IoT-based Secure Wireless Medical Sensor Networks using Multifactor Authentication

Manish Bali
Department of Computer Science and Engineering
Presidency University
Bengaluru, India
balimanish0@gmail.com

Anuradha Yenkikar
Department of CSE (AI)
Vishwakarma Institute of Information Technology
Pune, India
anu.jamkhande@gmail.com

ABSTRACT

Wireless Medical Sensor Networks (WMSN) integrated with the Internet of Things (IoT) have the potential to revolutionize the healthcare industry by enabling remote patient monitoring and personalized healthcare services. Due to wireless communication, securing communication becomes a vital issue. Since the vital signs parameters are sensitive to the patients' health status and this information must not be revealed to others except the healthcare professionals, protection of patients' privacy becomes a key issue for WMSN applications. User authentication with anonymity property is the most basic and commonly used method to resolve the security and privacy issues in WMSNs. This chapter proposes a multifactor authentication schema that uses smart card, password and biometrics of a health professional (user) to address these issues to improve the effectiveness, security, and scalability of IoT-based WMSNs for enhanced patient care. We observe that the proposed schema can tolerate most of the common attacks and offers additional functionality features compared to other contemporary solutions.

Keywords—authentication; internet of things; smart card; biometrics; wireless medical sensor networks

I. INTRODUCTION

With the improvement of living standards and the rapid development of public health, the life expectancy of humans has increased rapidly over the past decades. For example, the average life expectancy of Indians was 39.93 years in 1960, but in the last 50 years it has risen to 70.7 years for females and 68.2 years for males in 2020 as shown in Figure 1. With increasing age, lots of elderly people may suffer from various types of chronic diseases and unable to take care of themselves, and these will lead to a heavy burden to the next generations and the healthcare system. To handle this challenge, remote monitoring has emerged as an effective solution for the healthcare system [1] [2]. Wireless Body area networks (WBANs), as an important part of remote monitoring system, have received a great deal of attention from researchers in the academic and industrial field because of its potential to improve the quality of healthcare services.

The Internet of Things (IoT) has emerged as a transformative technology with the potential to revolutionize various industries, and healthcare is no exception. One of the most promising applications of IoT in the healthcare sector is its integration with Wireless Medical Sensor Networks (WMSNs) for remote patient monitoring. This integration offers tremendous opportunities to improve patient care, enhance medical diagnostics, and transform healthcare delivery.

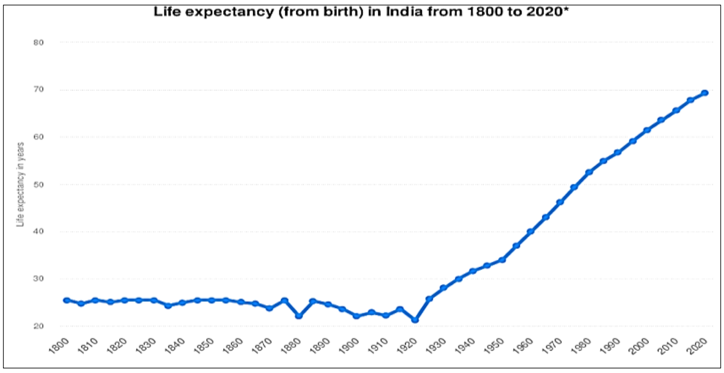

Figure 1: Life expectancy in India over the years

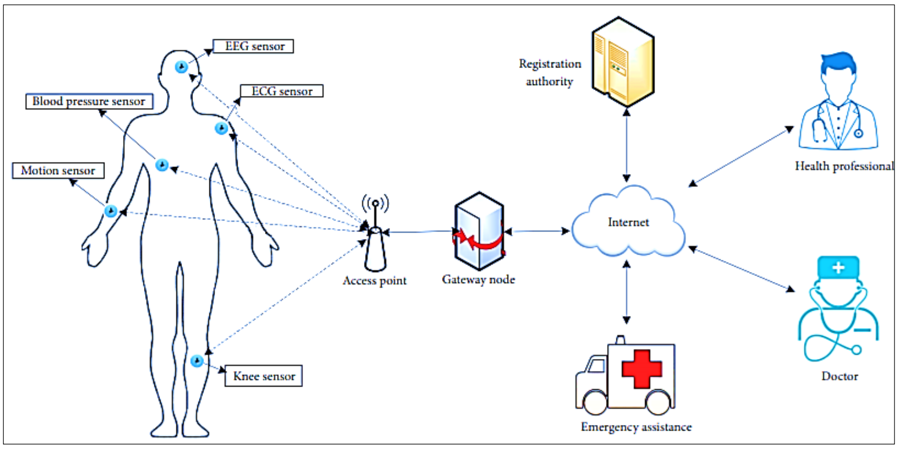

Figure 2: Network model for remote patient monitoring

Remote patient monitoring, facilitated by IoT-enabled WMSNs, involves the continuous and non-invasive collection of patient data from various medical sensors placed on or within the patient's body. A typical architecture for remote patient monitoring using WMSNs is illustrated in Figure 2, which is adapted from [3] [4] [5].

