IOT-BASED SECURE WIRELESS MEDICAL SENSOR NETWORKS USING MULTIFACTOR AUTHENTICATION

Abstract

Wireless Medical Sensor Networks (WMSN) integrated with the Internet of Things (IoT) have the potential to revolutionize the medical sector, offering remote patient monitoring and personalized healthcare services. Security is of paramount importance due to the wireless nature of communication. Since vital sign parameters are overly sensitive to a patient's health status and should only be accessible to healthcare experts, maintaining patient privacy is a major concern for WMSN applications. A fundamental and widely accepted approach to address security and privacy issues in WMSNs is through user authentication while ensuring anonymity. This chapter introduces a multifactor authentication system that tackles these challenges by utilizing a combination of smart cards, passwords, and the biometrics of a healthcare professional (user). This approach aims to enhance the effectiveness, security, and scalability of IoT-based WMSNs for better patient care. Our findings suggest that the proposed system can withstand common attacks and offers more functionality compared to existing alternatives.

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

Authors

Manish Bali
Department of Computer Science and Engineering
Presidency University
Bengaluru, Karnataka, India.

Anuradha Yenkikar
Department of CSE (AI)
Vishwakarma Institute of Information Technology
Pune, India.

I. INTRODUCTION

In recent decades, human life expectancy has significantly increased due to better living conditions and advancements in public health. For instance, in 1960, the average life expectancy for Indians was only 39.93 years. However, over the years, it has risen as indicated in Figure 1. As individuals age, the likelihood of developing chronic illnesses rises, leading to a challenge in self-care and placing a significant burden on their dependents and medical system. To address this challenge, remote monitoring has emerged as a promising solution within the healthcare system, as mentioned in references [1] [2]. Wireless body area networks (WBANs), a vital component of remote monitoring setups, have attracted considerable interest from both academia and industry researchers. This is due to their potential to enhance the quality of healthcare services.

IoT is a disruptive technology that has the power to transform various sectors, including healthcare. Integrating IoT with WMSNs for remote patient monitoring stands out as one of the most promising applications of IoT in the healthcare field. This connection opens vast possibilities for enhancing patient care, advancing medical diagnostics, and revolutionizing healthcare delivery.

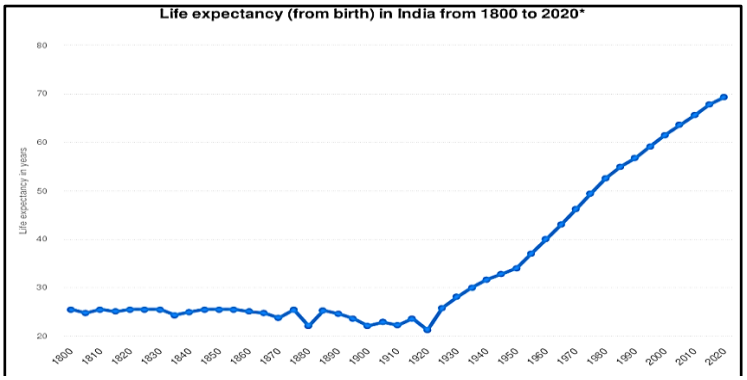

Figure 1: Life expectancy in India over the years

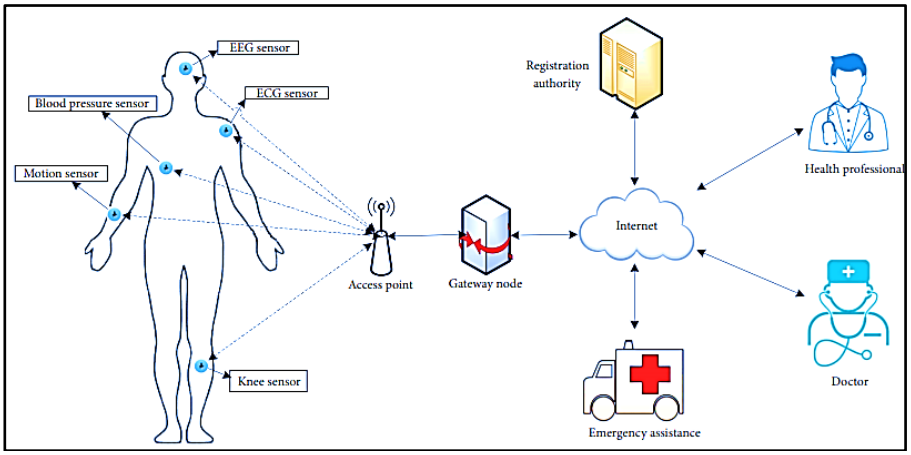

Figure 2: Network model for remote patient monitoring

Remote patient monitoring, made possible by IoT connected WirelessWMSNs, involves the continuous and non-invasive collection of patient data from various medical sensors placed on or inside the patient's body. Figure 2 illustrates an overall schematic for remote patient monitoring using WMSNs, adapted from references [3] [4] [5].

