electronics

MDPI

Article

Cross-SN: A Lightweight Authentication Scheme for a Multi-Server Platform Using IoT-Based Wireless Medical Sensor Network

Haqi Khalid [1,*,†], Shaiful Jahari Hashim [1,*,†], Sharifah Mumtazah Syed Ahmad [1,†] and Fazirulhisyam Hashim [1,†] and Muhammad Akmal Chaudhary [2]

[1] Department of Computer and Communication Systems Engineering, Faculty of Engineering, Universiti Putra Malaysia, Serdang 43400, Malaysia; s_mumtazah@upm.edu.my (S.M.S.A.); fazirul@upm.edu.my (F.H.)
[2] Department of Electrical and Computer Engineering, College of Engineering and Information Technology, Ajman University, Ajman 346, United Arab Emirates; m.akmal@ajman.ac.ae
* Correspondence: haqikhalid1@gmail.com (H.K.); sjh@upm.edu.my (S.J.H.)
† These authors contributed equally to this work.

Abstract: Several wireless devices and applications can be connected through wireless communication technologies to exchange data in future intelligent health systems (e.g., the Internet of Medical Things (IoMT)). Smart healthcare requires ample bandwidth, reliable and effective communications networks, energy-efficient operations, and quality of service support (QoS). Healthcare service providers host multi-servers to ensure seamless services are provided to the end-users. By supporting a multi-server environment, healthcare medical sensors produce many data transmitted via servers, which is impossible in a single-server architecture. To ensure data security, secure online communication must be considered since the transmitted data are sensitive. Hence, the adversary may try to interrupt the transmission and drop or modify the message. Many researchers have proposed an authentication scheme to secure the data, but the schemes are vulnerable to specific attacks (modification attacks, replay attacks, server spoofing attacks, Man-in-the middle (MiTM) attacks, etc.). However, the absence of an authentication scheme that supports a multi-server security in such a comprehensive development in a distributed server is still an issue. In this paper, a secure authentication scheme using wireless medical sensor networks for a multi-server environment is proposed (Cross-SN). The scheme is implemented with a smart card, password, and user identity. Elliptic curve cryptography is utilized in the scheme, and Burrows–Abadi–Needham (BAN) logic is utilized to secure mutual authentication and to analyse the proposed scheme's security. It offers adequate protection against replies, impersonation, and privileged insider attacks and secure communication in multi-server parties that communicate with each other.

Keywords: authentication; security; WSN; multi-server environment; WMSN

Citation: Khalid, H.; Hashim, S.J.; Syed Ahmad, S.M.; Hashim, F.; Chaudhary, M.A. Cross-SN: A Lightweight Authentication Scheme for a Multi-Server Platform Using IoT-Based Wireless Medical Sensor Network. *Electronics* **2021**, *10*, 790. https://doi.org/10.3390/electronics10070790

Academic Editors: Neetesh Saxena, Prosanta Gope and Daisuke Mashima

Received: 31 December 2020
Accepted: 22 February 2021
Published: 26 March 2021

1. Introduction

The Internet of Things (IoT) technology allows healthcare to shift from traditional hub-based systems to customized eHealth systems, allowing for more preventive intervention, lower overall costs, improved patient attention, and increased sustainability. By offering to everyone unobtrusive monitoring and highly personalized rich medical information and successful clinical choices, efficient IoT-enabled eHealth systems can be implemented [1]. Wireless sensor networks (WSNs) are essential parts of the IoT architecture. WSNs consist of low-power sensors with low processing and limited resources [2]. The main task of the sensor is to collect and send data through the outside gateway. WSNs play an essential role in IoT health applications. Health and health services profit from WSNs, which offer practical applications such as real-time patient monitoring, medical administration, diagnostic support, patient tracking systems in a hospital, etc. A wide range of fields has been

used to develop the Wireless Sensor Network (WSN), such as environmental assessment, military detection, industry monitoring, healthcare, etc., technical developments in wireless networking, low-power integrated systems, and sensors [3]. WSN is gaining ever more interest from academia and the industry due to its bright prospects in many applications. WSNs primarily aim to deploy a collection of sensor devices over an isolated area and to collect and transmit environmental data to a base or remote station. The raw data are subsequently processed online or offline according to application specifications for a comprehensive review on a remote server [4,5]. Remote patient monitoring is beneficial for doctors if the patient is outside the hospital. Wireless medical sensor networks (WMSNs) are at the root of this idea, and its implementation is a crucial issue to achieve this potential [6,7]. In the 21st century, the healthcare industry witnessed drastic developments due to Wireless Medical Sensor Networks (WMSN) in health applications [8]. WSNs in different healthcare applications are growing at an unprecedented rate in developed and developing countries to provide a high standard of treatment [9]. The sensors then obtain physiological data from patients, such as heartbeat rates, pulses, temperature, etc. Healthcare professionals can access wireless monitoring through handheld devices in real-time. In this context, wireless sensors' technology can give useful tools for health monitoring of the elderly and continuously monitoring patients. Thus, wireless sensor networks are an exciting and growing area of healthcare for scientific research. Internet of Medical Things (IoMT) comprises many entities, including health centers, emergency centers, medical equipment, and users of e-health (including patients, physicians, pharmacists, medical researchers, etc.). A Wireless Body Area Network (WBAN) consists of nodes and hubs of sensors/actuators operating in, on, or around a body (but not limited to human bodies) and serving a range of medical and non-medical applications [10]. Indeed, in an old-world, the future of modern healthcare would require omnipresent health surveillance with the least successful contact between doctor and patient [11–13]. The gateway and users usually have extensive capacity for storage and processing, but sensors change. A sensor is fitted with weak resources, including a limited memory and low battery power. It is, therefore, necessary to economically use the sensors. If someone unlawfully gathers patient data, the patient's privacy is breached. If the patient's data is corrupted, medical professionals may diagnose incorrectly, leading to dire consequences [14]. It is, therefore, essential to have a secure environment for communication. Different security vulnerabilities were explored, including insecure authentication schemes [15,16]; these include mutual authentication, sensor node detection, offline password detection, key impersonation, and attack privileges. As the distributed system is commonly used, increasingly multi-server environments will provide secure and robust network services [12,17].

In a multi-server environment, healthcare providers host many servers to provide an efficient and reliable service to the users. The number of servers is increasing recently, which leads to more identities and passwords that users need to remember and causes a high database cost. The traditional single server architecture does not meet the user's needs due to the growing number of users. In addition, sensitive information transmitted through the servers must be secured in online communication. Moreover, the identity and passwords that the user uses are not secured when the same set are used to register with different servers. However, many authentication schemes with conventional authentication principles such as passwords and usernames were proposed to comply with realistic application requirements. Passwords and usernames can, however, be revealed or forgotten and may be devalued. The current researches cannot stand up separately to impersonation attacks and spoofing attacks. A robust user authentication protocol (i.e., competent authentication) has not yet been adequately addressed at the application level to prevent unauthorized access to wireless medical sensor data. Authentication of the user is vital in such wireless medical applications. The architecture of the wireless medical sensor network in a multi-server environment is shown in Figure 1. This article proposes a secure authentication scheme for secure and trustworthy communication via a wireless network

of medical sensors, the proposed scheme, based on smart cards and on usernames and passwords in a multi-server environment (Cross-SN).