These sensors can monitor vital signs such as heart rate, blood pressure, body temperature, oxygen saturation, and glucose levels, among others. The collected data is then transmitted wirelessly through IoT communication protocols to a centralized platform or a cloud-based server for real-time analysis and storage. A malicious adversary can intercept, modify, insert, and delete the transmitted messages over insecure public communication channel easily [6]. In addition, it is extremely dangerous if the unauthorized users send instructions to stop the function of wearable devices, especially the wearable devices that are critical to the life of a patient, like heart bumps. By securely enabling healthcare professionals to remotely monitor patients' health status, IoT-based WMSNs offer a plethora of benefits like:

- Continuous Monitoring: Unlike traditional in-person visits, remote patient monitoring allows continuous data collection, providing a comprehensive and dynamic view of a patient's health status. This enables early detection of anomalies or changes in vital signs, enabling timely interventions.
- Improved Patient Outcomes: IoT-based WMSNs facilitate early detection of health issues, enabling timely medical interventions. This proactive approach can lead to better patient outcomes and reduced hospital readmissions.
- Enhanced Efficiency and Cost Savings: Remote patient monitoring can optimize healthcare resource utilization by reducing unnecessary hospital visits and streamlining patient care. This can result in significant cost savings for healthcare providers and patients alike.
- Personalized Healthcare: The continuous data stream from IoT-enabled sensors enables healthcare professionals to tailor treatment plans and medical interventions according to each patient's unique health needs.
- Remote Accessibility: Patients in rural or remote areas, or those with limited mobility, can receive quality healthcare without the need for frequent visits to healthcare facilities.
- Real-time Data Analytics: IoT-based WMSNs generate vast amounts of patient data. Leveraging data analytics and machine learning techniques, healthcare providers can derive valuable insights from this data, leading to evidence-based decision-making.
- Early Disease Detection: IoT-enabled WMSNs can help detect early signs of deteriorating health, enabling timely preventive measures and reducing the severity of certain health conditions.

In the past years, many authentication schemes have been proposed to provide secure and effective healthcare monitoring of the patients using WBANs. Since the wearable sensor nodes have weak energy and computation ability, authentication schemes based on public key encryption, such as elliptic curve cryptography (ECC) [7] and Rabin cryptosystem [8] [9], have heavy computation burdens, and they are not suitable for realistic scenarios. Therefore, the method of using the lightweight operations, liking symmetric encryption/decryption and hash functions, is an effective way to deal with the weaknesses of public key encryption. However, after careful analysis, we find that most of these existing schemes using lightweight cryptographic primitives are susceptible to security threats and not suitable for practical use. Specifically, all these schemes fail to provide forward secrecy and suffer from many known attacks.

The key contribution of this chapter is a novel secure and efficient user authentication schema for healthcare applications in wireless medical sensor networks. Following is a summary of the remaining parts of this chapter. The related research in this field is discussed in Section II. Section III discusses the methodology and the proposed schema, while Section IV presents and discusses the results. Conclusion comes next in Section V, followed by the references at the end.

II. RELATED WORKS

There have been a lot of research in this domain providing valuable insights into the current state of research and developments. They cover various aspects such as architecture, data analytics, security, clinical applications, and interoperability, providing a holistic understanding of this evolving field in modern healthcare. This section will discuss some of the recent literature in this domain. [10] provide a comprehensive review of the latest developments in IoT-enabled Wireless Medical Sensor Networks for remote patient monitoring. It discusses various IoT-based architectures, communication protocols, and data analytics techniques employed in these networks. The authors analyze the potential benefits and challenges of implementing IoT in healthcare and highlight the impact of remote patient monitoring on improving patient outcomes. [11] provide a systematic review that examines the current state of IoT-enabled wearable medical devices used in remote patient monitoring. The authors assess the accuracy and reliability of these devices in measuring vital signs and analyze the usability and user acceptance. The paper also discusses the security and privacy concerns associated with wearable IoT devices and proposes potential solutions. [12] present a case study focusing on the application of IoT-based Wireless Medical Sensor Networks in cardiac monitoring. The authors discuss the design and implementation of the network, the selection of suitable sensors, and the integration with existing healthcare infrastructure. The study showcases the effectiveness of remote patient monitoring in detecting cardiac anomalies and improving patient outcomes.

To explore the various data analytics techniques employed in IoT-enabled Wireless Medical Sensor Networks for real-time health monitoring, [13] discuss various machine learning algorithms, data fusion methods, and anomaly detection approaches used to analyze patient data and provide timely medical interventions. The paper also discusses the challenges and opportunities in data analytics for remote patient monitoring. [14] focus on the security and privacy aspects of IoT-based healthcare systems, including Wireless Medical Sensor Networks for remote patient monitoring. The authors review the potential vulnerabilities and attacks on IoT devices and propose security measures to protect patient data and ensure confidentiality, integrity, and availability. [15] analyze the clinical trials and studies that have evaluated the effectiveness of IoT-based remote patient monitoring in chronic disease management. The authors discuss the impact of IoT-enabled WMSNs in managing conditions such as diabetes, hypertension, and respiratory diseases. The paper highlights the potential benefits of continuous monitoring in improving patient adherence to treatment plans and reducing hospital visits. [16] addresses the interoperability challenges in IoT-based healthcare systems, including Wireless Medical Sensor Networks. The authors review the existing standards and protocols for data exchange among heterogeneous medical devices and propose solutions to achieve seamless interoperability. The paper emphasizes the importance of interoperability in facilitating data sharing and medical decision-making in remote patient monitoring scenarios.

