exchanges a significant size of messages during authentication. Wazid et al. [38] proposed a device authentication scheme and key management protocol for IoT-based edge computing. However, this scheme increases computation and communication costs. So, this scheme is not suitable for resource-constrained devices.

Masud et al. [39] proposed an anonymity-preserving user authentication scheme for IoT-based healthcare. This scheme adopted a complicated and lengthy procedure for user authentication. Therefore, the scheme increases computation and communication costs. Rana et al. [40] extended their work presented in [41] and proposed an upgraded scheme by ensuring secure communication over the public channel. The authors claimed that their proposed secure communication system is most suitable for IoT infrastructure. But the scheme exchanges a significant amount of messages. So, the scheme increases communication costs.

Son et al. [42] found that the scheme presented in [43] is vulnerable to various attacks such as offline password guessing, impersonation, privileged insider, and known session-specific temporary information attacks. Therefore, the authors proposed a novel authentication scheme that resolved the security problems found in [43]. The scheme uses only hash and exclusive-OR operations to be applicable in IoT environments. Kumar et al. [44] proposed a physical unclonable function (PUF) based on the multi-factor authentication technique for IoT-based healthcare. The scheme adopts a complicated and lengthy procedure for user authentication and exchanges a significant amount of messages. Therefore, the scheme increases computation and communication costs. So, this scheme is not suitable for smart devices.

Chen et al. [45] analyzed and observed that the scheme presented in [39] cannot effectively resist against privileged internal attacks, sensor node capture attacks, and stolen authentication attacks. The scheme does not have perfect forward security. Therefore, the authors proposed a new lightweight and robust user authentication scheme for IoT-based healthcare and resolved the security vulnerabilities that existed in [39]. However, the scheme adopts a complex procedure for user authentication. So, the scheme is not suitable for smart devices. Qualitative comparisons between existing schemes based on computation and communication costs are shown in Table 1.

Table 1. Qualitative comparisons between existing schemes.

Components	**[38]**	**[39]**	**[40]**	**[42]**	**[44]**	**[45]**
Computation Cost (ms)	0.1236	0.0853	0.1101	0.0656	0.0749	0.0762
Communication Cost (bits)	2976	2048	3296	1600	4822	1792
Number of Messages Exchanged	4	4	2	3	6	4

There are several attacks that are possible in the existing schemes reviewed in this section, such as reply attacks and MITM attacks. The mentioned schemes failed to address the amenity features to strengthen remote user privacy. The analysis shows that the proposed schemes are heavy with respect to communication, computation, and overheads, which can be overcome by giving motivation to lightweight authentication methods. To address the mentioned loophole in the existing schemes, our research proposes an efficient authentication mechanism to prevent unauthorized users from accessing the resources remotely.

3. System Model and Security Goals

3.1. IoT-Based System Model

The system model of the next-generation IoT-based healthcare environment is depicted in Figure 1. In the healthcare environment, several components such as physicians as remote users, patients, IoT-based sensor nodes, gateway or servers, access points (APs), etc., communicate with each other and exchange sensitive data.

3.1.1. Remote User (Physician)

The physician connects to the server remotely through a recourse-constraint mobile device and wants to access the sensor nodes to see the patient’s reports. It is necessary to verify the remote user’s legitimacy before granting access. The physician updates the patient’s history online.

3.1.2. Gateway/Server

The server behaves as a gateway among sensor nodes and remote users. The server is a powerful machine that verifies the legitimacy of the remote users and grants access to the resources available in the healthcare environment. The server also plays a role as a registration authority (RA). We assume that the server contains a secure database and that the attacker cannot access data stored in the database.

3.1.3. IoT-Based Sensor Nodes

Sensor nodes are low-power equipment that performs restricted computation and communication processes. IoT-enabled sensor nodes collect and transmit the real-time data of the patients. Sensor nodes connect to the server through the wireless access point.

3.1.4. Wireless Access Point

Usually, a wireless access point has a wired connection to the server and provides wireless connectivity to other devices.

3.1.5. Patient

A patient is an entity that is admitted to the hospital for treatment. Different types of IoT-based sensor nodes are attached to the body of the patient. IoT-based nodes collect data about the vital signs of the patient and send them to the doctor for treatment.

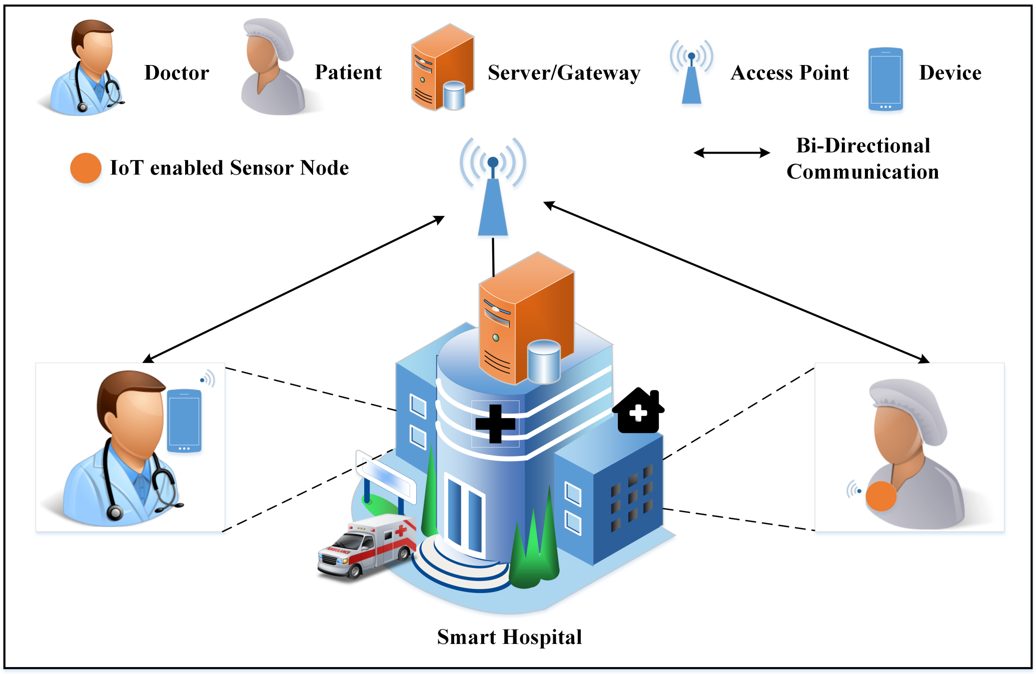


Figure 1. Smart hospital environment.