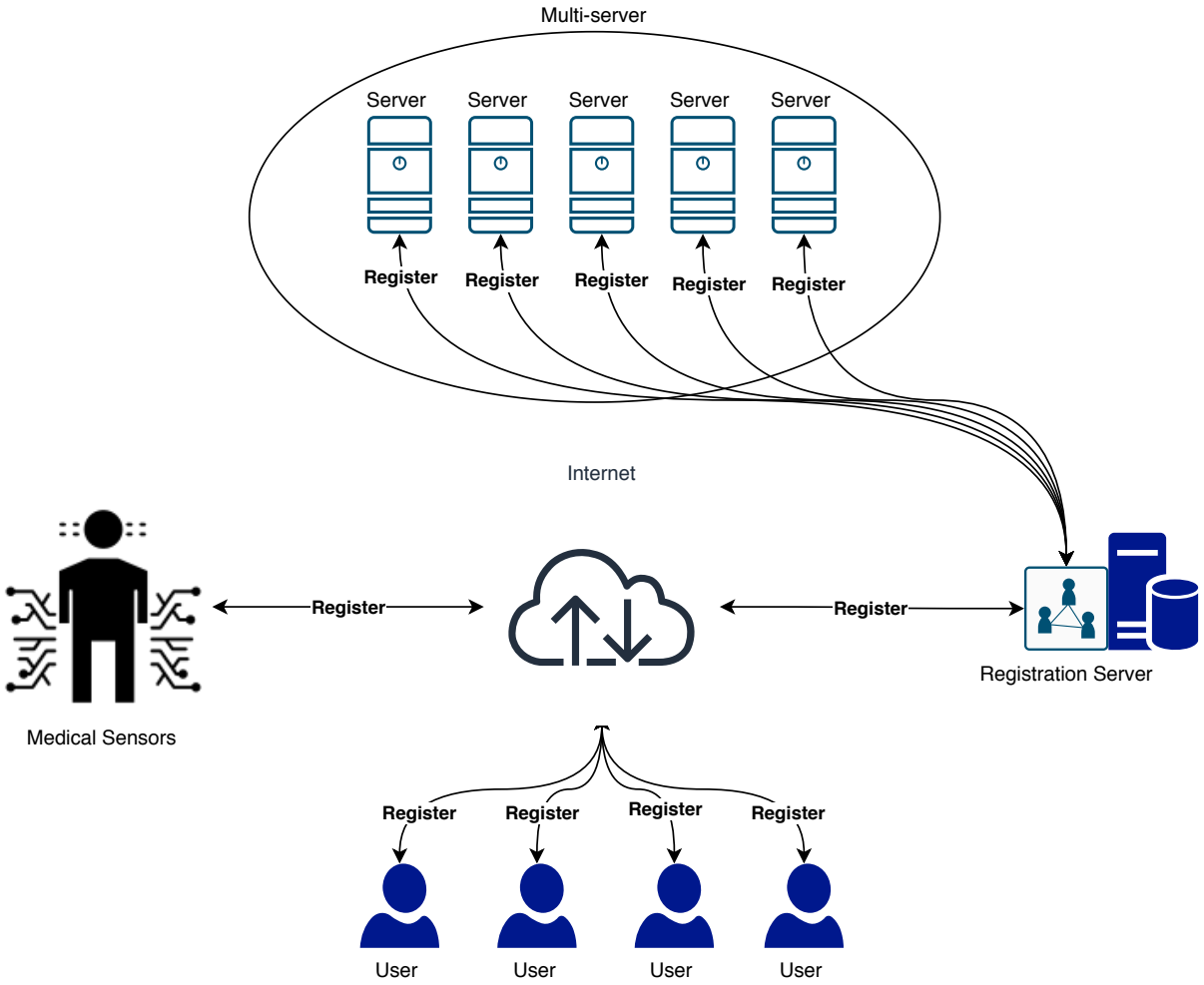

Figure 1. Wireless medical sensor network in multi-server environment.

2. Related Works

In the area of health and medical applications, IoT has great potential. Some IoT-related technologies are of particular interest, such as body zone sensors, advanced healthcare systems, wearable sensors, wireless cloud networks, storage and display of clinical data, etc. In 2012, Kumar et al. [18] proposed a WMSN authentication protocol to track a patient's health and claimed that this could protect the protocol against established threats to security. Their protocol is efficient as they use only symmetrical encryption and hash function to protect communication protection. They introduced an Efficient Strong Authentication Protocol (E-SAP) for WMSN healthcare applications. They also suggested that the user needs to authenticate using the MS Node and to set the session key. In terms of cost and protection, they considered their scheme better than other existing protocols. However, [10] explains that the protocol [18] is ineffective against security threats. Wu et al. (2017) [19] developed a WMSN-based, stable, two-factor remote authentication scheme. Their device is more potent than current schemes and is immune to known safety threats. The device sends a validation code to pairs (for instance, cell phones or smart cards) that generate keys. Proverif Blanchet and Smyth are used to validate the proposed scheme's protection to battle various attacks (2011). A study and comparison of the scheme also revealed that it is acceptable for customized systems of healthcare (PHS). It addresses traditional security and user untraceability criteria. They say that their scheme is immune to attacks, insider attacks, offline guessing, and main session disclosure

attacks but does not have forward confidentiality. Similarly, Ali et al. (2018) [20] developed an improved 3-factor authentication protocol for wireless healthcare applications. Burrows–Abadi–Needham and Automated Validation of Internet Security Protocols and Applications (AVISPA) were used to validate the security of their scheme. They thought they would patch their device for offline evaluation of passwords, user-independence attacks, documented temporary session-key information attacks, and identity devaluation attacks. Unfortunately, in 2019 [21], Shuai et al. showed that the system [20] was vulnerable to attacks on the user, deletion of passwords offline, and temporarily attacks on session-based key information. Yoney et al. (2018) [15] nevertheless introduced WBAN 's anonymous e-Healthcare User Authentication Scheme. The proposed scheme uses better elliptical cryptography and is secure to defend users against password guessing attacks and lost/stolen smart card verifier attacks. The author developed a user authentication framework to prevent the transmission of knowledge to intruders. The system offers good, easy, and convenient communication with calculations and controls. A structured security analysis was conducted using the AVISPA tool to validate the proposed structure. In parallel, in Li et al. (2019) [22], an Elliptic Curve Cryptography (ECC) based 3-factor wireless network sensor authentication protocol was developed using error correction code and fluent engagement schemes to manage biometric details and secrecy forward. To resolve the problem of local password search, the fuzzy checker and honey list techniques were also adopted when resisting attacks on mobile devices. While Li et al. used the fuzzy checker technique and argued its wireless medical sensor network protocol [22] fulfilling several safety features, we found that it could not withstand replay attacks. Shuai et al. implemented a three-factor authentication solution in 2019 [21] that is lightweight and effective for remote control of On-Body Wireless Networks (OBWN) patients. The proposed scheme adopts a specific hash chain technique for future users' anonymity, and a pseudonym identity is given to resist attacks of synchronization. The proposed framework adopts the pseudonym identity approach for user anonymity and provides possible confidentiality using a one-time hash chain technique. However, Mo et al. [23] have shown that their method [21] still has three security drawbacks: offline dictionary devaluation attacks, privileged insider attacks, and password change errors.

Although many researchers have proposed a large number of research in wireless medical sensor networks, we found out that the current research activities are still not considering authentication in heterogeneous networks, especially in a multi-server environment. In distributed systems, the transmitted data are sensitive and the adversary could interrupt the communication and attempts to drop, modify, or impersonate the message. Unfortunately, most of the proposed schemes still suffer certain attacks such as offline dictionary attacks, modification attacks, and insider attacks. Therefore, we designed a secure authentication scheme using a wireless medical sensor network in a multi-server environment. To design a secure authentication scheme for a wireless medical sensor network, a few security requirements must be considered, as shown in the following section.

3. Security Requirements of Medical Sensors

In IoMT, protection and privacy play critical roles, although most health-related organizations do not spend enough time protecting security and privacy. IoMT devices create an increasingly complex and susceptible amount of real-time data. The failure of the health system or protection of the network could have disastrous implications [24]. However, data security information for patients is given at all data handling, delivery, cloud storage, and data republication levels [24,25]. For medical security and privacy systems on the network of wireless medical sensors, the following four requirements should be considered [26].

- Mutual authentication: The proposed protocol should include mutual authentication to ensure participants' protection. Participants interacting should be authenticated [27].

- Data integrity: Data integrity refers to the fact that all data values' syntactic and semantic specifications are met without unauthorized interference. Two specific and reliable criteria are implemented. Data integrity can be divided into four categories: integrity of individuals, the integrity of places, referential integrity, and integrity defended by primary keys, controls, laws, and external triggers [25].
- Backward and Forward Secrecy: Backward and forward secrecy play critical roles in securing exchanged messages in previous and next communication. Therefore, any proposed scheme needs to provide this property to prevent adversaries from obtaining the session keys. In case the adversary receives the current session key, he/she cannot obtain the previous and next session key [28].
- Data Usability: The use of data implies the usage of data or data structures by approved users. Big data provides immense benefits and crucial challenges, including false data and non-standard data. Moreover, unauthorized access-caused data manipulation or failure often destroys data usability [29].
- Various attack resistance: In a multi-server environment, the authentication scheme should be able to resist specific passive and active attacks, practically in real-world applications [28].
- Key Agreement for Secure Session: The proposed scheme should provide a secure session key to encrypt communication and protect the authentication message between entities [26].

4. Preliminaries

The hash functions and elliptic curve cryptography used in this paper are described here. Table 1 contains a summary of the notations used in the rest of the article.

Table 1. Notations.