III. METHODOLOGY

IoT-enabled Wireless Medical Sensor Networks (WMSNs) are designed to collect, transmit, and analyze patient data in real-time for remote patient monitoring and healthcare applications. The architecture involves a combination of hardware components, network protocols, and data management systems to ensure seamless and secure communication between medical sensors and healthcare infrastructure. A typical architecture of WMSN in a hospital environment is shown in Figure 2. In this chapter, we adapt this network model in the proposed schema. The medical sensors (e.g., ECG electrodes, pulse oxi-meter, blood pressure, and temperature sensors) are deployed on a patient's body, which forms a wireless body area network (WBAN). The sensors then collect the individual's physiological data and sends the collected data via a wireless channel to the health professionals' hand-held devices (i.e., personal digital assistant (PDA), iPhone, laptop, etc.) [17]. Thus, a physician can use these medical sensor readings to gain a broader assessment of patient's health status as and when he/she demands for that. A patient's physiological data may include heartbeat rates, temperature, blood pressure, blood oxygen level, etc. The next sections detail the threat model and the notations used in this research.

A. Threat model

An adversary can retrieve all the sensitive information stored in a lost/stolen smart-card's memory using the power analysis attacks. We use the Dolev-Yao threat model [18], in which any two communicating parties can communicate over an insecure public channel. A similar threat model in our scheme is adopted, where the communicating channels are insecure, and the endpoints (sensor nodes) cannot in general be trustworthy. The base station (the gateway node *GWN*) is trusted, and it will never be compromised by an adversary (attacker); otherwise, the whole network will be compromised. Sensor nodes deployed on the patients' body are not equipped with tamper-resistant hardware due to cost constraints. As a result, if an adversary physically captures a sensor from a patient body, the adversary will know all the sensitive information stored in that sensor's memory.

The Dolev-Yao model was chosen as its Intruder is the Most Powerful Attacker. It models the attacker as an active saboteur. He is omnipotent and can therefore intercept, eavesdrop, or modify all communication of the network. Furthermore, the attacker can pose as a legitimate communication partner and can therefore initiate a communication with every participant in the network. Compromising or breaking cryptographic primitives is not possible for a Dolev-Yao attacker.

B. **Notations**

Notations used in this chapter are described below in Table 1.

Table 1: Notations used

Notation	Description
U_i	Remote health professional
GWN	Gateway node
SN_j	Medical sensor node
ID_i	Unique identity of U_i
PW_i	Password of U_i
BIO_i	Biometric information of U_i
HID_i	Pseudonym identity of U_i
SID_j	Unique identity of SN_j
Ek [.]/Dk [.]	Symmetric encryption/decryption with key *k*
R, R_A	Random number
T_1 , T_2 , T_3 , T_4	Current time stamp
ΔT	The maximum of the transmission delay time
K	Secret key generated by *GWN*
SK	Session key
h(.)	One-way hash function
BH(.)	Biohash function
$X\|\|Y$	Concatenate operation
$\oplus$	*XOR* operation

C. **Proposed schema**

The schema consists of five phases: (i) professional registration phase, (ii) patient registration phase, (iii) pre-deployment phase, (iv) login phase, and (v) authentication and session key agreement phase. The following assumptions are applied while designing the schema:

- The registration authority is a trusted entity in the network
- Three 256-bits secret keys *A*, *B* and *C* are maintained by the gateway (*GW*) node.
- All entities in the WMSN are synchronized with their clocks
- We use the fuzzy extractor technique [19] to withstand the privileged-insider attack and flaw in password change phase found in some of the other schemes proposed. Fuzzy extractor can extract the uniformly distributed random key R_i from biometric input BIO_i in an error-tolerant way. If another biometric input BIO_i* remains reasonably like BIO_i, the extracted random key R_i remains unchanged with the help of an auxiliary string P_i. An fuzzy extractor contains two procedures (*Gen*, *Rep*).
- $Gen(BIO_i) = (R_i, P_i)$. Gen is a probabilistic generation procedure allowing to extract random key R_i and an auxiliary string P_i from biometric input BIO_i
- $R_i{*}= Rep(BIO_i{*}, P_i)$. Rep is a deterministic reproduction procedure allowing to reproduce random key *Ri* from any biometric input BIO_i* close to BIO_i with the help of auxiliary string P_i .

(i) Professional Registration Phase

In this phase, if a health professional U_i wants to become a legal user of WMSN, he/she needs to register in the *GW* by performing the following steps:

Step 1. U_i first chooses an identity ID_i and password PW_i. U_i then imprints his/her personal biometrics BIO_i on a specific device.