3.2. Adversary Model

The Dolev–Yao adversary model was introduced in 1983. It is applied for the cryptanalysis of the proposed security models [46]. All possible controls that can be performed by adversaries such as duplicating the messages, modification of traffic, and wrongly updating are considered to prove the analysis. For example, an intruder attempts to listen in on a conversation and gain right of entry into personal data. Considering the adversary model in an IoT-based healthcare environment, the attacker can change the frequency rate for controlling the patient's vital signs consisting of coronary heart rate, blood stress, and blood glucose ranges. Cyberattacks can result in severe results such as patient death, economic loss, and a bad reputation for the healthcare system.

3.3. Security Goals

The proposed scheme describes prominent security features.

3.3.1. Key Exchange and Mutual Authentication

In the hospital network, very sensitive data are exchanged between several nodes and users. Users can access critical data remotely. Mutual authentication between remote users and servers is required for secure communication. Remote users exchange symmetric keys and then perform authentication to avoid the anonymity of the users. The mutual remote user authentication process blocks unauthorized access to the network and data.

3.3.2. Anonymity of Identity

The adversary searches for loopholes or weak points in the systems. An intruder wants to access confidential data such as user identity, password, secret keys, etc., to perform MITM attacks and impersonate attacks. So, the identity of the remote users and devices must be kept anonymous while messages are exchanged. If an adversary attempts to access the network or data by using malicious attacks, then the system should deny such attempts.

3.3.3. Data Privacy

Sensitive and private data such as user identity, passwords, secret keys, patient records, etc., are exchanged in the hospital network. If the data are leaked, then this may affect the reputation of the hospital. So, data must be exchanged confidentially and no one should have access to the data. For data privacy, cryptography and hashing techniques are used with secret keys.

3.3.4. Freshness and Message Integrity

If data are altered by an intruder, this also causes damage to the hospital's reputation. So, security systems used in hospitals should ensure the freshness and integrity of the transferred data. Random numbers and timestamps are used for data freshness.

3.3.5. Lightweightness

IoT-based devices are resource-constrained in terms of low computing power, short memory, and short battery. The nodes can only execute restricted computations. So, security systems should be designed with lightweight cryptosystems that perform only simple arithmetic operations, hash functions, and bitwise XOR.

4. Proposed Scheme

Within this section, we introduce a streamlined authentication system designed for remote users. The scheme we propose encompasses several stages, including user registration, sensor node registration, login, secret key establishment, and mutual authentication, as shown in Figure 2. In Table 2, you will find a comprehensive list of notations and their corresponding explanations, which were employed throughout this research.

Table 2. Notations and descriptions.

Notation	Description
$Doctor_U$	Doctor as a user
SN	Sensor node
SN_{ID}	Identity of the sensor node
S	Server
ID_D	Identity of the doctor
PSW_D	Password of the doctor
HID_D	Hash-based identity of the doctor
$HPSW_D$	Hash-based password of the doctor
N_1, N_2	Randomly generated two secret natural larger numbers
N_D, N_S	Numbers generated by the doctor and server
R_D, R_S	Results sent by doctor and the server
K_S	Symmetric session key
$\bigoplus$	Bitwise XOR
$\|$	Concatenation
Hash (.)	Hash function
$HMAC_D$	Hash value sent by the doctor
$HMAC_S$	Hash value sent by the server

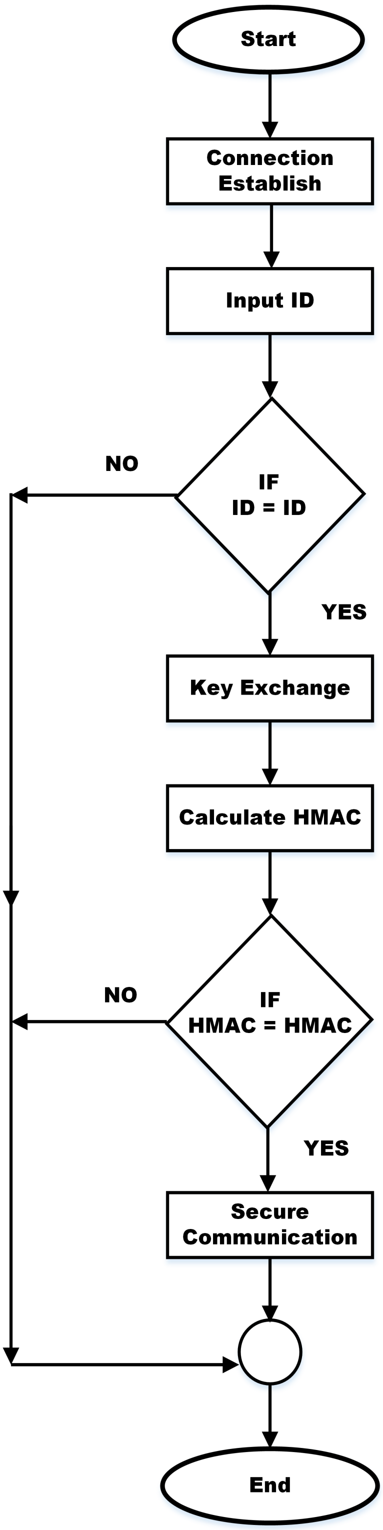


Figure 2. Flowchart of the proposed secure system.

4.1. User Registration Phase

As compared to other research studies [38–40,42,44,45], the user registration phase of our proposed scheme is very simple. A doctor must register themself on the server as a user. Sometimes, doctors need to access real-time patient health information remotely. During the registration, the doctor chooses a unique identity as an ID_D and a strong password as a PSW_D. For security reasons, the hash-based identity of the doctor must be generated as HID_D and the hash-based password as $HPSW_D$ by concatenation of identity and password in a hash function, as described in Equation (1) and Equation (2), respectively.

$$HID_D = hash\ (ID_D) \tag{1}$$

$$HPSW_D = hash\ (ID_D \parallel PSW_D) \tag{2}$$

The server stores the secret credentials of the users along with email addresses and mobile numbers in its database. If the identity of the user is the same as one already saved in a database, then the server rejects it.