These sensors can measure vital medical parameters. The collected data is then transmitted wirelessly via IoT communication protocols to a centralized platform or a cloud-based server for real-time analysis and storage. However, there is a potential risk of malicious actors intercepting, modifying, inserting, or deleting communications transmitted through unsecured public channels [6]. Additionally, unauthorized users transmitting commands to halt the operation of wearable devices, especially those critical to a patient's survival (like cardiac pumps), poses a significant danger.

IoT-enabled WMSNs offer numerous advantages, ensuring secure remote monitoring of patients' health status. Some of these benefits include:

1. Continuous Monitoring: Unlike traditional in-person visits, remote patient monitoring allows continuous data collection, giving a comprehensive and dynamic view of a patient's health. This facilitates early detection of anomalies or changes in vital signs, enabling timely interventions.

2. Improved Patient Outcomes: IoT-based WMSNs enable early detection of health issues, leading to prompt medical interventions. This proactive approach can result in better patient outcomes and fewer hospital readmissions.

3. Increased Efficiency and Cost Savings: By reducing unnecessary hospital visits and simplifying patient care, remote patient monitoring optimizes healthcare resource utilization. This has the potential to significantly reduce costs for both healthcare providers and patients.

4. Personalized Healthcare: The continuous data stream from IoT-enabled sensors empowers healthcare professionals to customize treatment plans and medical interventions based on each patient's unique health requirements.

5. Remote Accessibility: Patients in remote or rural areas, as well as those with limited mobility, can receive high-quality healthcare without frequent visits to healthcare facilities.

6. Real-time Data Analytics: IoT-based WMSNs generate vast amounts of patient data. Utilizing data analytics and machine learning techniques, healthcare providers can extract valuable insights from this data, enabling evidence-based decision-making.

7. Early Disease Detection: IoT-enabled WMSNs can assist in detecting early signs of deteriorating health, enabling timely preventive measures and potentially reducing the severity of certain health conditions.

Numerous authentication systems have emerged in recent years to establish secure and efficient healthcare monitoring of patients utilizing Wireless Body Area Networks (WBANs). However, due to the limited energy and processing capabilities of wearable sensor nodes, authentication techniques leveraging public key encryption techniques like elliptic

curve cryptography (ECC) [7] and the Rabin cryptosystem [8] [9], come with high computational costs and are not suitable for practical applications. Consequently, employing lightweight procedures such as symmetric encryption/decryption and hash functions becomes a more feasible approach to address the limitations of public key encryption. However, upon closer scrutiny, it becomes apparent that most existing systems based on lightweight cryptographic primitives are susceptible to security vulnerabilities and are ill-suited for practical use. These systems fail to ensure forward secrecy and are vulnerable to several known attacks.

The primary contribution of this chapter is a novel, secure, and efficient user authentication scheme designed specifically for healthcare applications in WMSNs. The remaining sections of this chapter are summarized as follows: Section II: This section explores relevant studies in this field, Section III: It delves into the methodology and presents the recommended authentication schema, Section IV: This part discusses the outcomes and their implications, Section V: The conclusion of the chapter and References: The reference section at the end provides the sources cited throughout the chapter.