Step 2. *Ui* picks a 1024-bit random number k_i, and computes $(\sigma_I, \tau_i) = Gen(BIO_i)$ and $RPW_i = h(ID_i||k_i||PW_i)$. U_i sends the registration request message $\{ID_i, RPW_i\}$ to the *GW* via a secure channel. Note that σ_i is the biometric key data and τ_I is the reproduction public parameter.

Step 3. After receiving the registration request from *Ui*, the *GW* picks a random number r_g, identity *IDg*, and then calculates $C_{ij} = E_J\left[r_g||ID_i||ID_g\right]$ using its secret key *J*, $N_i = h\left(ID_i\,||ID_g||\,K\right) \oplus RPW_i,$ where *K* is the secret key of the *GW*. The *GW* then sends a smart card *SCi* to the user *Ui* via a secure channel, where *SCi* contains the parameters $\{C_{ij}, N_i, h(.), Gen(.), Rep(.), t\}$

Step 4. After receiving the smart card SC_i from the *GW*, U_i further computes $e_i = h(ID_i) \oplus k_i, V_i = h(ID_i||RPW_i||\sigma_i)$ and $N_i^* = N_i \oplus h(k_i||\sigma_i) = h(ID_i\,||ID_g||\,K) \oplus RPW_i \oplus h(k_i||\sigma_i)$. Ui then stores τ_I, ei and V_i in his/her smart card SC_i and replaces N_i with N_i^*. Finally, the updated SC_i contains the information $\{C_{ij}, N_i^*, h(.), Gen(.), Rep(.), t, \tau_i, ei, Vi\}$.

(ii) Patient Registration Phase

In this phase, to enjoy the healthcare applications a patient needs to register in the hospital registration centre (RC) by executing the following three steps:

Step 1. The patient first sends his/her name to the *RC*.

Step 2. The *RC* selects a suitable sensor kit and then designates professionals.

Step 3. The *RC* finally submits the patient's identity *IDpt* and information of medical sensors to the designated professionals.

(iii) Pre-Deployment Phase

In this phase, the sensitive information is pre-loaded into each sensor node SN_n*'s* memory prior to its deployment in a patient's body in WMSN. This phase is executed in offline mode by the *GW* node as follows:

Step 1. For each deployed sensor node SN_n, the *GW* chooses a unique identity $IDSN_n$ and a unique randomly generated master key *MSSNn.*

Step 2. The *GW* computes the pre-shared secret key between SN_n and the *GW* as $SK_{GW,SN_n} = h(ID_g||ID_{SN_n}||Q||MK_{SN_n})$ using the identity ID_g of the *GW*, the identity ID_{SNn} of SN_n, the secret key *Q* of the *GW* and the master key $MKSN_n$ of SN_n. Note that each secret key SK_{GW}, SN_n between every SN_n and the *GW* is distinct.

Step 3. Finally, the *GW* pre-loads the following information into each sensor SN_n*'s* memory prior to its deployment: (i) $IDSN_n$ and (ii) SK_{GW}, SN_n.

(iv) Login Phase

After the sensor nodes are deployed in patient's body in WMSN, a health professional U_i needs to login to WMSN via the *GW* to access the physiological information of patients from WMSN. In this phase, the following steps are executed by U_i*:*

Step 1. U_i first inserts his/her smart card SC_i, and then inputs ID_i and PW_i. U_i also imprints the personal biometrics BIO_i' on a specific device.

Step 2. The smart card SC_i of *Ui* then computes $\sigma_i^* = Rep(BIO_i', \tau_i), k_i^* = e_i \oplus h(ID_i||\sigma_i^*), RPW_i^* = h(ID_i||k_i^*||PW_i),$ and $V_i^* = h(ID_i||RPW_i^*||\sigma_i^*)$. SC_i then checks the condition $V_i^* = V_i$. If it does not hold, it means that one of the identity, password or the biometric is not valid, and SC_i terminates the session.

Step 3. SC_i further computes $N_i^* = N_i \oplus RPW_i^* \oplus h(k_i^*||\sigma_i^*)$ and generates a random number r_i. SC_i also computes $CID_i = E_{N_i'}[h(ID_i\,||C_{ig}||\,ID_{SN_n}||r_i||TS_1)||IDD_{SN_n}||r_i]$, where TS_1 is the current timestamp and $IDSN_n$ is the identity of the accessed sensor node SN_n in a patient's body. Finally, SC_i sends the login request message $m_1 = \{C_{ig}, CID_i, TS_1\}$ to the *GW* via a public channel.

(v) Authentication and Session Key Agreement Phase

In this phase, a health professional *Ui* and an accessed sensor node SN_n establish a session key for their future secure communication after their mutual authentication via the *GW* in WMSN. This phase has the following steps:

Step 1. After receiving the login request message *m1* = $\{C_{ig}, CID_i, TS_1\}$ from *Ui* at time TS_1^*, the GW node verifies the validity of the timestamp *TS1* present in the message by the inequality $TS_1^* - TS_1 \leq \Delta T$. If it is not valid, the *GW* terminates the session.