4.2. Node Registration Phase

Before sending the real-time authentic credentials, the communication node which is a sensor device receives registration in the server and then transmits information. The server maintains the identification and status of communication nodes composed of sensors. At the sensor node registration, RA assigns a unique identity as SN_{ID} to every sensor node in the healthcare system. The server saves the identity and status of the sensor node in the server's database.

4.3. Session Key Exchange Phase

Before accessing devices and data, the authentication process is conducted. Before authentication, a key must be exchanged between the remote user and the server. We follow a simple and strong symmetric key exchange in Algorithm 1. Session key exchange processes are described as follows:

Step 1: The doctor enters identity as ID_D and password as PSW_D in the device (smartphone). The device computes hash-based identity as HID_D = h(ID_D) and hash-based password as $HPSW_D$ = h($ID_D \parallel PSW_D$). The device sends HID_D to the server for verification. When the server receives the login information of the remote user, then the server verifies it against its database. If the login information is not correct, then the server terminates the connection. If the login information is correct, then the server randomly generates two larger numbers, N_1 and N_2. The server computes N_1^* = ($N_1 \oplus HPSW_D$), N_2^* = ($N_2 \oplus HPSW_D$), and sends them to the remote user. The doctor receives the values of N_1^* and N_2^* from the server and derives N_1 and N_2 from ($N_1^* \oplus HPSW_D$) and ($N_2^* \oplus HPSW_D$), respectively.

Step 2: The doctor generates a larger random number N_D. The random number's size is 128 bits. The doctor's device multiplies the random number N_D with N_1, adds N_1, and computes the result, as shown in Equation (3). The device multiplies Res_D with the second number N_2, adds both numbers N_1 and N_2, and calculates the final result FR_D as shown in Equation (4). The device sends FR_D to the server for a session key of size 128 bits calculation. The final result FR_D is not a key. So, if an intruder catches it, then the intruder cannot retrieve the key.

$$Res_D = (N_D \times N_1) + N_1 \tag{3}$$

$$FR_D = (Res_D \times N_2) + N_1 + N_2 \tag{4}$$

Step 3: When the server receives the final result FR_D by the doctor's device, then the server extracts the hidden number N_D by using both numbers N_1 and N_2, respectively. The server subtracts the numbers N_1 and N_2 and obtains the result Res_S as shown in Equation (5).

$$Res_S = FR_D - (N_1 + N_2) \tag{5}$$

The server extracts N_D, as presented in Equation (6).

$$N_D = (Res_S/(N_1 \times N_2)) - 1 \tag{6}$$

Step 4: Similarly, the server generates a larger random number of N_S and sends FR_S to the doctor. The doctor extracts the hidden number N_S by following the same procedure, as shown above.

Step 5: When both sides have shared secret numbers N_D and N_S with each other, then both sides compute bitwise XOR of N_D with N_S, calculate mod with M, and obtain the final session key K_S on both sides secretly, as shown in Equation (7), where M is a variable that stores the larger value of size 128 bits.

$$K_S = (N_D \oplus N_S) \ mod \ M \tag{7}$$

The same session key is exchanged between the remote user (doctor) and the server. The key would be used in security services such as mutual authentication, data confidentiality, and data integrity over vulnerable public networks. Figure 3 shows the complete process of session key exchange and mutual authentication among server and remote user.

Algorithm 1 Proposed Key Exchange Algorithm

```
Require: M is a variable that stores the value of size 128 bits. The server registered the
    clients and saved the identity and password of the clients $HID_C \ and \ HPSW_C$
 1: Client Sends $HID_C \ to \ Server : HID_C \rightarrow Server$
 2: if $HID_C = HID_C$ then
 3:     Server generates $N_1$, $N_2$ and sends to client secretly $N_1^* \ and \ N_2^* \rightarrow Client$
 4:     Client generates a larger random number as $N_C : N_C \leftarrow rand()$
 5:     if $N_C = 0$ then
 6:         Go to Step 4
 7:     end if
 8:     Set $C = (N_C \times N_1) + N_1$
 9:     Set $R_C = (C \times N_2) + N_1 + N_2$
10:     Client sends $R_C \ to \ Server : R_C \rightarrow Server$
11:     Set $r_C = R_C - (N_1 + N_2)$
12:     Set $N_C = (r_C/(N_1 \times N_2)) - 1$
13:     Server generates a larger random number as $N_S : N_S \leftarrow rand()$
14:     if $N_S = 0$ then
15:         Go to Step 13
16:     end if
17:     Set $S = (N_S \times N_1) + N_1$
18:     Set $R_S = (S \times N_2) + N_1 + N_2$
19:     Server sends $R_S \ to \ client : R_S \rightarrow Client$
20:     [Client performs the same process from 11 to 12]
21:     /* Client and server compute the same key as */
22:     Set $K_S = (N_C \oplus N_S) \ mod \ M$
23:     if $K_S = 0$ then
24:         Go to Step 4
25:     end if
26: else
27:     $Connection \ Terminate$
28: end if
```

4.4. Mutual Authentication Phase

After sharing the secret key, the mutual authentication process is performed to ensure the legitimacy of the remote users. We propose a simple method of mutual authentication using a "Hash-based Message Authentication Code" (HMAC) and a symmetric session key. The HMAC generates a fixed-length message code that can be used in the authentication. The hashing value depends upon the hashing algorithm [47]. The server and doctor's device generate HMAC by using an IP address, a session key S_K, and a random number in hashing algorithm SHA-256, as shown in Equation (8) and Equation (9), respectively.