II. RELATED WORKS

Significant research has taken place in this domain, offering valuable insights into the current landscape of research and developments. These studies encompass various facets, including architecture, data analytics, security, clinical applications, and interoperability, thus providing a comprehensive understanding of the evolving field of modern healthcare. In this section, we will highlight some recent literature in this area. [10] offers an extensive review of the latest advancements in IoT-enabled Wireless Medical Sensor Networks (WMSNs) for remote patient surveillance. It explores different IoT-based architectures, communication protocols, and data analytics techniques utilized in these networks. The authors analyze the potential advantages and challenges of incorporating IoT in healthcare, emphasizing how remote patient monitoring can enhance patient outcomes. [11] is a systematic review that focuses on IoT-enabled wearable medical devices used in remote patient monitoring. The study evaluates the accuracy and reliability of these devices in measuring vital signs and assesses usability and user acceptance. Furthermore, it addresses security and privacy concerns associated with wearable IoT devices, proposing potential solutions. [12] presents a case study centered on the application of IoT-based WMSNs in cardiac monitoring. The authors discuss the network's design and implementation, the selection of suitable sensors, and the integration with existing healthcare infrastructure. The study highlights the effectiveness of remote patient monitoring in detecting cardiac anomalies, leading to improved patient outcomes. These studies collectively contribute to a deeper understanding of the potential of IoT-enabled WMSNs in healthcare, shedding light on its benefits, challenges, and practical applications across various aspects of patient monitoring and care.

To delve into the diverse data analytics techniques used in IoT-enabled Wireless Medical Sensor Networks (WMSNs) for real-time health surveillance, [13] provide an overview of various machine learning algorithms, data fusion methods, and anomaly detection approaches employed to analyze patient data and enable timely medical interventions. The paper also examines the challenges and opportunities within the realm of data analytics for remote patient monitoring. [14] concentrate on the crucial security and privacy aspects of IoT-based healthcare systems, including WMSNs for remote patient

surveillance. The authors review potential vulnerabilities and attack vectors targeting IoT devices, proposing security measures to safeguard patient data and ensure the confidentiality, integrity, and availability of information. [15] undertake an analysis of clinical trials and studies that have evaluated the effectiveness of IoT-based remote patient monitoring, specifically in chronic disease management. The paper focuses on conditions such as diabetes, hypertension, and respiratory diseases, demonstrating the impact of IoT-enabled WMSNs in enhancing patient adherence to treatment plans and reducing the need for hospital visits. [16] address the interoperability challenges inherent in IoT-based healthcare systems, which extend to Wireless Medical Sensor Networks. The authors review existing standards and protocols for seamless data exchange among heterogeneous medical devices and propose solutions to achieve interoperability. The paper underscores the significance of interoperability in facilitating data sharing and medical decision-making in remote patient monitoring scenarios.

These studies contribute to the comprehensive understanding of the technical, security, clinical, and interoperability aspects of IoT-enabled WMSNs for healthcare applications, shedding light on both the potential benefits and the challenges that need to be addressed for effective implementation in modern healthcare systems.

III. METHODOLOGY

IoT-enabled Wireless Medical Sensor Networks (WMSNs) are specifically designed to enable the real-time collection, transmission, and analysis of patient data for remote patient monitoring and other healthcare applications. This architecture involves the integration of hardware components, network protocols, and data management systems to ensure seamless and secure communication between medical sensors and the healthcare infrastructure. Figure 2 illustrates a typical WMSN design, which has been adapted in this chapter to align with the proposed authentication schema.

In this network model, medical sensors are strategically placed on a patient's body, creating a WBAN. These sensors actively record the individual's physiological data and transmit it wirelessly to the handheld devices of health professionals, which could include devices like personal digital assistants (PDAs), iPhones, laptops, and similar devices [17]. Consequently, physicians can access this data from the medical sensors, providing them with a more comprehensive and up-to-date assessment of the patient's health status as and when needed. The physiological data collected may encompass parameters like heart rates, body temperature, blood pressure, blood oxygen levels, and so forth. This setup allows for efficient remote patient monitoring, enabling healthcare professionals to make informed decisions and take timely actions based on the real-time patient data.

1. **Threat model:** Through power analysis attacks, an assailant can gain access to sensitive information stored within the memory of a lost or stolen smart card. To assess these security concerns, we utilize the Dolev-Yao threat model [18], which assumes that any two parties communicating can do so over an unsecured public channel. In our approach, we adopt a similar threat model where communication channels are considered insecure, and the endpoints (sensor nodes) are inherently untrustworthy. However, we trust the base station (designated as the gateway node or GWN), and the assumption is that an adversary (attacker) will never compromise the base station, as doing so would

compromise the entire network. This assumption is crucial due to economic constraints, as sensor nodes implanted on patients' bodies lack tamper-resistant hardware. Consequently, if an adversary physically seizes a sensor from a patient's body, they will gain access to all sensitive information contained within that sensor's memory.