Notation	Abbreviation
SC	Smart Card
S_j	Server
RC	Registration Centre
S_n	Node Sensor
U_i	User
SID_j	Identity of server
k	Server's private key
NID_j	Identity of node sensor
$y, r_n, r_i, r_g, x,$	Random Numbers $\in Z_n^*$
id_u	User identity
pw_u	User Password
id_{rc}	Registration Centre identity
$h(.)$	Hash function

4.1. Hash Functions

A fixed hash value output size is generated by taking the input of of the string O = H(String). The output generated is called a hash code. A small change in the string value can make a significant difference [30]. A particular hash function has the following specifications:

- It is easy to find O = H(String) if the string is described.
- If O = H(String) is illustrated, the string cannot be identified.
- The difficult job is to differentiate between the inputs of String1 and String2, so H(String1) = H(String2). It has called collision resistance.

4.2. Elliptic Curve Cryptography

Assume that E/F_q is a set of points over a prime field F_q , which is defined by the following non-singular elliptic curve:

$$y^2 modq = (x^3 + ax + b) modq \quad (1)$$

where $x, y, a, b \in F_q$ and $(4a^3 + 27b^2) modq \neq 0$. A point $P(x, y)$ is an elliptic curve point if it satisfies Equation (1), and the elliptical curve equation is defined as $E_p(e, f) : c^2 = d^3 + f$ over the finite field $(d, c) \in W_p^* \times W_p, e, f$ and $4e^3 + 27f^2 \neq 0(modP)$, where P is a prime number and the size of P is $\geq$160 bits. The point multiplication is computed by repeated addition, $nP = P + P + P + ... + P(ntimes)$, over the defined t of $E_p(e, f)$, and n is the smallest positive integer. (e, f, t, P, n) belonging to finite field $F_p.E$ defines the Abelian group [31].

5. Cross-SN Scheme

We propose a lightweight multi-server authentication scheme using a wireless medical sensor network in this section. However, the proposed authentication system uses a smart card in a multi-server environment with wireless medical sensors. The architecture of the proposed scheme is illustrated in Figure 2. The scheme comprises five stages: the login and authentication process, the registration process of node sensors, registration of the device, and updating passwords.

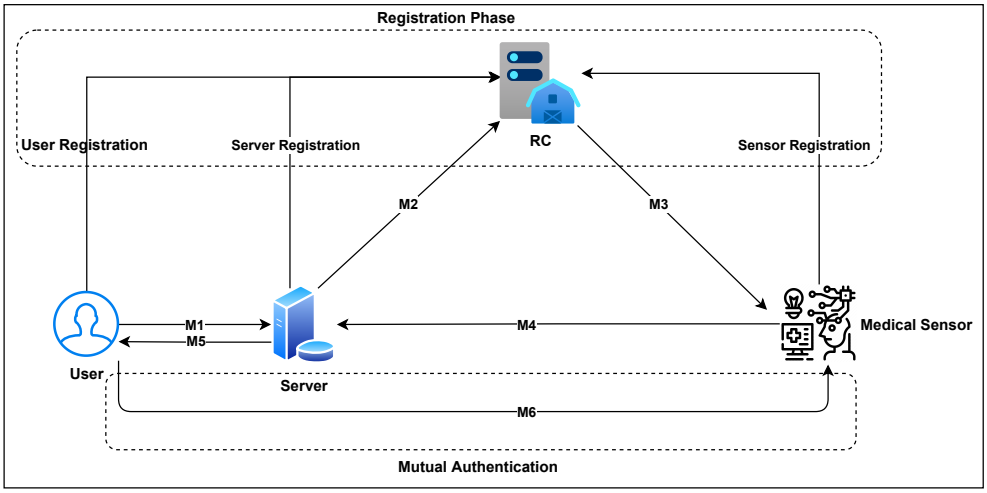

Figure 2. Proposed multi-server architecture.

5.1. Server Registration Phase

In this phase, the server Sj sends a registration center RC request to obtain their RC secret key. The steps of this phase are explained in detail in Figure 3 and listed as follow:

1. The server first selects an identity SID_j; then, through a secure channel, the message will be forwarded to the RC.
2. RC receives the server identity SID_j and computes $R_j = h(SID_j \parallel k)$; then, it sends the message R_j to the S_j.
3. Now, the server receives the message and store R_j securely.

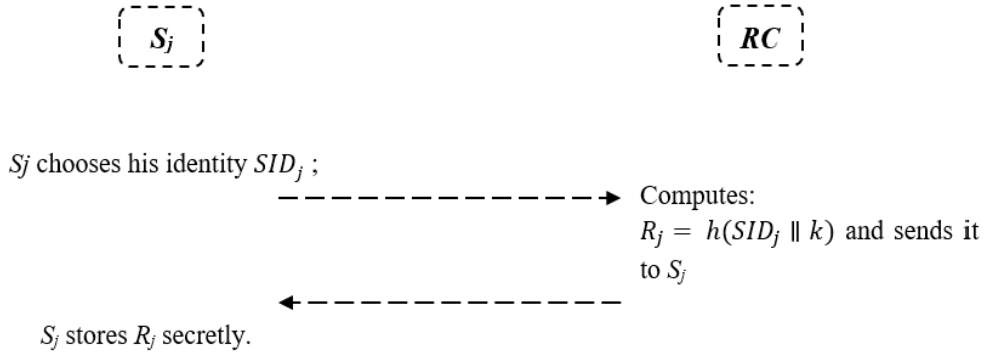

Figure 3. Server registration phase.

5.2. Sensor Node Registration Phase

In this phase, the sensor node requests to register itself in the RC to obtain their RC secret key. The registration steps are as presented in Figure 4, listed as follows:

1. First, the sensor node Sn selects NID_j and a random number y; then, it computes $V_i = h(NID_j \| y)$ and send the message $\{V_i, NID_j\}$ to RC through a secure channel.
2. RC receives the message $\{V_i, NID_j\}$; RC generates a random number rn computing $TC_j = h(NID_j \| r_n \oplus V_i)$ and stores NID_j, TC_j in its database. Then, RC sends TC_j to the sensor node through a secure channel.
3. After RC receives the message TC_j from the sensor node, Sn computes $G = TC_j \oplus V_i = h(NID_j \| y)$ and stores G into its memory, which is safe.

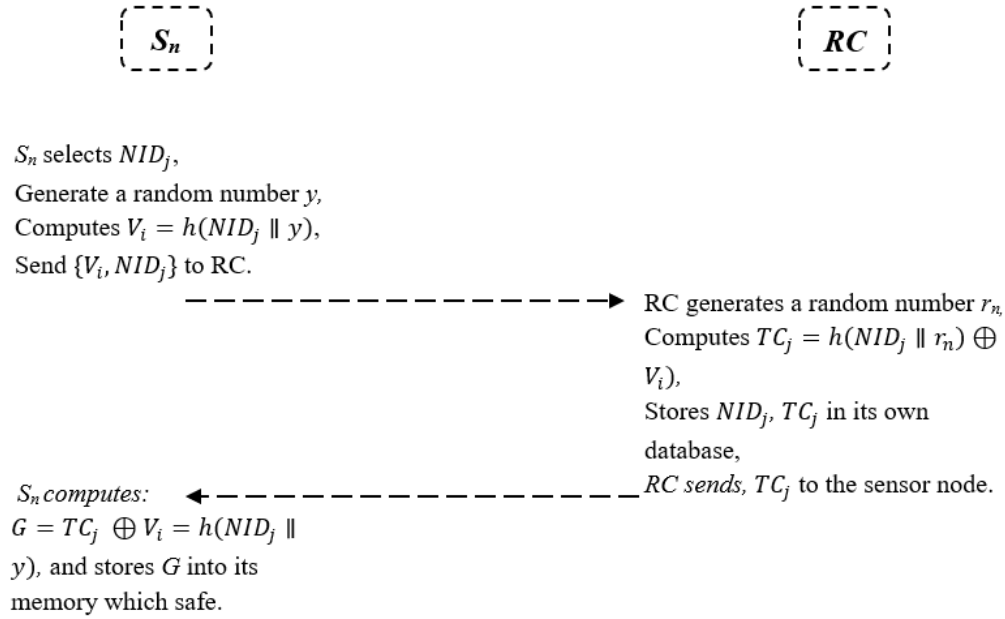

Figure 4. Sensor node registration phase.