Random numbers and session keys ensure the freshness of the HMAC because, in every new session, random numbers and session keys will be changed.

$$HMAC_D = SHA - 256\ (IP\ Address_D \parallel N_D, K_S) \tag{8}$$

$$HMAC_S = SHA - 256\ (IP\ Address_S \parallel N_S, K_S) \tag{9}$$

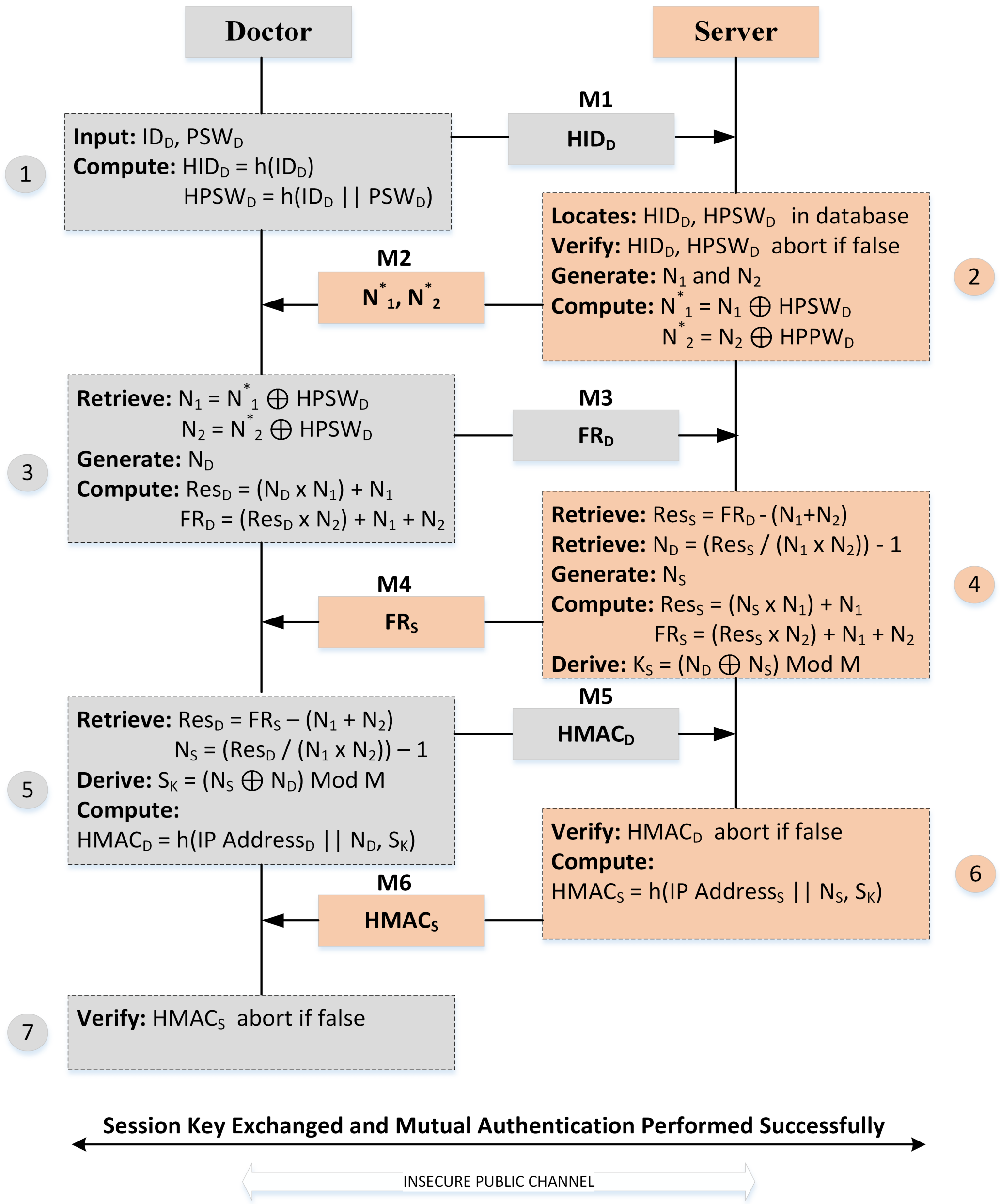

Doctor
Server
M1
HID_D
1
Input: ID_D, PSW_D
Compute: HID_D = h(ID_D)
HPSW_D = h(ID_D || PSW_D)
2
Locates: HID_D, HPSW_D in database
Verify: HID_D, HPSW_D abort if false
Generate: N_1 and N_2
Compute: N*_1 = N_1 ⊕ HPSW_D
N*_2 = N_2 ⊕ HPPW_D
M2
N*_1, N*_2
3
Retrieve: N_1 = N*_1 ⊕ HPSW_D
N_2 = N*_2 ⊕ HPSW_D
Generate: N_D
Compute: Res_D = (N_D x N_1) + N_1
FR_D = (Res_D x N_2) + N_1 + N_2
M3
FR_D
4
Retrieve: Res_S = FR_D - (N_1+N_2)
Retrieve: N_D = (Res_S / (N_1 x N_2)) - 1
Generate: N_S
Compute: Res_S = (N_S x N_1) + N_1
FR_S = (Res_S x N_2) + N_1 + N_2
Derive: K_S = (N_D ⊕ N_S) Mod M
M4
FR_S
5
Retrieve: Res_D = FR_S – (N_1 + N_2)
N_S = (Res_D / (N_1 x N_2)) – 1
Derive: S_K = (N_S ⊕ N_D) Mod M
Compute:
HMAC_D = h(IP Address_D || N_D, S_K)
M5
HMAC_D
6
Verify: HMAC_D abort if false
Compute:
HMAC_S = h(IP Address_S || N_S, S_K)
M6
HMAC_S
7
Verify: HMAC_S abort if false
Session Key Exchanged and Mutual Authentication Performed Successfully
INSECURE PUBLIC CHANNEL

Figure 3. Secret key exchange and authentication processes.

The server and doctor's device send HMAC to each other for mutual authentication. Both sides calculate HMAC and verify it. If any one side does not verify it, then the established connection is terminated immediately on either side. If authentication is performed, then the server fetches the patient's record of that doctor and displays it on the device. For security reasons, the doctor can only access their patient's records remotely.

5. Security Analysis

In this section, we prove the robustness of our proposed security model by using informal security analysis and formal security analysis by using different tools.