We selected the Dolev-Yao model due to its portrayal of the Intruder as the most potent attacker. This attacker is depicted as an active saboteur, omnipotent in the sense that they can intercept, eavesdrop on, or manipulate all network traffic. Furthermore, the attacker can impersonate a valid communication partner, enabling them to initiate contact with any network participant. However, it is important to note that a Dolev-Yao attacker is incapable of compromising or breaking cryptographic primitives.

2. Notations

Table 1 describes the terminology used in this chapter

.

Table 1: Terminology 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

3. Proposed Scheme

The Scheme Comprises Five Distinct Phases:

- **Professional Registration Phase:** In this phase, professionals (users) are registered, with the registration authority being a trusted entity within the network.
- **Patient Registration Phase:** Patients are registered in this phase.
- **Pre-deployment Phase:** Actions taken prior to deployment of the authentication system are covered in this phase.
- **Login Phase:** The phase where users attempt to log into the system.
- **Authentication and Session Key Agreement Phase:** Once the login is successful, authentication is performed, and session keys are agreed upon.

The design of this scheme is based on following assumptions:

- The registration authority is trusted within the network.
- The gateway (*GW*) node maintains three secret keys, *A*, *B*, and *C*, each consisting of 256 bits.
- All entities within the WMSN are synchronized with their clocks.
- A "fuzzy extractor" technique [19] is employed to counter privileged-insider attacks and flaws in the password change phase, as observed in some other proposed schemes.
- The fuzzy extractor can derive a uniformly distributed random key, R_i, from biometric input BIO_i in a tolerant manner to errors. If another biometric input BIO_i^* is reasonably similar to BIO_i, the extracted random key R_i remains unchanged with the assistance of an auxiliary string P_i.

The fuzzy extractor comprises two procedures:

- ***Gen*(*BIO*$_i$)**: A probabilistic generation procedure that extracts random key R_i and auxiliary string P_i from biometric input BIO_i.
- **R_i^* = *Rep*(BIO_i^*, P_i)**:** A deterministic reproduction procedure that reproduces random key R_i from any biometric input BIO_i^* closely resembling BIO_i, with the aid of auxiliary string P_i.

1. **Professional Registration Phase:** In this registration phase, a health professional (referred to as U_i) aims to become a legitimate user of the WMSN. This process involves a series of steps:

- **Step 1:** U_i selects an identity (*IDi*) and a password (PW_i). Additionally, U_i*'s* personal biometrics (BIO_i) are recorded using a specific device.
- **Step 2:** *Ui* generates a 1024-bit random number (k_i) and computes the following:
  - $(\sigma_I, \tau_i) = Gen(BIO_i)$, where σ_I represents biometric key data, andτ_i is the reproduction public parameter.
  - $RPW_i = h(ID_i||k_i||PW_i)$, where *h* denotes a cryptographic hash function.

U_i sends a registration request message *{ID_i, RPW_i}*to the Gateway (*GW*) through a secure channel. Notably, σ_I and τ_i are parts of the biometric data, and RPW_i incorporates U_i*'s* identity, a random number, and the chosen password.

- **Step 3:** Upon receiving U_i*'s* registration request, the *GW* performs the following:
  - Generates a random number (r_g) and a new identity (*IDg*).
  - Computes $C_{ij} = E_J\left[r_g||ID_i||ID_g\right]$, where E_J represents encryption using the secret key *J*.
  - Computes *J*, $N_i = h\left(ID_i\left|\left|ID_g\right|\right|K\right) \oplus RPW_i$, where *K* is the *GW's* secret key.

The GW then sends a smart card (*SCi*) to U_i through a secure channel. The smart card *SCi* contains parameters including $\{C_{ij}, N_i, h(.), Gen(.), Rep(.), t\}$. This smart card plays a vital role in the user's authentication process.

- **Step 4:** Upon receiving the smart card *SCi* from the GW, U_i performs the following computations:
  - Computes $e_i = h(ID_i) \oplus k_i$
  - Computes $V_i = h\left(ID_i||RPW_i||\sigma_i\right)$
  - Computes $N_i^* = N_i \oplus h(k_i||\sigma_i)$

U_i then updates the smart card *SCi* with the following information: $\{C_{ij}, N_i^*, h(.), Gen(.), Rep(.), t, \tau_i, ei, Vi\}$. The updated smart card now contains these additional parameters, which are crucial for the authentication process in the subsequent phases.