5.3. User Registration Phase

First, the RC receives a request message from the user Ui and acquires the SC with the secret key in it, received earlier from the RC. Figure 5 shows the registration steps described as follows:

1. After the user, U_i, inserts the smart card and selects the identity id_u and password pw_u, he/she chooses a random number r_i and, then, sends the message $\{id_u, h(pw_u \| r_i)\}$ to RC via a secure channel;
2. Now, the RC has the message $\{id_u, h(pw_u \| r_i)\}$ and generates a random number rrc. Later, it calculates $R_i = h(id_u \| id_{rc} \| k)$, $Z_i = R_i \oplus h(pw_u \| r_i)$, where k is RC's secret

key. After that, RC stores $\{h(.), Zi\}$ into a smart card. RC finally sends the embedded SC to the user U_i.

3. The user stores $\{h(.), Z_i\}$ into the smart card.

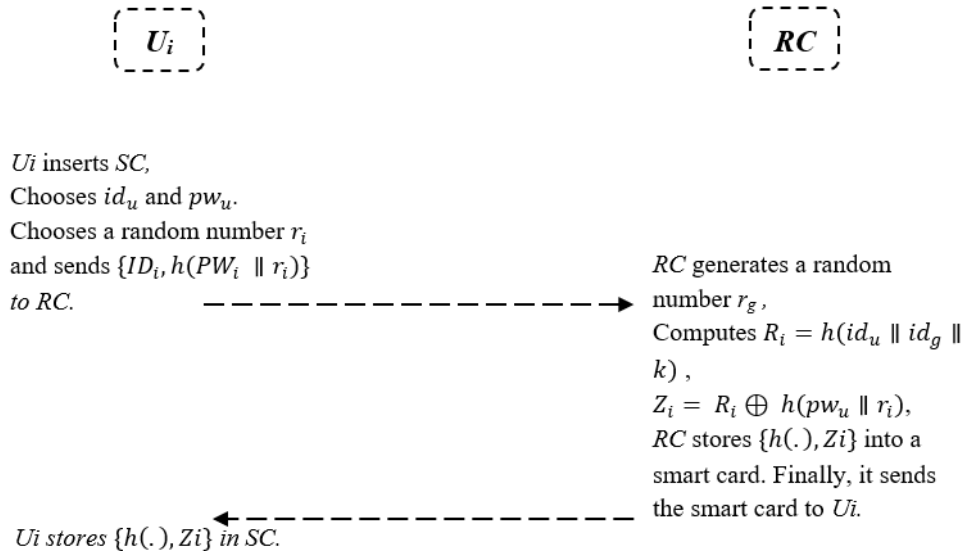

Figure 5. User registration phase.

5.4. Login and Authentication Phase

The RC plays the third party's role for login and authentication of user U_i and S_j server. The user and the server have a generated session key for future communication. The steps are shown simply in Figure 6 and listed as follow:

1. The user U_i first inserts his/her smart card and types the username id_u and password pw_u. It chooses a random number $x \in Z_n^*$ to compute $R_i = Z_i \oplus h(pw_u \| r_i)$, $X = xP, X^* = xP_{pub}$, $CID_i = id_u \oplus h(X^*)$, and $\alpha = h(id_i \| SID_j \| R_i \| X \| X^*)$.$Ui$ sends the message $\{CID_i, X, \alpha\}$ to S_j.
2. Upon receiving the message $\{CID_i, X, \alpha\}$, server S_j selects a random number $y \in Z_n^*$, and calculates $Y = yP, Y^* = yP_{pub}$, $\beta = h(CID_i \| X \| \alpha \| SID_j \| R_j \| Y \| Y^*)$, and $CSID_j = SID_j \oplus h(Y^*)$. Then, it sends $\{CID_i, X, \alpha, CSID_j, Y, \beta\}$ to RC.
3. The RC receives $\{CID_i, X, \alpha, CSID_j, Y, \beta\}$, and computes $Y^* = kY, SID_j = CSID_j \oplus h(Y^*)$ and $R_j = h(SID_j \| k)$. It then verifies β and $h(CID_i \| X \| \alpha \| SID_j \| R_j \| Y \| Y^*)$. If not valid, end the session; else, RC calculates $X^* = kX$, $id_u = CID_i \oplus h(X^*)$, and $R_i = h(id_u \| k)$. Also, verify α by computing $h(id_u \| SID_i \| R_i \| X \| X^*)$. If valid, $TID_i = id_i \oplus h(Y \| Y^* \| R_j)$, $\phi = h(id_u \| TID_i \| X \| SID_j \| NID_j \| Y \| R_j)$, $TSID_j = SID_j \oplus h(X \| X^* \| R_i)$, and $\varphi = h(id_u \| X \| X^* \| SID_j \| NID_j \| Y \| R_i)$. Otherwise, it ends the session. Later, the RC sends $\{TID_i, \phi, TSID_j, \varphi\}$ to the sensor node Sn.
4. The sensor node receives the message $\{TID_i, \phi, TSID_j, \varphi\}$, and computes $id_u = TID_i \oplus h(Y \| Y^* \| R_j)$. Then, validate the identity id_u. If not, end the session; otherwise, it validates ϕ and $h(id_u \| TID_i \| X \| SID_j \| NID_j \| Y \| R_j)$. If valid, it calculates the session key $SK = yX = xyP$ and $\eta = h(id_u \| SID_j \| X \| Y \| SK \| \varphi)$; else, end the session. After that, Sn sends the message $\{TSID_j, Y, \varphi, \eta\}$ to Sj.
5. The message $\{TSID_j, Y, \varphi, \eta\}$ is now received by the Sj to calculate $SID_j = TSID_j \oplus h(X \| X^* \| R_i)$. It validates φ and $h(id_u \| X \| X^* \| SID_j \| Y \| R_i)$. If valid, it computes the session key $SK = xY = xy$P and checks whether $\eta = h(id_u \| SID_j \| X \| Y \| SK \| \varphi)$; if not, the server ends the session.

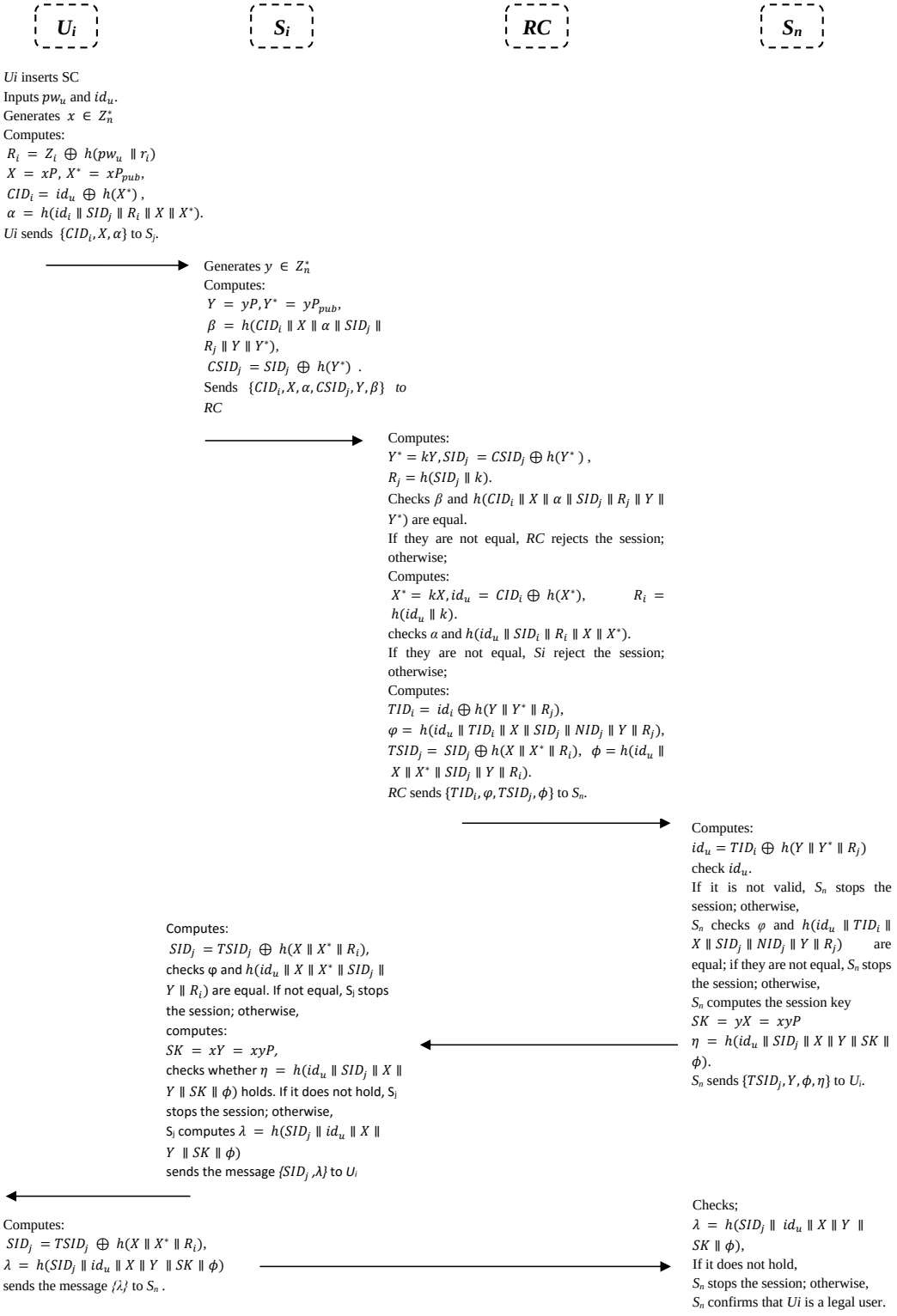

Figure 6. Login and authenticated key exchange phase.