5.1. Informal Security Analysis

Our scheme's strength against various attacks, including password guessing, brute force, impersonation, replay, forgery, denial of service, man-in-the-middle, and perfect forward secrecy, has been substantiated through informal security analysis, as documented in [30].

5.2. Formal Security Analysis

In this section, we prove the robustness of our proposed scheme against known attacks through "Burrows-Abadi-Needham" (BAN) logic and the "Automated Validation of Internet Security Protocols and Applications" (AVISPA) simulation tool.

5.2.1. BAN Logic

BAN logic is a symbolic logic system that is used for analyzing security protocols. It focuses on ensuring that various security properties are held in a protocol. The detailed BAN logic analysis for the user registration phase of our proposed protocol, including equations and explanations, is given below:

1. Initial Assumptions;
    - Doctor D trusts the server S.
    - Doctor D chooses a unique identity ID_D and a strong password PSW_D.
    - The hash function is used for generating HID_D and $HPSW_D$ for secure communication.
    - The server S securely stores the secret credentials of users, including email addresses and mobile numbers.
    - The server S verifies the identity of the user based on the stored data in its database.

    The database is secure and safe.
2. Idealized Protocol Model;
3. Protocol Description;
4. Formal Agreement Analysis.

BAN Logic Formal Analysis for User Registration Phase:

- Doctor D selects a unique identity ID_D and a strong password PSW_D.
- Doctor D computes hash-based identity HID_D = hash(ID_D) and hash-based password $HPSW_D$ = hash($ID_D \parallel PSW_D$).

Server S receives HID_D for Verification:

- Doctor D sends HID_D to server S for verification.
- Server S checks the received HID_D against its stored database to verify the identity.
- If the identity is correct, server S proceeds; otherwise, it terminates the connection.

Equations and BAN Logic Analysis:

1. Initial Assumptions (Idealization);
    - D believes {S, K_S} is secure: D|S, K_S.
    - D chooses a unique identity and strong password: D|{ID_D, PSW_D}.
    - D believes the hash function is secure: D|hash(ID_D).
    - S securely stores user credentials: S|{Secrets}.
    - S verifies identities based on stored data: S|{Verified}.
2. Idealized Protocol Model (Idealization);
    - Doctor D sends HID_D to server S for verification: D → S: {HID_D}.
    - Server S verifies HID_D in its database and verifies the identity: S → D: {Verified}.
3. Protocol Description (Formalization);

   - Doctor D believes that the server S has received HID_D: D|S: {HID_D}.
   - Doctor D believes that the server S has verified the identity: D|S: {Verified}.

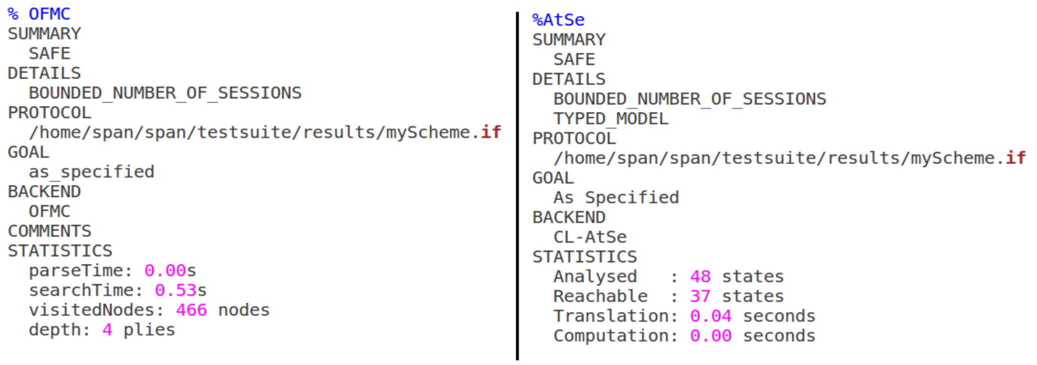
4. Formal Agreement Analysis (Inference Rules).
   - Doctor D believes that server S has verified the identity based on the received HID_D: D | S: {HID_D, Verified}.
   - Server S securely stores user credentials: S|{Secrets}.
   - Server S verifies identities based on stored data: S|{Verified}.
   - Doctor D has securely registered with server S: D|S: {Registered}.

BAN Logic Analysis

The user registration phase ensures that doctor D can securely register with server S using a unique identity and a strong password. The server S verifies the identity based on the stored data, and the protocol ensures that only legitimate users can register. The protocol guarantees that the chosen identity and password are used correctly. This BAN logic formal analysis demonstrates that the user registration phase of the protocol satisfies the security properties and is designed to prevent unauthorized access. Similar analyses can be performed for other phases of the protocol as needed.

5.2.2. AVISPA

We employed a widely utilized, open-source, and reputable tool known as AVISPA to validate security objectives. In AVISPA, programmers utilize the "High-Level Protocol Specification Language" (HLPSL) to write code, which is then converted into the "Intermediate Format" (IF) using HLPSL2IF. Following the execution, AVISPA provides one of three specific outcomes: "safe", "unsafe", or "inconclusive". In the context of AVISPA, the channel is susceptible to all the attacks outlined in Section 3.2. Our proposed scheme consists of two basic roles of entities: The user device as a client and the server as a gateway. These basic roles comprise agent details as C and S. The description of the basic roles of the agents also includes crypto-operations, local declarations, channel (dy), initial state, and transitions to limit the boundaries of evaluation. Other roles are environment role and session role. The environment role specifies the global constants, knowledge of the intruder primarily based on the adversary model (dy), and the information of all the communication sessions between authentic and unauthentic communicating entities. The AVISPA code is publicly accessible on GitHub [48]. The simulation results reveal that, in the backend, the OFMC (Observational Finite Model Checker) algorithm explored 466 nodes up to a depth of four layers in just 0:53 s to confirm the protocol's safety against security threats. Similarly, the CL-AtSe (Compositional Logic for Attack and Security) tool in the backend analyzed 48 states in just 0:04 s to assert the protocol's safety, as shown in Figure 4.



```
% OFMC
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/myScheme.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.53s
  visitedNodes: 466 nodes
  depth: 4 plies
```

```
%AtSe
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/myScheme.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 48 states
  Reachable  : 37 states
  Translation: 0.04 seconds
  Computation: 0.00 seconds
```

Figure 4. Simulation results from OFMC and CL-AtSe on AVISPA.