2. **Patient Registration Phase:** In this phase, for a patient to access healthcare applications, they are required to register at the hospital's registration center (RC) through the following three steps:

- **Step 1:** The patient initiates the process by sending their name to the registration center (*RC*). This initial communication establishes the patient's intent to register for healthcare services.

- **Step 2:** The *RC*, upon receiving the patient's name, proceeds to select an appropriate sensor kit based on the patient's needs and requirements. Additionally, the *RC* designates healthcare professionals who will be responsible for overseeing the patient's healthcare needs.

- **Step 3:** The RC completes the registration process by submitting the patient's unique identity (*IDpt*) and relevant information about the chosen medical sensors to the healthcare professionals it has designated. This step ensures that the designated professionals are aware of the patient's registration and the specific sensors that will be employed for healthcare monitoring and management.

By completing these three steps, the patient is officially registered in the hospital's system, enabling them to access and benefit from the various healthcare applications offered within the network.

3. **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 *SKGW*, 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) SKGW, SN_n.

In the pre-deployment phase, sensitive information is pre-loaded into the memory of each sensor node (SN_n) before its deployment within the WMSN. This phase is carried out in an offline mode by the Gateway (*GW*) node and involves the following steps:

- **Step 1:** For each sensor node (SN_n) that will be deployed, the Gateway (*GW*) node selects a unique identity ($IDSN_n$) for that sensor node. Additionally, a unique randomly generated master key (*MSSNn*) is assigned to each sensor node.

- **Step 2:** The *GW* node calculates the pre-shared secret key between the specific sensor node (*SNn*) and the *GW* as follows:
  - $SK_{GW,SN_n} = h(ID_g||ID_{SN_n}||Q||MK_{SN_n}$,

  where:
  - ID_g is the identity of the *GW*,
  - ID_{SN_n} is the identity of the specific sensor node (SN_n),
  - *Q* is the secret key of the *GW*,
  - MK_{SN_n} is the master key of the sensor node SN_n.

  It is important to note that each secret key (*SK*) between every sensor node (SN_n) and the *GW* is distinct, ensuring unique communication between each sensor node and the *GW*.

- **Step 3:** Finally, the *GW* pre-loads the following information into the memory of each sensor node (SN_n) before its deployment:

  - The unique identity of the sensor node (ID_{SNn}).
  - The pre-shared secret key (SK_{GW}, SN_n) that was computed in Step 2.

By completing these steps, each sensor node (SN_n) is equipped with the necessary information to establish secure and unique communication with the Gateway (*GW*) node once deployed within the WMSN.

4. **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 $\sigma_i^* = Rep\left(BIO_i^{'}, \tau_i\right), k_i^* = e_i \oplus h(ID_i||\sigma_i^*), RPW_i^* = h\left(ID_i\middle||k_i^*\middle||PW_i\right)$, and $V_i^* = h\left(ID_i\middle||RPW_i^*\middle||\sigma_i^*\right)$. 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_ialso computes $CID_i = E_{N_i^{'}}[h(ID_i\left||C_{ig}\right||ID_{SN_n}||r_i||TS_1)|\left|IDD_{SN_n}\right||r_i]$, where TS_1 is the current timestamp and $IDSN_n$ is the identity of the accessed sensor node SN_nin a patient's body. Finally, SC_isends the login request message $m_1 = \{C_{ig}, CID_i, TS_1\}$ to the *GW* via a public channel.

After the sensor nodes are deployed within a patient's body in the WMSN, a health professional (referred to as U_i) needs to log in to the WMSN through the Gateway (*GW*) to access the physiological information of patients.

In this login phase, U_i follows these steps:

- **Step 1:** U_i initiates the login process by first inserting their smart card (SC_i).U_i then inputs their identity (*IDi*) and password (PW_i). Additionally, U_i records their personal biometrics ($BIO_i^{'}$) using a designated device.

- **Step 2:** U_i*'s*smart card (SC_i) performs the following computations:

  - $\sigma_i^* = Rep\left(BIO_i^{'}, \tau_i\right)$: Reproduction of the biometric key σ_i^* using the stored $\tau_i$parameter.
  - $k_i^* = e_i \oplus h(ID_i||\sigma_i^*)$: Computation of a derived key k_i^* based on e_i, the identity ID_i, and σ_i^*.
  - $RPW_i^* = h\left(ID_i\middle||k_i^*\middle||PW_i\right)$: Calculation of an updated RPW_i^* using ID_i, k_i^*, and PW_i.
  - $V_i^* = h\left(ID_i\middle||RPW_i^*\middle||\sigma_i^*\right)$: Generation of an updated V_i^* using ID_i, RPW_i^*, and σ_i^*.