Then, it computes $\lambda = h(SID_j \| id_u \| X \| Y \| SK \| \varphi)$ and sends the message $\{SID_j, \lambda\}$ to Ui.

1. The user receives $\{SID_j, \lambda\}$, and computes $SID_j = TSID_j \oplus h(X \| X^* \| R_i)$, and $\lambda = h(SID_j \| id_u \| X \| Y \| SK \| \varphi)$; then, it sends $\{\lambda\}$ to the sensor node Sn.
2. Sn checks λ by calculating $\lambda = h(SID_j \| id_u \| X \| Y \| SK \| \varphi)$. If it does not hold, it ends the session; otherwise, Sn confirms that U_i is a legal user.

5.5. Password Updates Phase

In this phase, the user can change or update the used password pw_u to a new password $pw_u^{(+1)}$. The executed steps of this phase are listed as follow:

1. After inserting the SC into a card reader, the user types pw_u and id_u.Then, U_i has to type the newly selected password pw_u^{+1}.
2. SC calculates $Rep(b_u^*, \vartheta_i) = \sigma_i$, $R_i = Z_i \oplus h(pw_u \parallel \sigma_i)$, and $Z_i^{new} = R_i \oplus h(pw_u^{+1} \parallel \sigma_i)$.
3. Finally, Z_i is replaced with Z_{new}.

6. Security Analysis

The security of the proposed scheme is analyzed in terms of security in this section. Based on the widely known formal analysis tool, Burrows-Abadi-Needham (BAN) logic [32] is applied to demonstrate the proposed scheme's validity and practicality. The BAN logic is widely used to prove the scheme's mutual authentication and was utilized in [33,34], for example. In addition, informal security analysis will be further discussed in this section against specific known attacks and ensures that the proposed scheme meets the necessary security requirements of medical sensors and a multi-server platform.

6.1. BAN Logic Proof

In this section, the popular formal BAN mode logic is used to validate cryptographic protocols. The notes and logical rules used in BAN logic are illustrated in Table 2.

Table 2. Notations and logical rules.

Notation	Abbreviation
$P\mid\equiv X$	P believes X
(X)	X is fresh
$P \Rightarrow X$	P has jurisdiction over X
$P \lhd X$	P sees X
$P\mid\sim X$	P once said X
(X, Y)	X or Y is one part of (X, Y)
$< X >_Y$	X combined with Y
$(X)_Y$	X is fresh with the key K
$P \xrightarrow{k} Q$	P and Q use the shared key K to communicate
SK	The current session key
$\frac{P\mid\equiv P\overset{k}{\leftrightarrow}Q, P\lhd\{X\}_k}{P\mid\equiv Q\mid\sim X}$	The message-meaning rule
$\frac{P\mid\equiv(X)}{P\mid\equiv(X,Y)}$	The freshness-conjuncatenation rule
$\frac{P\mid\equiv(X), P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$	The nonce verification
$\frac{P\mid\equiv QX, P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$	The jurisdiction rule

Goals: We first identify the main entities that will be used in BAN logic. Four entities represent the proposed scheme: the user (Ui), server (Sj), registration center (RC), and the medical sensor node (Sn). The procedure of the BAN logic is demonstrated theoretically in the following sections to meet the following goals:

- Goal 1: $U_i\mid\equiv U_i \xleftrightarrow{sk} S_j$.
- Goal 2: $U_i\mid\equiv U_i \xleftrightarrow{sk} S_n$.
- Goal 3: $S_j\mid\equiv U_i \xleftrightarrow{sk} S_j$.
- Goal 4: $S_n\mid\equiv U_i \xleftrightarrow{sk} S_n$.

Messages: The messages of the proposed scheme should be changed to the idealized form, shown as follows:

- Msg 1: $U_i \Rightarrow RC : (CID, X)_{h(id_u \| k)}$.
- Msg 2: $S_j \Rightarrow RC : (id_u, X, SID, Y)_{h(SID \| k)}$.
- Msg 3: $RC \Rightarrow Sn : (TID, TSID)_{h(id_u \| X \| X' \| SID)}$.
- Msg 4: $Sn \Rightarrow Sj : (TSID, Y, \phi, n)_{h(id_u \| SID \| X \| Y \| sk \| \phi)}$.
- Msg 5: $S_j \Rightarrow Ui : (SID, \lambda)_{h(SID \| id_u \| X \| Y \| sk)}$.
- Msg 6: $U_i \Rightarrow Sn : (\lambda)_{h(id_u \| X \| Y \| sk \| \phi)}$.

Assumption: The following assumptions are essential for a systematic analysis using BAN logic for the initial status of the proposed scheme:

- A1: $Ui| \equiv (X)$.
- A2: $Sj| \equiv (Y)$.
- A3: $Ui| \equiv S_j \xleftrightarrow{h(id_u \| k)} RC$
- A4: $Sj| \equiv S_j \xleftrightarrow{h(SID \| k)} RC$.
- A5: $RC| \equiv U_i \xleftrightarrow{h(Id_u \| k)} RC$.
- A6: $Sj| \equiv S_j \xleftrightarrow{h(SID \| k)} RC$.
- A7: $RC| \equiv S_j \xleftrightarrow{h(SID \| k)} RC$.
- A8: $Sn| \equiv RC \xleftrightarrow{h(id_u \| k)} Sn$.
- A9: $Sn| \equiv S_j \xleftrightarrow{h(SID \| k)} Sn$.
- A10: $Ui| \equiv RC \Rightarrow (U_i \xleftrightarrow{Y} S_j)$.
- A11: $S_j| \equiv RC \Rightarrow (U_i \xleftrightarrow{X} S_j)$.
- A12: $Sn| \equiv RC \Rightarrow (U_i \xleftrightarrow{Y} Sn)$.
- A13: $Sn| \equiv U_i \Rightarrow (U_i \xleftrightarrow{sk} Sn)$.
- A14: $U_i| \equiv Sn \Rightarrow (U_i \xleftrightarrow{sk} Sn)$.

Analysis: We carry out verification of the proposed scheme according to the above assumptions and BAN logic rules:

1. **Message 1:** $U_i \Rightarrow RC : (CID, X)_{h(id_u \| k)}$.
   - S1) RC $\triangleleft (id_u, X)_{(h(id_u \| k))}$.// The message-meaning rule is applied according to assumption A4 to obtain the following:
   - S2) $Sj| \equiv Ui|(id_u, X)$.// We could obtain it according to Msg 2.
2. **Message 2:** $S_j \Rightarrow RC : (id_u, X, SID, Y)_{h(SID \| k)}$.
   - S3) RC $\triangleleft (id_u, X, SID, Y)_{h(SID \| k)}$.// Based on the assumption A6, the message-meaning is applied to obtain
   - S4) RC $| \equiv Sj|(id_u, X, SID, Y)$.// Then, we obtain S5, according to Msg 3.
3. **Message 3:** $RC \Rightarrow Sn : (TID, TSID)_{h(id_u \| X \| X' \| SID)}$.
   - S5) Sn $\triangleleft (TID, \varphi, TSID, \phi, RC \xleftrightarrow{Y} Sn)$.// The message meaning is applied to obtain S6 based on assumption A4.
   - S6) Ui $| \equiv RC|(id_u, SID, X, Y, Ui \xleftrightarrow{Y} S_j)$. // We applied the freshness conjuncatention based on assumption A3 to obtain S7.
   - S7) Ui $| \equiv RC| \equiv (id_u, SID, X, Y, Ui \xleftrightarrow{Y} S_j)$. // Then, we apply the BAN logic rule to break conjunction according to S7.
   - S8) Ui $| \equiv RC| \equiv (Ui \xleftrightarrow{Y} S_j)$. //Under assumption A7, we apply the law of competence to obtain
   - S9) Ui $| \equiv (Ui \xleftrightarrow{Y} S_j)$. // According to $sk = yx = xyp$, we could obtain
   - S10) Ui $| \equiv (Ui \xleftrightarrow{sk} S_j)$. **Goal 1.**