6. Performance and Comparative Analysis

In this phase, we examine the overall performance of our proposed scheme with other existing schemes in terms of computation cost, messages passing cost, and safety functions.

6.1. Computation Costs

The computation cost means the total time it takes to complete the different crypto operations during the key agreement and authentication phases. Normally, it measures in milliseconds (ms). We specified the expected unit time costs of several activities that were completed during a simulation [49]. The computation cost for one XOR operation is 0.002 ms, one hash operation is 0.0005 ms, concatenation is 0.0004 ms, random number generation is 0.0052 ms, and one arithmetic operation is 0.0004 ms.

Table 3 indicates the assessment outcomes of computational expenses between our proposed scheme and other associated schemes. Comparative analysis shows that our proposed scheme, including the key exchange procedure, consumed less envisioned computational time compared to other present schemes. Our proposed scheme reduced computation costs by up to 37.68% compared to [42].

Table 3. Computation cost comparison.

Schemes	Total Computation Cost	Estimated Time (ms)
[38]	$44T_H + 15T_\oplus + 127T_{\|\|} + 4T_{ran}$	0.1236
[39]	$9T_H + 27T_\oplus + 15T_{\|\|} + 4T_{ran}$	0.0853
[40]	$25T_H + 38T_\oplus + 28T_{\|\|} + 2T_{ran}$	0.1101
[42]	$28T_H + 13T_\oplus + 38T_{\|\|} + 2T_{ran}$	0.0656
[44]	$9T_H + 17T_\oplus + 26T_{\|\|} + 5T_{ran}$	0.0749
[45]	$10T_H + 27T_\oplus + 17T_{\|\|} + 2T_{ran}$	0.0762
Proposed	$4T_H + 6T_\oplus + 3T_{\|\|} + 4T_{ran} + 22T_A$	0.0448

6.2. Transmission Costs

The communication cost refers to the cumulative computation of various transmissions that have traversed the communication channels during the phases of key agreement and authentication, which is typically quantified in bits. For ease of communication evaluation, we defined the size of different variables such as the timestamp as 32 bits, the random number as 128 bits, the identifier as 128 bits, and the hash value as 256 bits, respectively. Our proposed approach incurs a communication cost of (128 + 256 + 128 + 128 + 256 + 256 = 1152) bits, spread across six messages. As illustrated in Figure 5, the comparative analysis of communication expenses is presented, contrasting our proposed method with alternative related strategies. The comparative assessment reveals that our suggested approach, which integrates the key exchange technique, experiences notably lower estimated communication overhead in comparison to various preexisting methodologies. Specifically, our proposed method achieves a reduction in communication costs of up to 32.55% when compared to the approach discussed in reference [42].

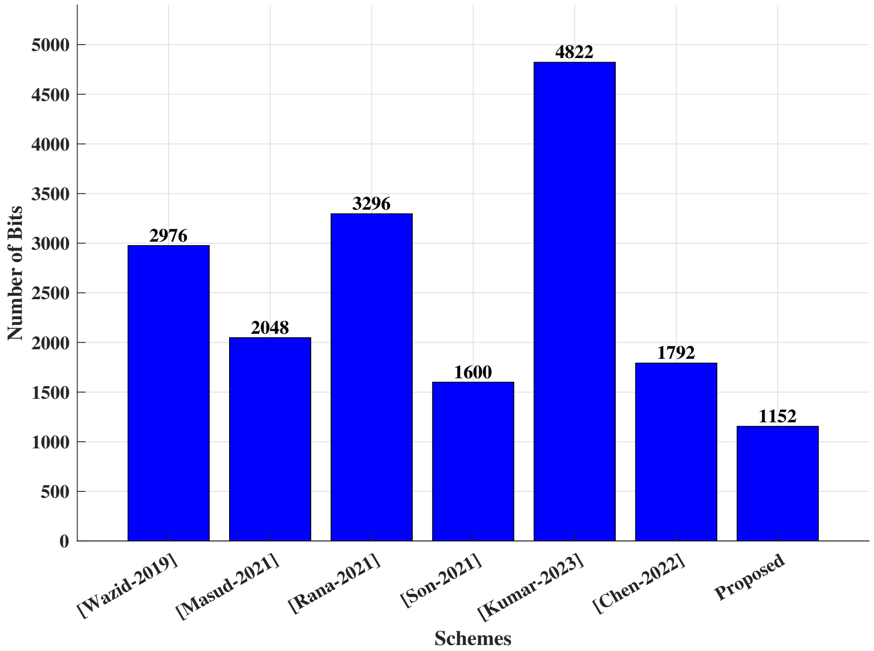


Figure 5. Transmission cost comparisons [38–40,42,44,45].

7. Conclusions and Future Directions

This study introduced efficient, lightweight, and secure symmetric key exchange and remote user verification methods for advanced IoT-driven smart healthcare systems. The approach employs uncomplicated procedures combined with a unidirectional hashing function, XOR operations, and arithmetic calculations for both the session key exchange and remote user verification stages. It offers substantial security against recognized threats like replay attacks, MITM attacks, DoS attacks, and others. Furthermore, we illustrated that our proposed method incurs minimal computational and communication expenses in comparison to existing methods. Specifically, the computational workload was reduced by up to 37.68%, and communication expenses were lowered by up to 32.55%, as contrasted with earlier approaches in this field. Consequently, we conclude that our suggested method is highly suitable for IoT-based smart healthcare scenarios that work with limited resources.

In future work, we plan to focus on data sovereignty, ethical and legal requirements with data sharing, and environmental costs regarding the CO_2 footprint. Data sovereignty issues will be addressed through access control, data localization, and data encryption. Environmental costs related to CO_2 footprint issues will be addressed through a transition to renewable energy sources such as solar and implementing energy-efficient technologies.

Author Contributions: Conceptualization, methodology, validation, Z.A.; formal analysis, Z.A. and Z.M.; investigation, writing—original draft preparation, Z.A.; writing—review and editing, Z.A.; visualization, Z.M.; project administration, M.I.; funding acquisition, M.I. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was funded by Prince Sultan University, Saudi Arabia.