Step 2. The *GW* computes $(r_g' || ID_i' || ID_g') = D_j[C_{ig}], N_i'' = h\left(ID_i' \left|\right| ID_g' \left|\right| K\right)$ and $\left(h_1 \left|\right| ID_{SN_n}' \left|\right| r_i'\right) = D_{N_i''}[CID_i]$. The *GW* then checks if $h_1 = h\left(ID_i' \left|\right| C_{ig} \left|\right| ID_{SN_n}' || r_i' || TS_1\right)$? If it does not hold, the *GW* terminates the session.

Step 3. The *GW* continues to generate a temporary pseudo-random identity *NIDi* for the actual identity ID_i' of the user *Ui*. The GW stores $(ID_i', ID_{SN_n}', NID_i)$ in its database corresponding to the accessed sensor *SNn* for the user *Ui*. Note that *NID*$_i$ is used achieve the user anonymity property in our scheme. The *GW* then computes

$A_i = r_i' \oplus h(SK_{GW,SN_n} || NID_i || ID_{SN_n}' || TS_2)$; B_i=$E_{SK_{GW,SN_n}}[h\left(NID_i \left|\right| ID_{SN_n'} \left|\right| r_i' || TS_2\right) || NID_i || ID_{SN_n}' || A_i \left|\right| TS_2\right]$ where *TS*$_2$ is the current timestamp and sends the message $m_2 = \{B_i, TS_2\}$ to the sensor node *SN*$_n$ via a public channel.

Step 4. After receiving the message $m_2 = \{B_i, TS_2\}$ at time S_2^*, *SN*$_n$ checks the validity of the timestamp *TS*$_2$ by the inequality $TS_2^* - TS_2 \leq \Delta T$. If it is not valid, *SN*$_n$ terminates the session. Otherwise, *SN*$_n$ calculates $\left(h_2 \left|\right| NID_i'' \left|\right| ID_{SN_n}'' || A_i' || TS_2'\right) = D_{SK_{GW,SN_n}}[B_i]$ and checks the conditions $ID_{SN_n}' = ID_{SN_n}, TS_2' = TS_2$. If these are valid, SNn continues to calculate $r_i'' = A_i' \oplus h\left(SK_{GW,SN_n} \left|\right| NID_i'' \left|\right| ID_{SN_n} || TS_2\right)$ and checks the condition $h_2 = h(NID_i'' || ID_{SN_n} \left|\right| r_i'' \left|\right| TS_2)$. If it does not hold, the session is terminated. Otherwise, the *GW* is credible.

Step 5. *SN*$_n$ further generates a random number rn and computes $F_i = r_n \oplus h\left(SK_{GW,SN_n} \left|\right| NID_i'' \left|\right| ID_{SN_n} || TS_3\right)$, $G_i = E_{SK_{GW,SN_n}}[h\left(NID_i'' \left|\right| ID_{SN_n} \left|\right| r_n || TS_3\right) \left|\right| h\left(SK_{U_i,SN_n}\right) || NID_i'' \left|\right| ID_{SN_n} \left|\right| F_i \left|\right| TS_3]$ and $SK_{U_i,SN_n} = h(NID_i'' | \left| ID_{SN_n} \right|| r_i'' \left|\right| r_n)$, where TS3 is the current timestamp. *SN*$_n$ then sends the message $m_3 = \{G_i, TS_3\}$ to the GW via a public channel.

Step 6. After receiving the message *m*$_3$ from *SN*$_n$ in Step 5 at time TS_3^*, the GW checks the validity of the timestamp *TS*$_3$ by the inequality $TS_3^* - TS_2 \leq \Delta T$. If it is not valid, the *GW* terminates the session. Otherwise, the *GW* computes $(h_3 || h_4 || NID_i''' || ID_{SN_n}''' || F_i' || TS_3') = D_{SK_{GW,SN_n}}[G_i]$, and checks the conditions $NID_i''' = NID_i, ID_{SN_n}''' = ID_{SN_n}'$ and $TS_3' = TS_3$. If any one of these conditions is not satisfied, the *GW* terminates the session.

Step 7. The GW computes $r_n' = F_i' \oplus h(SK_{GW,SN_n} || NID_i || ID_{SN_n}' || TS_3)$ and checks the condition $h_3 = h(NID_i || ID_{SN_n}' || r_n' || TS_3)$. If it is valid, the GW generates a new random number r_g^{new} , and computes $C_{ig}^{new} = E_j[\, r_g^{new} || ID_i' || ID_g'], r_t = r_n' \oplus r_i'$ and $M_i = E_{N_i''}[h\left(ID_i || NID_i || C_{ig}^{new} \left|\right| ID_{SN_n}' \left|\right| r_t || h_4 || TS_4\right]$, where TS4 is the current timestamp. The GW then sends the message $m_4 = \{M_i, TS_4\}$ to *U*$_i$ via a public channel.