- The smart card (SC_i) verifies the condition $V_i^* = V_i$. If this condition is not met, it indicates that one of the elements (identity, password, or biometric) is invalid, leading to the termination of the session.

- **Step 3:** SC_i continues with further computations:
  - $N_i^* = N_i \oplus RPW_i^* \oplus h(k_i^* || \sigma_i^*)$: Calculation of an updated N_i^* using N_i, RPW_i^*, k_i^*, and σ_i^*.
  - Generation of a random number r_i.
  - Computing $CID_i = E_{N_i'}[h(ID_i \left|\right| C_{ig} \left|\right| ID_{SN_n} || r_i || TS_1) || IDD_{SN_n} || r_i]$, where TS_1 is the current timestamp, ID_{SN_n} is the identity of the accessed sensor node SN_n within a patient's body.

Finally, SC_i sends the login request message $m_1 = \{C_{ig}, CID_i, TS_1\}$to the Gateway (*GW*) through a public channel.

These steps ensure secure authentication and access to the WMSN, allowing the health professional U_i to retrieve physiological information from the deployed sensor nodes within the network.

5. **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 mutual authentication via the Gateway (*GW*) in the WMS). This phase is composed of the following complex 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 $\left(r_g' \left|\right| ID_i' \left|\right| ID_g'\right) = D_j[C_{ig}], N_i'' = h\left(ID_i' \left|\right| ID_g' \left|\right| K\right)$ and $\left(h_1 \left|\right| ID_{SN_n}' \left|\right| r_i'\right) = D_{N_i''}[CID_i]$. The *GW* then checks if $h_1 = h\left(ID_i' \left|\right| C_{ig} \left|\right| ID_{SN_n}' \left|\right| r_i' \left|\right| TS_1\right)$? 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 $\left(ID_i', ID_{SN_n}', NID_i\right)$ in its database corresponding to the accessed sensor *SNn* for the user *Ui*. Note that *NIDi* is used to achieve the user anonymity property in our scheme. The *GW* then computes

- $A_i = r_i' \oplus h\left(SK_{GW,SN_n} || NID_i || ID_{SN_n}' || TS_2\right)$; $B_i = E_{SK_{GW,SN_n}}[h\left(NID_i \left|\right| ID_{SN_n'} \left|\right| r_i' || TS_2\right) || NID_i || ID_{SN_n}' || A_i \left|\right| TS_2]$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 $\left(h_2 \left|\left|NID_i^{"}\right|\right| ID_{SN_n}^{"} \left|\left|A_i^{'}\right|\right| TS_2^{'}\right) = D_{SK_{GW,SN_n}}[B_i]$ and checks the conditions $ID_{SN_n}^{'} = ID_{SN_n}, TS_2^{'} = TS_2$. If these are valid, SNn continues to calculate $r_i^{"} = A_i^{'} \oplus h\left(SK_{GW,SN_n} \left|\left|NID_i^{"}\right|\right| ID_{SN_n} || TS_2\right)$and checks the condition $h_2 = h(NID_i^{"} || ID_{SN_n} \left|\left|r_i^{"}\right|\right| TS_2)$. If it does not hold, the session is terminated. Otherwise, the *GW* is credible.