4. **Message 4:** $Sn \Rightarrow Sj : (TSID, Y, \phi, n)_{h(id_u \| SID \| X \| Y \| sk \| \phi)}$.
   - S11) Sj $\triangleleft$ $(TSID, Y, \phi, Sn \xleftrightarrow{X} S_j)_{h(id_u \| SID \| X \| Y)}$ // We applied the message meaning according to assumption A7 to obtain
   - S12) Sj $\mid \equiv RC \mid (id_u, SID, X, Y, U_i \xleftrightarrow{X} Sn)_{h(SID \| k)}$. // We apply the freshness conjuncatention rule to obtain S13 under assumption A2.
   - S13) Sn $\mid \equiv RC \mid \equiv (id_u, SID, X, Y, U_i \xleftrightarrow{X} Sn)$ .// Again, the BAN logic rule is extended to break conjunctions.
   - S14) Sn $\mid \equiv RC \mid \equiv (U_i \xleftrightarrow{X} Sn)$. // According to $sk = yx = xyp$, we could obtain
   - S16) Sn $\mid \equiv (U_i \xleftrightarrow{sk} Sn)$. **Goal 2.**
5. **Message 5:** $S_j \Rightarrow Ui : (SID, \lambda)_{h(SID \| id_u \| X \| Y \| sk)}$.
   - S17) Sj $\triangleleft$ $(id_u, SID, X, Y, Sj \xleftrightarrow{X} Ui)$. // We apply the message sense rule according to assumption A10.
   - S18) Sj $\mid \equiv Ui \mid \equiv (id_u, SID, X, Y, Ui \xleftrightarrow{sk} Sj)$. // We apply the A1 freshness conjuncatenation rule.
   - S19) Ui $\mid \equiv Sj \mid \equiv (id_u, SID, X, Y, Ui \xleftrightarrow{sk} Sj)$.// Then, we apply the BAN logic rule for breaking the S20 conjunction.
   - S20) Ui $\mid \equiv Sj \mid \equiv Ui \xleftrightarrow{sk} Sj$. // **Goal 3.**
6. **Message 6:** $U_i \Rightarrow Sn : (\lambda)_{h(id_u \| X \| Y \| sk \| \phi)}$.
   - S21) Sn $\triangleleft$ $(id_u, SID, X, Y, Ui \xleftrightarrow{sk} Sn)_{sk}$.// We use the message meaning rule to get S22.
   - S22) Sn $\mid \equiv Ui \mid (id_u, SID, X, Y, Ui \xleftrightarrow{sk} Sn)$. // Again, under assumption A13, we use the freshness conjuncatention rule.
   - S23) Sn $\mid \equiv Ui \mid \equiv (id_u, SID, X, Y, Ui \xleftrightarrow{sk} Sn)$. // Then, we apply BAN to break the conjunction in order to produce
   - S24) Sn $\mid \equiv Ui \mid \equiv Ui \xleftrightarrow{sk} Sn$. **Goal 4.**

As is evident, S7 establishes goal 1, S13 establishes goal 2, S19 establishes goal 3, and S23 shows goal 4. This finally indicates that a session key between the user and the medical sensor is recognized and ensures that they connect mutually.

6.2. Informal Security Analysis

The proposed scheme is analysed informally and discusses the security of the proposed scheme against such known attacks, and the ability to withstand these attacks (e.g., stolen verifier attacks and man-in-the-middle attacks) are security requirements for the multi-server platform and medical sensors. Table 3 shows a comparison of the security properties of the proposed scheme against other schemes.

- Multi-server Support: From the abovementioned, we know that Ui has access to numerous services from different servers and only needs to register with RC once. One authentication password is required for the user to remember. The proposed framework is, therefore, suitable for configuration of the multi-server.
- Data integrity: In the proposed scheme, the one-way hash function h(.) is used to protect the identity and the password before transmission, which modifies the message to be impossible $\alpha = h(id_i \parallel SID_j \parallel R_i \parallel X \parallel X^*)$. In addition, the information is attached to a random number $x \in Z_n^*$ that it generates freshly. Therefore, the message's modification is difficult in our scheme; thus, it provides data integrity.
- Backward and forward secrecy support: If the attackers know the current session key, it will be challenging to know the next session key. The session key is calculated $SK = yX = xyP$, where the secret values $Y = yP, Y^* = yP_{pub}$ are generated randomly by the Ui, Sj, and Sn. These values are different when the protocol is executed. Every

session is independent; thus, even though the session's current key is known, the previous and future key cannot be obtained.

- Mutual authentication: In the proposed scheme, the user Ui, server Sj, and sensor node Sn authenticate each other. The server authenticates the user if the values ϕ and $h(id_u \parallel TID_i \parallel X \parallel SID_j \parallel NID_j \parallel Y \parallel R_j)$ calculated are valid. In addition, the RC authenticates the server if the value β and $h(CID_i \parallel X \parallel \alpha \parallel SID_j \parallel R_j \parallel Y \parallel Y^*)$ calculated by the RC are equal to the message received from the server. The sensor node then validates the message received from the RC ϕ and $h(id_u \parallel X \parallel X^* \parallel SID_j \parallel Y \parallel R_i)$; if the calculated value is equal, then the Sn authenticates the RC.
- Session key agreement: In the proposed scheme, the adversary cannot obtain the key session's information to compute the key for the next session even if the adversary knows the current key because the key session is calculated as $SK = yX = xyP$, where the secret values $Y = yP, Y^* = yP_pub$ are generated randomly by the Ui, Sj, and Sn. The values are different when the protocol is executed. The key session is developed independently in every session. Therefore, the key session agreement is achieved in the proposed scheme.
- Stolen verifier attack: RC calculates the Ui secret key and sends it to Ui during the proposed scheme's user registration phase. RC does not maintain an Ui password or secret key verifier table. Then, even though the opponent may access the Ui database, the adversary cannot obtain authentication information. The proposed scheme should therefore avoid a stolen attack by the verifier.
- Man-in-the-middle attack: We are aware of the discussion that the scheme proposed could provide mutual authentication between Ui, Sj, Sn, and RC. The proposed scheme should therefore avoid an attack also on the man in the middle.
- Impersonation attack: The adversary cannot send a legal message $CIDi, X, \alpha$, even though they obtains two authentication factors. The suggested scheme, therefore, resists a user-impersonation attack.
- Server spoofing attack: To impersonate Ui, Sj, Sn, and RC, the adversary has to generate the valid message $\beta = h(CID_i \parallel X \parallel \alpha \parallel SID_j \parallel R_j \parallel Y \parallel Y^*)$. It is easy to know $h(CID_i \parallel X \parallel \alpha \parallel SID_j \parallel R_j \parallel Y \parallel Y^*)$ to obtain authentication, but he/she cannot finish the task since they do not know Rj and whether $h()$ is a secure hash function. The proposed scheme could therefore resist a server spoofing attack.
- Offline password guessing attack: If the adversary steals the user's smart card and extracts information $h(.), Zi$ using a side-channel attack, the adversary might be able to guess the password pw_u. The accuracy of the value, however, is secured by a secure hash function and is not plaintext. In addition, by comparing the RC with the one in the database, it checks the password and identification. The proposed scheme is, therefore, immune to an offline attack.
- Replay attack: Suppose that an intruder intercepts the message $CIDi, X, \alpha$ and attempts to replay Ui by replaying it with Sj. They could detect the attack by checking the validity of $\lambda = h(SID_j \parallel id_u \parallel X \parallel Y \parallel SK \parallel \varphi)$. Using a similar approach, it might be shown that Ui finds a replay attack by testing the validity of $\varphi = h(id_u \parallel X \parallel X^* \parallel\parallel SID_j \parallel NID_j \parallel Y \parallel R_i)$. The proposed scheme could therefore withstand a replay attack.
- Modification attack: In the authentication phase, the authentication message CID_i, X, α i s sent as a hash value and contains a unique random number. Therefore, the server then calculates $Y = yP, Y^* = yP_{pub}$, $\beta = h(CID_i \parallel X \parallel \alpha \parallel SID_j \parallel R_j \parallel Y \parallel Y^*)$, and $CSID_j = SID_j \oplus h(Y^*)$ to check if there was any modification carried out. If the message is modified, the server will detect it and the rest of the values will not be decrypted. Likewise, when the server Sj sends the message $CID_i, X, \alpha, CSID_j, Y, \beta$ to the RC, it will verify the message by computing β and $h(CID_i \parallel X \parallel \alpha \parallel SID_j \parallel R_j \parallel Y \parallel Y^*)$; if the message is not valid, the RC will end the session. Therefore, the proposed scheme withstands a modification attack.