Step 8. After receiving the message $m_4 = \{M_i, TS_4\}$ at time *TS*$_4$, *U*$_i$ validates the timestamp *TS*$_4$ by the inequality $S_4^* - TS_4 \leq \Delta T$. If it is not valid, *U*$_i$ terminates the session. Otherwise, *U*$_i$ calculates $(h_5 || NID_i^* || C_{ig}^{new^*} || ID_{SN_n}^* || r_t^* || h_4^* || TS_4^*) = D_{N_i'}[M_i]$. After that *U*$_i$ checks the conditions $ID_{SN_n}^* = ID_{SN_n}', TS_4^* = TS_4$. If these are valid, *U*$_i$ computes $r_n'' = r_i^* \oplus r_i, SK_{U_{i,SN_n}}^* = h(NID_i^* || ID_{SN_n} || r_i || r_n'')$.

Step 9. *U*$_i$ then checks the conditions $h_4^* = h\left(SK_{U_{i,SN_n}}^*\right)$ and $h_5 = h\left(ID_i || NID_i^* || C_{ig}^{new^*} \left|\right| ID_{SN_n} \left|\right| h_4^* \left|\right| r_n'' \left|\right| TS_4\right)$. If these conditions are met, *SN*$_n$ is authenticated by *U*$_i$ and stores the session key $SK_{U_{i,SN_n}}^* \left(= SK_{U_{i,SN_n}}\right)$shared with *SN*$_n$ for future secure communication. On the other hand, *SN*$_n$ also stores the session key $SK_{U_{i,SN_n}} \left(= SK_{U_{i,SN_n}}^*\right)$ shared with *U*$_i$ for future secure communication.

We carry out an Informal analysis and check the ability of the proposed schema to tolerate some of the common attacks and its functionality features. Also, since the schema involves wireless communication, securing communication becomes a vital issue in WMSNs. We test the hypothesis if the proposed protocol (*PP*) is attack resilient (*AR*) to various well-known attacks i.e. *(AR)*$_{PP}$ is equal to the hypothesized attack resiliency *(AR)*$_{PPH0}$ using multifactor authentication and results in secure wireless medical sensor networks. The null (1) and alternate hypothesis (2) can then be symbolically expressed as:

$H_0 = (AR)_{PP} = (AR)_{PPH0} = Secure\ WMSN$ (1)

$H_a = (AR)_{PP} \neq (AR)_{PPH0}$ (2)

The alternative hypothesis can be read as that the proposed protocol is not secure and doesn't protect from various known attacks applicable in WMSNs.

IV. RESULTS AND DISCUSSION

We compare the performance of the proposed schema with some of the state-of-the-art models and tabulate the results in Table 2.

- **Privileged insider attack:** In this attack, a privileged insider of the *GW* may collect user credentials from the registration centre and try to obtain the services on behalf of a legal user. In order to prevent this attack, in our schema the credentials ID_i, PW_i and Bio_i are sent securely by masking with the one-hash function and the random secret k_i as $\{ID_i, RPW_i\}$, where $RPW_i = h(ID_i' || k_i || PW_i)$. Moreover, we hide the random number k_i using the personal biometric key data σ_I obtained from the biometric BIO_i of the user U_i as $e_i = h(ID_i| \quad |\sigma_i) \oplus k_i$. Even if an adversary has the lost/stolen smart card SC_i of U_i and extracts the information using the power analysis but will be unable to perform the password guessing attack because k_i is unknown. Therefore, RPW_I and ID_I do not help the adversary to obtain PW_i. Similarly, the adversary cannot obtain the biometric key data σ_{I} using the extracted information from the lost/stolen smart card SC_i without knowing BIO_i. Hence, our schema successfully resists the privileged insider attack.

Table 2: Security and functionality feature comparison

Security feature	Yeh et al. [5]	Shi Gong [6]	Kumar et al. [20]	He et al. [21]	Li et al. [22]	Proposed schema
Wrong password detection	☑	☑	☑	☒	☑	☑
Stolen smartcard attack	☒	☒	☒	☑	☑	☑
Mutual authentication	☒	☑	☑	☑	☑	☑
Session key agreement	☒	☑	☑	☑	☑	☑
Resists replay attack	☑	☑	☑	☑	☑	☑
Insider attack resiliency	☑	☑	☒	☒	☒	☑
Denial-of-service attack	☑	☑	☒	☒	☒	☑
User anonymity	☒	☒	☒	☒	☒	☑
Sensor node capture attack	☒	☒	☒	☒	☒	☑
Supports biometric update phase	☒	☒	☒	☒	☒	Extendable
Supports dynamic medical sensor node addition phase	☒	☒	☒	☒	☒	Extendable