- **Step 5:** SN_nfurther generates a random number r_n and computes $F_i = r_n \oplus h\left(SK_{GW,SN_n} \left|\left|NID_i^{"}\right|\right| ID_{SN_n} || TS_3\right), G_i = E_{SK_{GW,SN_n}}[h\left(NID_i^{"} \left|\left|ID_{SN_n}\right|\right| r_n || TS_3)\right| \left|h\left(SK_{U_i,SN_n}\right) || NID_i^{"}\right| \left|_{ID_{SN_n}}\right| |F_i| \left|TS_3\right]$and $SK_{U_i,SN_n} = h(NID_i^{"} | \left|ID_{SN_n} \left|\left|r_i^{"}\right|\right| r_n\right)$, 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 $r_n^{'} = F_i^{'} \oplus h\left(SK_{GW,SN_n} || NID_i || ID_{SN_n}^{'} || TS_3\right)$ and checks the condition $h_3 = h(NID_i || ID_{SN_n}^{'} \left|\left|r_n^{'}\right|\right| TS_3)$. If it is valid, the GW generates a new random numberr_g^{new} , and computes $C_{ig}^{new} = E_j \left[r_g^{new} \left|\left|ID_i^{'}\right|\right| ID_g^{'}\right], r_t = r_n^{'} \oplus r_i^{'}$ and $M_i = E_{N_i^{'}}[h\left(ID_i || NID_i || C_{ig}^{new} \left|\left|ID_{SN_n}^{'}\right|\right| r_t || h_4 || TS_4\right]$, 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 $(h_5 || NID_i^* || C_{ig}^{new\ *} || ID_{SN_n}^* \left|\left|r_t^*\right|\right| h_4^* || TS_4^*) = D_{N_i^{'}}[M_i]$. After that U_i checks the conditions $ID_{SN_n}^* = ID_{SN_n}^{'}, TS_4^* = TS_4$. If these are valid, U_i computes $r_n^{''} = r_i^* \oplus r_i, SK_{U_i,SN_n}^* = h(NID_i^* || \left|ID_{SN_n}\right|| r_i \left|\left|r_n^{"}\right|\right|)$.

- Step 9. $U_i$then checks the conditions $h_4^* = h\left(SK_{U_{i,SN_n}}^*\right)$ and $h_5 = h\left(ID_i||NID_i^*||C_{ig}^{new^*}\left||ID_{SN_n}\right|\right|h_4^*\left||r_n^{"}\right|\left|TS_4\right)$. 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.

The informal analysis aims to evaluate the proposed schema's ability to withstand common attacks and to assess its functionality features. Given that the schema involves wireless communication, ensuring secure communication is of paramount importance in WMSNs. The hypothesis being evaluated is whether the proposed protocol (*PP*) demonstrates attack resilience (*AR*) against well-known attacks, which implies that it results in a secure WMSN. This hypothesis is expressed in terms of a null hypothesis (H_0) and an alternative hypothesis (H_1) as follows:

- **Null Hypothesis (H_0):** $(AR)_{PP} = (AR)_{PPH0}$ (1)

  This hypothesis assumes that the proposed protocol is not significantly more attack resilient than the hypothesized baseline level of attack resilience.

- **Alternative Hypothesis (H_1):** $(AR)_{PP} \neq (AR)_{PPH0}$ (2)

  This hypothesis suggests that the proposed protocol demonstrates a significant level of attack resilience beyond the hypothesized baseline level, making it more secure than expected.

  In other words, the null hypothesis states that the proposed protocol's attack resilience is not significantly different from the baseline (expected) level, while the alternative hypothesis asserts that the proposed protocol indeed exhibits a higher level of attack resilience than expected. The goal is to gather evidence through testing and analysis to determine whether the proposed protocol enhances the security of WMSNs by effectively countering common attacks, thereby validating the alternative hypothesis.

IV. RESULTS AND DISCUSSION

In Table 2, we compare the performance of the suggested schema to that of various state-of-the-art models.

1. **Privileged Insider Attack**: This type of attack involves a privileged insider collecting user credentials and attempting to use them on behalf of a legal user. The schema ensures security by securely conveying user credentials, such as ID_i, PW_i and Bio_i, using a one-way hash function and a random secret key k_i. Even if an attacker gains access to the smart card SC_i, the password guessing attack will fail since k_i is unknown. Similarly, without knowledge of Bio_i, the attacker cannot acquire the biometric key data σ_1. Therefore, the schema effectively withstands the privileged insider attack.

Table 2: Comparison of security and functionality features

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

2. **Stolen Smart Card Attack**: If a user's smart card SC_i is stolen or lost, an attacker may attempt to extract information from it. However, the schema's design ensures that the user identification (ID_i) and password (PW_i) are protected using the secret biometric key data σ_I and the secret random number k_i. Deriving the user credentials is computationally infeasible, making the schema resistant to smart card theft.

3. **Stolen Verifier Attack**: This attack involves an attacker stealing user information from the *GW*. However, the proposed schema does not save any information on the user's password or biometrics in the *GW*. As a result, this type of attack is not feasible within the architecture of the schema.