- Stolen smart card attack: let us assume that the adversary can extract the information $h(.), Zi$ after it is st olen by a side-channel attack. The RC will recalculate the message $id_u, h(pw_u \parallel r_i)$ that received and verified it with the stored one. In this case, the attacker cannot obtain the correctness of the value due to the hash function that hides the username and password in the hash value. Therefore, the proposed scheme achieves resistance against a stolen smart card attack.

Table 3. Security feature comparison.

Feature	He et al. [12]	Wu et al. [14]	Sammoud et al. [35]	Proposed Scheme
Multi-server Support	✓	×	×	✓
Data integrity	×	×	×	✓
Backward and forward secrecy	✓	×	✓	✓
Data Usability	×	×	×	✓
Mutual Authentication	✓	✓	✓	✓
Session key agreement	×	×	✓	✓
Stolen Verifier Attack	✓	✓	×	✓
Man-in-the-middle attack	✓	×	✓	✓
Impersonation Attack	✓	✓	✓	✓
Server Spoofing Attack	✓	✓	×	✓
Offline Password Guessing Attack	×	✓	×	✓
Replay Attack	✓	✓	✓	✓
Modification Attack	✓	×	×	✓
Stolen Smart Card Attack	×	×	×	✓

7. Functionality Analysis

This section compares our protocol's functionality and performance with the latest protocols, namely the schemes of He et al. [12], Wu et al. [14], and Sammoud et al. [35]. A comparison between the scheme is proposed for measuring the total communication costs and computational costs for resource use by the sensor node.

7.1. Computation Cost

We define some notations as follows to test the performance of various protocols: T_h, the hash function execution time (Th); T_m, the multiplication execution time (T_m); and T_{he}, the fuzzy extractor execution time (T_{he}). An exclusive operation's cost may be overlooked bitwise compared to the multiplication operation costs in the elliptic curve scale and the hash function. Therefore, the calculation costs of an elliptical multiplication curve operation and a hash function in calculation costs must only be considered. The proposed scheme's simulation was carried out on Intel Core™i7-5700HQ, CPU 2.70 GHzplatform using Java Pairing-Based Cryptography Library (JPBC) library. Table 4 compares the cost of authentication proposed with the new multi-server authentication schemes [12]. In Wu et al. [14], the user needs to apply $4T_h$ on the user side and $10T_h + 3T_E$ on the server side, and the computation cost in the registration centre is $7T_h + 2T_E$. On the sensor node side, the sensor applies $6T_h + 2T_E$; therefore, the total communication cost is 0.0622 ms. Likewise, Sammoud et al. [35] needs to apply $6T_h + 2T_E + 1T_fe$ on the user side. On the central authority, there is a need to apply $11T_h + 3T_E$ of the hash operation and encryption operations. on the sensor node, the sensor needs to apply $6T_h + 1T_E$. In the registration phase of the scheme of He et al. [12], $16T_h$ of the hash function and $5T_m$ of the multiplication operation are used. In the login and authentication phase, there is a need to apply the $19T_h$ hash function and the $6T_m$ multiplication operation. The proposed scheme needs a $6T_h$ hash function operation in the server, sensor node, and user side separately in the registration phase. While the computation cost in the login and authentication phase is $21T_h$ of the hash function in all entities except the server including two-time scalar multiplications of the ECC, our proposed scheme has fewer computation costs than the scheme of He et al. The

wireless medical sensor network is a resource-constrained device, and the authentication scheme must have less computation cost, memory, and resource consumption.

7.2. Communication Cost

For comparison, we considered the length of the random number, password, identity, and timestamp being 64 bits each. The message digest of the hash function (SHA-1) takes 160 bits, and the symmetric key en/decryption (AES-256) produces 256 bits. To evaluate the communication cost of the proposed scheme, we found that Wu et al. [14] has three messages exchanged in the entire authentication phase: $m_1 = C_{ig}, CID_i, C_1, m_2 = C_5, C_6, C_7$, and $m_3 = C_5, C_7, C_8, C_9, C_{10}$. Therefore, the total communication cost in Wu et al. [14] is 1632 bits. In Sammoud et al. [35], the scheme exchanges the messages $M_4 = N_i \bigoplus h(K_{sn})$, $M_5 = h(ID_i||N_i||T_3||ID_g)$, and $M_6 = E_{(h(K_{sn}||Ni))(ID_g||ID_i||M_i||M_5||T_3)}$ in the login and authentication phase. Therefore, the total communication cost of Sammoud et al. is 1056 bits. In He et al. [12], the server sends the message the identity SID_j and receives the message (k_j, s_j) while, in the user registration phase, the user sends the message pair $(ID_i, H(pw_i||\alpha_i))$ and receives the message (z_i, s_i). The user also receives the parameters z_i and s_i, which adds an extra cost to the scheme. Therefore, the total communication cost in He et al. [12] is 980 bits. In our scheme, the user sends the message CID_i, X, α and receives the message SID_j, λ from the server while the server sends the message $CID_i, X, \alpha, CSID_j, Y, \beta$ to RC and recieves $TSID_j, Y, \varphi, \eta$ from the sensor node. The registration centre sends $TID_i, \phi, TSID_j, \varphi$ to the sensor node and receives $CID_i, X, \alpha, CSID_j, Y, \beta$ from the server. Therefore, the length of the exchanged messages is 800 bits. Table 4 shows that the proposed scheme achieved less communication and computation costs comparing to the selected works.

Table 4. Functionality comparison.

/	Wu et al. [14]	Sammoud et al. [35]	He et al. [12]	Cross-SN Scheme
E1	$4T_h$	$3T_h$	$3T_h$	$1T_h$
E2	$3T_h + 1T_E$	$1T_h + 2T_E + 1T_fe$	$2T_m$	$1T_h$
E3	$3T_h$	$2T_h$	$1T_m + 3T_h$	$1T_h$
E4	$4T_h + 2T_E$	$5T_h$	$5T_h$	$1T_h$
E5	$2T_h + 2T_E$	$4T_h + 2T_E$	$2T_m + 5T_h$	$2T_h$
E6	$2T_h$	$1T_E$	$8T_h$	$4T_h$
E7	$3T_h + 1T_E$	$1T_h + 2T_E$	$2T_m + 5T_h$	$2T_m + 4T_h$
E8	$2T_h + 1T_E$	$2T_h + 2T_E$	$2T_m + 5T_h$	$9T_h$
E9	$4T_h + 1T_E$	$4T_h + 1T_E$	$2T_m + 9T_h$	$4T_h$
Total Computation Cost	0.0622 ms	0.5857 ms	0.6524 ms	0.0957 ms
Total Communication Cost	1632 bits	1056 bits	980 bits	800 bits

Note: E1, computation cost at the central authority in the server registration phase; E2, computation cost at the sensor node side in the registration phase; E3, computation cost at the central authority in the sensor registration phase; E4 computation cost at the user side in the registration phase; E5, computation cost at the central authority in the user registration phase; E6, computation cost at the user side in the login and authentication phase; E7, computation cost at the server side in the login and authentication phase; E8, computation cost at the central authority side in the login and authentication phase; and E9, computation cost at the sensor node side in the login and authentication phase.

8. Conclusions

This paper proposed a secure multi-server authentication scheme based on smart cards using wireless medical sensors networks (Cross-SN). The scheme is mainly based on elliptical curve cryptography. It shows that the proposed scheme will meet security standards and characteristics. The proposed scheme provides secure online communication between end-users and medical sensors. It withstands specific passive and active attacks such as impersonation attacks, server spoofing attacks, and replay man-in-the-middle attacks. It successfully provides backward/forward secrecy, mutual authentication, data integrity, and a multi-server environment. Moreover, the proposed scheme's mutual authentication is proved using the wide-used formal analysis tool BAN logic tool

to verify secure mutual authentication between the users and the medical sensors. The results show that the proposed scheme achieves better efficiency in communication and computation costs due to lightweight cryptographic operations. Consequently, the scheme is suitable for IoT environments that enhance healthcare applications using a wireless medical sensor network.