Data Availability Statement: The data presented in this study are available in this article.

Acknowledgments: The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APCs) of this publication. The authors would like to thank Prince Sultan University for their support. The authors also thank the anonymous reviewers and the editor for their valuable feedback on the paper which helped the authors to improve its quality and presentation.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ghildiyal, Y.; Singh, R.; Alkhayyat, A.; Gehlot, A.; Malik, P.; Sharma, R.; Akram, S.V.; Alkwai, L.M. An imperative role of 6G communication with perspective of industry 4.0: Challenges and research directions. *Sustain. Energy Technol. Assess.* **2023**, *56*, 103047. [CrossRef]
2. Jayabalan, J.; Jeyanthi, N. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *J. Parallel Distrib. Comput.* **2022**, *164*, 152–167. [CrossRef]
3. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and security: Challenges and solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]
4. Mohindru, V.; Vashishth, S.; Bathija, D. Internet of Things (IoT) for Healthcare Systems: A Comprehensive Survey. In *Recent Innovations in Computing: Proceedings of ICRIC 2021, Volume 1*; Springer: Singapore, 2022; pp. 213–229.
5. Osama, M.; Ateya, A.A.; Sayed, M.S.; Hammad, M.; Pławiak, P.; Abd El-Latif, A.A.; Elsayed, R.A. Internet of Medical Things and Healthcare 4.0: Trends, Requirements, Challenges, and Research Directions. *Sensors* **2023**, *23*, 7435. [CrossRef]
6. Dwivedi, R.; Mehrotra, D.; Chandra, S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *J. Oral Biol. Craniofac. Res.* **2022**, *12*, 302–318. [CrossRef] [PubMed]
7. El-Shafai, W.; Khallaf, F.; El-Rabaie, E.S.M.; Abd El-Samie, F.E. Proposed neural SAE-based medical image cryptography framework using deep extracted features for smart IoT healthcare applications. *Neural Comput. Appl.* **2022**, *34*, 10629–10653. [CrossRef]
8. Sharma, A.; Kumar, R. A constrained framework for context-aware remote E-healthcare (CARE) services. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e3649. [CrossRef]
9. Davwar, P.P. Effective Health Care Plan for National Health Insurance Scheme Patients with Non-Communicable Diseases in Plateau North Senatorial District. *Am. J. Appl. Stat. Econ.* **2023**, *2*, 1–6. [CrossRef]
10. Nosouhi, M.R.; Sood, K.; Grobler, M.; Doss, R. Towards spoofing resistant next generation IoT networks. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 1669–1683. [CrossRef]
11. Rawat, R.; Garg, B.; Mahor, V.; Telang, S.; Pachlasiya, K.; Chouhan, M. Organ trafficking on the dark web—the data security and privacy concern in healthcare systems. In *Internet of Healthcare Things: Machine Learning for Security and Privacy*; Wiley: Hoboken, NJ, USA, 2022; pp. 189–216.
12. Rehman, A.; Abbas, S.; Khan, M.; Ghazal, T.M.; Adnan, K.M.; Mosavi, A. A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. *Comput. Biol. Med.* **2022**, *150*, 106019. [CrossRef]
13. Zhang, L.; Zhu, Y.; Ren, W.; Zhang, Y.; Choo, K.K.R. Privacy-preserving fast authentication and key agreement for e-health systems in iot, based on three-factor authentication. *IEEE Trans. Serv. Comput.* **2022**, *16*, 1324–1333. [CrossRef]
14. Majid, M.; Habib, S.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.W. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. *Sensors* **2022**, *22*, 2087. [CrossRef]
15. Daoui, A.; Yamni, M.; Karmouni, H.; Sayyouri, M.; Qjidaa, H.; Motahhir, S.; Jamil, O.; El-Shafai, W.; Algarni, A.D.; Soliman, N.F.; et al. Efficient Biomedical Signal Security Algorithm for Smart Internet of Medical Things (IoMTs) Applications. *Electronics* **2022**, *11*, 3867. [CrossRef]
16. Singla, R.; Kaur, N.; Koundal, D.; Bharadwaj, A. Challenges and developments in secure routing protocols for healthcare in WBAN: A comparative analysis. *Wirel. Pers. Commun.* **2022**, *122*, 1767–1806. [CrossRef] [PubMed]
17. Arif, M.S.; Mukheimer, A.; Asif, D. Enhancing the Early Detection of Chronic Kidney Disease: A Robust Machine Learning Model. *Big Data Cogn. Comput.* **2023**, *7*, 144. [CrossRef]
18. Ahmad, N.; Shahzad, B.; Arif, M.; Izdrui, D.; Ungurean, I.; Geman, O. An energy-efficient framework for WBAN in health care domain. *J. Sensors* **2022**, *2022*, 5823461. [CrossRef]
19. Cornet, B.; Fang, H.; Ngo, H.; Boyer, E.W.; Wang, H. An overview of wireless body area networks for mobile health applications. *IEEE Netw.* **2022**, *36*, 76–82. [CrossRef]
20. Zhong, L.; He, S.; Lin, J.; Wu, J.; Li, X.; Pang, Y.; Li, Z. Technological Requirements and Challenges in Wireless Body Area Networks for Health Monitoring: A Comprehensive Survey. *Sensors* **2022**, *22*, 3539. [CrossRef]
21. Jegadeesan, S.; Azees, M.; Babu, N.R.; Subramaniam, U.; Almakhles, J.D. EPAW: Efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs). *IEEE Access* **2020**, *8*, 48576–48586. [CrossRef]
22. Peng, K.; Li, M.; Huang, H.; Wang, C.; Wan, S.; Choo, K.K.R. Security challenges and opportunities for smart contracts in Internet of Things: A survey. *IEEE Internet Things J.* **2021**, *8*, 12004–12020. [CrossRef]
23. Abdulmalek, S.; Nasir, A.; Jabbar, W.A.; Almuhaya, M.A.; Bairagi, A.K.; Khan, M.A.M.; Kee, S.H. IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review. *Healthcare* **2022**, *10*, 1993. [CrossRef]
24. Wang, G.; Badal, A.; Jia, X.; Maltz, J.S.; Mueller, K.; Myers, K.J.; Niu, C.; Vannier, M.; Yan, P.; Yu, Z.; et al. Development of metaverse for intelligent healthcare. *Nat. Mach. Intell.* **2022**, *4*, 922–929. [CrossRef]
25. Cheikhrouhou, O.; Mershad, K.; Jamil, F.; Mahmud, R.; Koubaa, A.; Moosavi, S.R. A lightweight blockchain and fog-enabled secure remote patient monitoring system. *Internet Things* **2023**, *22*, 100691. [CrossRef]
26. Radhakrishnan, N.; Muniyandi, A.P. Dependable and provable secure two-factor mutual authentication scheme using ecc for iot-based telecare medical information system. *J. Healthc. Eng.* **2022**, *2022*, 9273662. [CrossRef] [PubMed]
27. Kumar, A.; Saha, R.; Conti, M.; Kumar, G.; Buchanan, W.J.; Kim, T.H. A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions. *J. Netw. Comput. Appl.* **2022**, *204*, 103414. [CrossRef]