- **Stolen smart card attack**: Assume that the smart card SC_i of user U_i is stolen/lost. Then, an adversary can extract all the information $\{C_{ig}, N_i^*, h(.), Gen(.), Rep(.), t, \tau_i, e_i, V_i\}$, where, $C_{ig} = E_J[r_g || ID_i || ID_g], N_i^* = N_i \oplus h(k_i || \sigma_i) = h(ID_i || ID_g || K) \oplus RPW_i \oplus h(k_i || \sigma_i), e_i = h(ID_i || \sigma_i) \oplus k_i \; and \; V_i = h\,[ID_i || RPW_i || \sigma_i]$ using the power analysis. Clearly, from this information, the user identity ID_i and password PW_i are protected using the secret biometric key data σ_i and the secret random number k_i. Since copying or guessing the user biometrics is computationally hard problem deriving the user credentials is computationally infeasible. As a result, our scheme is secure against stolen smart card attack.
- **Stolen verifier attack**: In this attack, an adversary can steal the user information stored in the *GW* and try to perform some malicious attacks. However, in our scheme, the *GW* does not store any information related to the user's password and biometrics. Thus, this attack is not possible in our scheme.
- **Password guessing attack:** In the scheme, the user U_i*'s* identity ID_i and password PW_i are protected by using the user personal biometrics BIO_i and the random secret ki in the smart card SC_i. In addition, in our scheme the encrypted identity is transmitted during the session establishment. Therefore, no attacker has ability to derive the

identity ID_i of the user U_i from the smart card as well as the transmitted messages during the login phase, and authentication and session key agreement phase, and as a result, our scheme is secure against the identity and password guessing attacks.

- **Replay attack**: Since each communication message during the login phase, and authentication and session key agreement phase consists of timestamps, the entities U_i, GW and SN_n identify the freshness of each message, and mutually authenticate to establish a session between U_i and SN_n. Thus, our scheme efficiently detects the reply to messages.
- **User anonymity:** In most security critical applications, the user anonymity plays an important role. Thus, it is a very essential feature in the wireless communication technology and ubiquitous computing. In our scheme, it is clear from the above discussion that the identity of the user is protected in the smart card using the user secret biometric key data and the random number. Moreover, in the communication messages, the identity is protected using the symmetric-key encryption. Hence deriving the identity in our scheme is computationally infeasible and our scheme provides the user anonymity property.

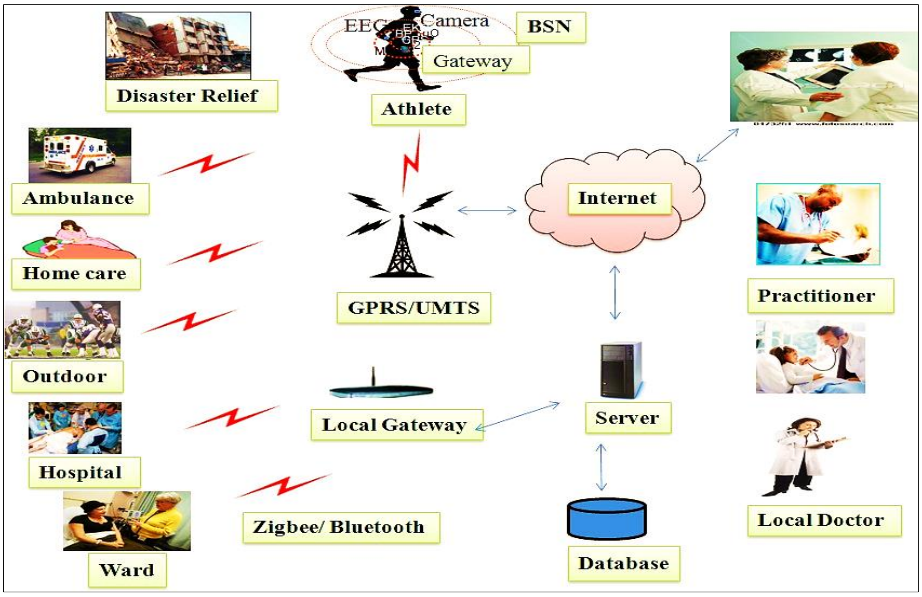

Figure 3: Usage of proposed schema in Healthcare applications

- **Forgery attack:** Suppose an attacker intercepts the login request message $m_1 = \{C_{ig}, CID_i, TS_1\}$ and try to impersonate a legal user U_i by generating the valid login request from the intercepted messages. However, the login message is protected using the symmetric-key encryption, and without the knowledge of the symmetric keys J and N_i', the attacker has no ability to generate the valid request message m_1. Thus, ours is secure against the forgery attack.
- **Unauthorised login detection with wrong password:** To avoid the denial of service to a legal user, an authentication scheme needs to quickly detect the unauthorized login credential. In our scheme, the user credentials are verified locally by the smartcard and it rejects the wrong login credentials. Thus, our scheme provides an efficient solution to detect the invalid login credentials with low complexity.
- **Efficient Password change:** In our scheme, a user freely chooses his/her password to register at the registration centre. Moreover, our scheme supports the password change locally at the smart card without contacting the registration centre. Thus, our scheme provides efficient and user-friendly password change phase.

From informal analysis, it is observed that the schema is high on security and functionality features as compared to other contemporary solutions. Thus, we accept null hypothesis

$H_0 = (AR)_{PP} \quad = (AR)_{PPH0} = \text{Secure WMSN}$

i.e., the proposed protocol (*PP*) is attack resilient (*AR*) to various well-known attacks i.e. $(AR)_{PP}$ is equal to the hypothesized attack resiliency $(AR)_{PPH0}$ using multifactor authentication and results in secure wireless medical sensor networks.