Author Contributions: Conceptualization, H.K. and S.J.H.; methodology, H.K. and S.J.H.; software, H.K.; validation, H.K.; results interception, H.K. and S.J.H.; formal analysis, H.K.; writing—original draft preparation, H.K.; writing—review and editing, H.K. and S.J.H.; supervision, S.J.H., S.M.S.A., F.H., and M.A.C.; and project administration, S.J.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: We would like to thank the reviewers for their careful, constructive, and insightful comments in relation to this work.

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

References

1. Landaluce, H.; Arjona, L.; Perallos, A.; Falcone, F.; Angulo, I.; Muralter, F. A Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks. *Sensors* **2020**, *20*, 2495. [CrossRef]
2. Ugrenovic, D.; Gardasevic, G. CoAP protocol for Web-based monitoring in IoT healthcare applications. In Proceedings of the 2015 23rd Telecommunications Forum Telfor (TELFOR), Belgrade, Serbia, 24–26 November 2015; pp. 79–82.
3. Khalid, H.; Lun, K.Y.; Othman, M.; Ahmad, I. Authentication Groups With Privacy-Protection of Machine-to-Machine in LTE-LTE-A networks. *J. Theor. Appl. Inf. Technol.* **2017**, *95*, 2896–2905.
4. Yu, S.; Park, Y. SLUA-WSN: Secure and Lightweight Three-Factor-Based User Authentication Protocol for Wireless Sensor Networks. *Sensors* **2020**, *20*, 4143. [CrossRef] [PubMed]
5. Alezabi, K.A.; Hashim, F.; Hashim, S.J.; Ali, B.M. A new tunnelled EAP based authentication method for WiMAX networks. In Proceedings of the 2013 IEEE 11th Malaysia International Conference on Communications (MICC), Kuala Lumpur, Malaysia, 28–30 November 2013; pp. 412–417.
6. Wu, T.; Redouté, J.M.; Yuce, M.R. A wearable wireless medical sensor network system towards internet-of-patients. In Proceedings of the 2018 IEEE SENSORS, New Delhi, India, 28–30 October 2018; pp. 1–3.
7. Azmi, N.; Kamarudin, L.M. *Enabling IoT: Integration of Wireless Sensor Network for Healthcare Application Using WASPMOTE*; AIP Publishing LLC: New York, NY, USA, 2017; Volume 1808, p. 020010.
8. Gardašević, G.; Katzis, K.; Bajić, D.; Berbakov, L. Emerging Wireless Sensor Networks and Internet of Things Technologies—Foundations of Smart Healthcare. *Sensors* **2020**, *20*, 3619. [CrossRef]
9. Kumar, P.; Lee, H.J. Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors* **2012**, *12*, 55–91. [CrossRef]
10. Khalid, H.; Hashim, S.J.; Ahmad, S.M.; Hashim, F.; Chaudary, M.A. Cybersecurity in Industry 4.0 context: Background, issues, and future directions. *Nine Pillars Technol. Ind.* **2020**, 263–307. [CrossRef]
11. Ko, J.; Lu, C.; Srivastava, M.B.; Stankovic, J.A.; Terzis, A.; Welsh, M. Wireless sensor networks for healthcare. *Proc. IEEE* **2010**, *98*, 1947–1960. [CrossRef]
12. He, D.; Wang, D. Robust biometrics-based authentication scheme for multiserver environment. *IEEE Syst. J.* **2014**, *9*, 816–823. [CrossRef]
13. Mir, O.; Munilla, J.; Kumari, S. Efficient anonymous authentication with key agreement protocol for wireless medical sensor networks. *Peer Peer Netw. Appl.* **2017**, *10*, 79–91. [CrossRef]
14. Wu, F.; Xu, L.; Kumari, S.; Li, X. An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. *Multimed. Syst.* **2017**, *23*, 195–205. [CrossRef]
15. Ever, Y.K. Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks. *IEEE Syst. J.* **2018**, *13*, 456–467. [CrossRef]
16. Zmezm, H.F.; Hashim, S.; Sali, A.; Alezabi, K.A. Pre-authentication design for seamless and secure handover in mobile WiMAX. *Int. Rev. Comput. Softw. (IRECOS)* **2015**, *10*, 764–772. [CrossRef]
17. Khalid, H.; Hashim, S.J.; Syed Ahmad, S.M.; Hashim, F.; Akmal Chaudhary, M. Security and Safety of Industrial Cyber-Physical System : Systematic Literature Review. *Palarch'S J. Archaeol. Egypt/Egyptol.* **2020**, *17*, 1592–1620.
18. Kumar, P.; Lee, S.G.; Lee, H.J. E-SAP: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. *Sensors* **2012**, *12*, 1625–1647. [CrossRef] [PubMed]
19. Wu, F.; Li, X.; Sangaiah, A.K.; Xu, L.; Kumari, S.; Wu, L.; Shen, J. A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. *Future Gener. Comput. Syst.* **2018**, *82*, 727–737. [CrossRef]

20. Ali, R.; Pal, A.K.; Kumari, S.; Sangaiah, A.K.; Li, X.; Wu, F. An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring. *J. Ambient. Intell. Humaniz. Comput.* **2018**, 1–22. [CrossRef]
21. Shuai, M.; Liu, B.; Yu, N.; Xiong, L. Lightweight and secure three-factor authentication scheme for remote patient monitoring using on-body wireless networks. *Secur. Commun. Netw.* **2019**, *2019*. [CrossRef]
22. Li, X.; Peng, J.; Obaidat, M.S.; Wu, F.; Khan, M.K.; Chen, C. A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. *IEEE Syst. J.* **2019**, *14*, 39–50. [CrossRef]
23. Mo, J.; Hu, Z.; Lin, Y. Cryptanalysis and Security Improvement of Two Authentication Schemes for Healthcare Systems Using Wireless Medical Sensor Networks. *Secur. Commun. Netw.* **2020**, *2020*. [CrossRef]
24. Sun, W.; Cai, Z.; Li, Y.; Liu, F.; Fang, S.; Wang, G. Security and privacy in the medical internet of things: A review. *Secur. Commun. Netw.* **2018**, *2018*. [CrossRef]
25. Pal, S.; Hitchens, M.; Rabehaja, T.; Mukhopadhyay, S. Security requirements for the internet of things: A systematic approach. *Sensors* **2020**, *20*, 5897. [CrossRef] [PubMed]
26. Somasundaram, R.; Thirugnanam, M. Review of security challenges in healthcare internet of things. *Wirel. Netw.* **2020**, 1–7. [CrossRef]
27. Sun, Y.; Lo, F.P.W.; Lo, B. Security and privacy for the internet of medical things enabled healthcare systems: A survey. *IEEE Access* **2019**, *7*, 183339–183355. [CrossRef]
28. Zhang, Y.; Luo, M.; Choo, K.K.R.; He, D. A General Architecture for Multiserver Authentication Key Agreement with Provable Security. *Secur. Commun. Netw.* **2018**, *2018*. [CrossRef]
29. Cichonski, J.; Marron, J.; Hastings, N.; Ajmo, J.; Rufus, R. [Project Description] Security for IoT Sensor Networks: Building Management Case Study (Draft). Available Online: https://csrc.nist.gov/publications/detail/white-paper/2019/02/01/security-for-iot-sensor-networks/draft (accessed on 2 February 2019).
30. Dubrawsky, I. *Eleventh Hour Security+: Exam SY0-201 Study Guide*; Syngress: Boston, MA, USA, 2009.
31. Hankerson, D.; Menezes, A.J.; Vanstone, S. *Guide to Elliptic Curve Cryptography*; Springer Science & Business Media: New York, NY, USA, 2006.
32. Rubin, A.D.; Honeyman, P. *Formal Methods for the Analysis of Authentication Protocols*; Technical Report; Center for Information Technology Integration: Ann Arbor, MI, USA, 8 November 1993.
33. Chen, C.L.; Chen, Y.X.; Lee, C.F.; Deng, Y.Y.; Chen, C.H. An efficient and secure key agreement protocol for sharing emergency events in VANET systems. *IEEE Access* **2019**, *7*, 148472–148484. [CrossRef]
34. Chen, C.L.; Lin, D.P.; Chen, H.C.; Deng, Y.Y.; Lee, C.F. Design of a Logistics System with Privacy and Lightweight Verification. *Energies* **2019**, *12*, 3061. [CrossRef]
35. Sammoud, A.; Chalouf, M.A.; Hamdi, O.; Montavont, N.; Bouallegue, A. A secure and lightweight three-factor authentication and key generation scheme for direct communication between healthcare professionals and patient's WMSN. In Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 7–10 July 2020; pp. 1–6.