28. Challa, S.; Wazid, M.; Das, A.K.; Kumar, N.; Reddy, A.G.; Yoon, E.J.; Yoo, K.Y. Secure signature-based authenticated key establishment scheme for future IoT applications. *IEEE Access* **2017**, *5*, 3028–3043. [CrossRef]
29. Ashraf, Z.; Sohail, A.; Yousaf, M. Robust and lightweight symmetric key exchange algorithm for next-generation IoE. *Internet Things* **2023**, *22*, 100703. [CrossRef]
30. Ashraf, Z.; Sohail, A.; Yousaf, M. Lightweight and authentic symmetric session key cryptosystem for client–server mobile communication. *J. Supercomput.* **2023**, *79*, 16181–16205. [CrossRef]
31. Jia, X.; He, D.; Li, L.; Choo, K.K.R. Signature-based three-factor authenticated key exchange for internet of things applications. *Multimed. Tools Appl.* **2018**, *77*, 18355–18382. [CrossRef]
32. Zhou, L.; Li, X.; Yeh, K.H.; Su, C.; Chiu, W. Lightweight IoT-based authentication scheme in cloud computing circumstance. *Future Gener. Comput. Syst.* **2019**, *91*, 244–251. [CrossRef]
33. Masud, M.; Gaba, G.S.; Alqahtani, S.; Muhammad, G.; Gupta, B.B.; Kumar, P.; Ghoneim, A. A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care. *IEEE Internet Things J.* **2020**, *8*, 15694–15703. [CrossRef] [PubMed]
34. Farash, M.S.; Turkanović, M.; Kumari, S.; Hölbl, M. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. *Ad Hoc Netw.* **2016**, *36*, 152–176. [CrossRef]
35. Amin, R.; Islam, S.H.; Biswas, G.; Khan, M.K.; Leng, L.; Kumar, N. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Comput. Netw.* **2016**, *101*, 42–62. [CrossRef]
36. Sharma, G.; Kalra, S. A lightweight user authentication scheme for cloud-IoT based healthcare services. *Iran. J. Sci. Technol. Trans. Electr. Eng.* **2019**, *43*, 619–636. [CrossRef]
37. Subramani, J.; Maria, A.; Rajasekaran, A.S.; Al-Turjman, F. Lightweight privacy and confidentiality preserving anonymous authentication scheme for WBANs. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3484–3491. [CrossRef]
38. Wazid, M.; Das, A.K.; Shetty, S.; JPC Rodrigues, J.; Park, Y. LDAKM-EIoT: Lightweight device authentication and key management mechanism for edge-based IoT deployment. *Sensors* **2019**, *19*, 5539. [CrossRef]
39. Masud, M.; Gaba, G.S.; Choudhary, K.; Hossain, M.S.; Alhamid, M.F.; Muhammad, G. Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. *IEEE Internet Things J.* **2021**, *9*, 2649–2656. [CrossRef]
40. Rana, M.; Shafiq, A.; Altaf, I.; Alazab, M.; Mahmood, K.; Chaudhry, S.A.; Zikria, Y.B. A secure and lightweight authentication scheme for next generation IoT infrastructure. *Comput. Commun.* **2021**, *165*, 85–96. [CrossRef]
41. Kaul, S.D.; Awasthi, A.K. Security enhancement of an improved remote user authentication scheme with key agreement. *Wirel. Pers. Commun.* **2016**, *89*, 621–637. [CrossRef]
42. Son, S.; Park, Y.; Park, Y. A secure, lightweight, and anonymous user authentication protocol for IoT environments. *Sustainability* **2021**, *13*, 9241. [CrossRef]
43. Rajaram, S.; Maitra, T.; Vollala, S.; Ramasubramanian, N.; Amin, R. eUASBP: Enhanced user authentication scheme based on bilinear pairing. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 2827–2840. [CrossRef]
44. Kumar Chaudhary, R.R.; Chatterjee, K. A Lightweight PUF based Multi-factor Authentication Technique for Intelligent Smart Healthcare System. *Peer Peer Netw. Appl.* **2023**, *16*, 1975–1992. [CrossRef]
45. Chen, C.M.; Liu, S.; Chaudhry, S.A.; Chen, Y.; Khan, M.A. A Lightweight and Robust User Authentication Protocol with User Anonymity for IoT-Based Healthcare. *CMES-Comput. Model. Eng. Sci.* **2022**, *131*. [CrossRef]
46. Dolev, D.; Yao, A. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208. [CrossRef]
47. Kelly, S.; Frankel, S. Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec; RFC 4868. 2007. Available online: https://www.rfc-editor.org/info/rfc4868 (accessed on 17 September 2023).
48. AVISPA Code and Simulation Results. GitHub. 2023. Available online: https://www.github.com/zashraf-sudo/researchpaper-6-code (accessed on 15 October 2023).
49. Shuai, M.; Yu, N.; Wang, H.; Xiong, L. Anonymous authentication scheme for smart home environment with provable security. *Comput. Secur.* **2019**, *86*, 132–146. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.