V. CONCLUSION

In this chapter, we have addressed an important need in healthcare applications involving Wireless Medical Sensor Networks. Proposed is a three-factor user authentication schema that uses smart card, password and biometrics of a health professional (user). We have reviewed and analysed our proposed schema with other state-of-the-art user authentication schemes. We observe that the proposed schema can tolerate most of the common attacks and offers additional functionality features compared to other contemporary solutions. Overall, the results make our schema very suitable for various healthcare application using WMSNs as shown in Figure 3. As part of future research, it is proposed to add biometric update and dynamic medical sensor node addition phases. Also, the proposed protocol can be extended to other application areas like Intelligent Transportation Systems (ITS), smart grids, smart buildings, smart cities, intelligent drug delivery system and even Cyber-Physical Systems (CPS) such as Nuclear Power Plant (NPP) with domain-specific enhancements.

REFERENCES

[1] J. Srinivas, D.Mishra, and S.Mukhopadhyay, “A mutual authentication framework for wireless medical sensor networks,” Journal of Medical Systems, vol. 41, no. 5, article 80, pp. 80–99, 2017.

[2] Raza S, Duquennoy S, Chung T, Yazar D, Voigt T, Roedig U. “Securing communication in 6LoWPAN with compressed IPsec.” International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), p.1–8, 2011.

[3] Q. Jiang, J. Ma, X. Lu, and Y. Tian, “An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks,” Peer-Peer Netw. Appl.; vol. 8, no. 6, pp. 1070-1081, 2014.

[4] P. Gope and T Hwang, “A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks,” IEEE Trans. on Indust. Electron; vol. 63, no. 11, pp. 7124–7132, 2016. DOI: 10.1109/TIE.2016.2585081

[5] H. L. Yeh et al.,“A secured authentication protocol for wireless sensor networks using elliptic curves cryptography,” Sensors, 11(5):4767-4779, 2011.

[6] W. Shi and P. Gong. “A new user authentication protocol for wireless sensor networks using elliptic curves cryptography,” International Journal of Distributed Sensor Networks, 2013:1-7, 2013.

[7] J. Song, G. Li, B. Xu, and C.Ma, “A novel multiserver authentication protocol with multifactors for cloud service,” Security and Communication Networks, vol. 2018, pp. 1–13, 2018.

[8] T. Truong, M. Tran, and A. Duong, “Improved chebyshev polynomials-based authentication scheme in client-server environment,” Security and Communication Networks, vol. 2019, Article ID 4250743, 11 pages, 2019.

[9] Javeria Ambareen and Prabhakar M, “Secured Wireless Sensor Network Protocol using Rabin-assisted Multifactor Authentication,”, I. J. Computer Network and Information Security, 4, 60-74, 2022. DOI:10.5815/ijcnis.2022.04.05

[10] Smith, A., Johnson, B., Williams, C., "A Comprehensive Review of IoT-enabled Wireless Medical Sensor Networks for Remote Patient Monitoring," Journal of Medical Devices and Communications, 2018

[11] Lee, D., Kim, J., Park, S., "IoT-enabled Wearable Medical Devices for Remote Patient Monitoring: A Systematic Review," Journal of Healthcare Technology, 2019

[12] Chen, L., Wang, H., Liu, R., "Enhancing Patient Care through IoT-based Wireless Medical Sensor Networks: A Case Study in Cardiac Monitoring," in: Proceedings of the International Conference on IoT and Healthcare, 2020

[13] Gupta, S., Sharma, R., Kumar, P., "A Review of Data Analytics Techniques for Real-time Health Monitoring in IoT-enabled WMSNs," IEEE Internet of Things Journal, 2019

[14] Zhang, Y., Liu, Y., Chen, T., "Security and Privacy in IoT-based Healthcare Systems: A Survey," IEEE Communications Surveys & Tutorials, 2021

[15] Johnson, M., Brown, L., Patel, S., "IoT-based Remote Patient Monitoring for Chronic Disease Management: A Review of Clinical Trials and Studies," Journal of Telemedicine and Telecare, 2018

[16] Kim, H., Park, J., Lee, S., "Interoperability Challenges and Solutions in IoT-based Healthcare Systems: A Review," Journal of Healthcare Informatics, 2022

[17] R. Amin et al., “Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks,” Comput. Netw., vol. 101, no. C, pp. 42–62. DOI: 10.1016/j.comnet.2016.01.006, 2016.

[18] *Dolev, D.; Yao, A. C. (1983),* "On the security of public key protocols" (PDF), IEEE Transactions on Information Theory, IT-29 (2): 198–208, doi:10.1109/tit.1983.1056650, S2CID 13643880

[19] Elijah, Olakunle, et al. "An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges." IEEE Internet of Things Journal, 2018.

[20] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo. “Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks,” Multimedia Systems, 21(1):49{60, 2015.

[21] P. Kumar, S. G. Lee, and H. J. Lee. “E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks,” Sensors, 12(2):1625{1647, 2012.

[22] J. Song, G. Li, B. Xu, and C.Ma, “A novel multiserver authentication protocol with multifactors for cloud service,” Security and Communication Networks, vol. 2018, pp. 1–13, 2018.