4. **Password Guessing Attack**: The schema employs a technique that effectively protects the user's identity (ID_i) and password (PW_i) by utilizing personal biometrics (BIO_i) and a random secret key (k_i) stored in the smart card SC_i. Additionally, during the session setup, encrypted identification is transmitted. This approach ensures that attackers cannot deduce the user's identity or password from the smart card or the sent messages during the

login, authentication, and session key agreement phases. Thus, the schema effectively guards against identity and password guessing attacks.

5. **Replay Attack**: For preventing replay attacks, the schema incorporates timestamps in each communication message throughout the login, authentication, and session key agreement phases. These timestamps enable the involved entities (U_i, GW, and SN_n) to determine the freshness of each message and mutually authenticate, creating a secure session between U_i and SN_n. This feature efficiently detects message replays, enhancing the overall security of the system.

6. **User Anonymity**: The schema acknowledges the importance of user anonymity, particularly in security-critical applications. By utilizing the user's secret biometric key data and a random number, the smart card safeguards the user's identity. Furthermore, the identity remains secured in communication messages through symmetric-key encryption. As a result, determining the user's identity within this scheme is computationally impossible, ensuring user anonymity, a vital aspect of the system.

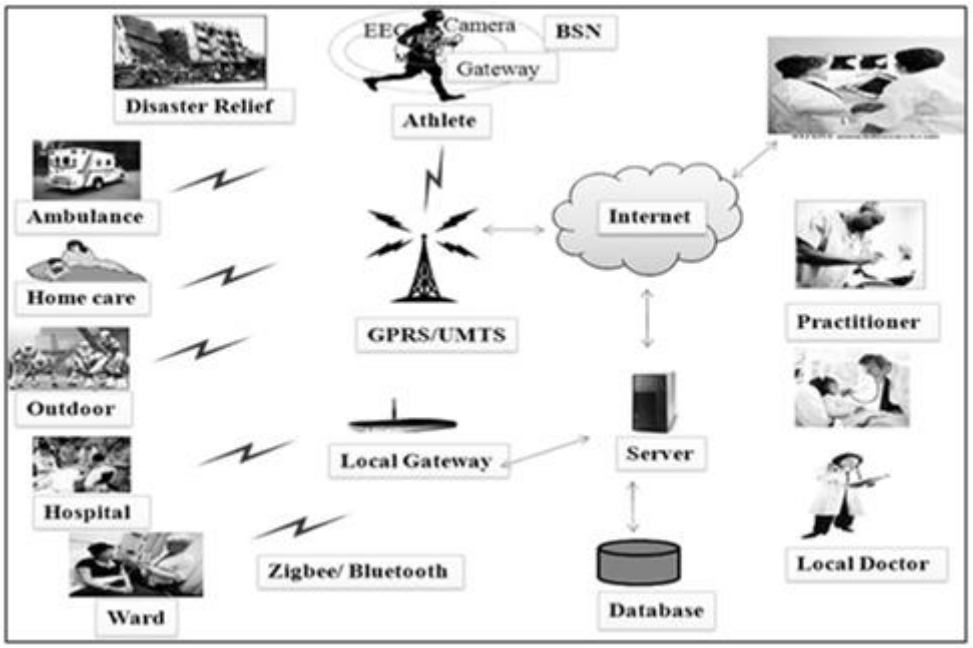

Figure 3: Usage of proposed schema in Healthcare applications

7. **Forgery Attack**: The scheme is resistant to forgery attacks. Even if an impersonator tries to decipher the message (m_1) and tries to act like a legitimate user, they cannot produce a valid request without knowing the symmetric keys (J and N_i'.). This property ensures that the schema is safe against counterfeit attempts.

8. **Unauthorized Login Detection with Wrong Password**: The authentication mechanism in the scheme efficiently identifies unauthorized login attempts with incorrect credentials. This feature helps prevent denial of service to legitimate users by quickly detecting and rejecting improper login credentials, adding an additional layer of security.

9. **Efficient Password Change:** The schema allows users to select their own passwords during registration, and it enables password changes to be made locally on the smart card without the need to visit the registration department. This approach enhances the user experience by offering an efficient and user-friendly process for password replacement.

These aspects collectively demonstrate that the proposed schema addresses key security concerns, provides efficient mechanisms for detecting unauthorized login attempts, and offers a user-friendly approach for password management, making it a robust and practical solution for secure authentication in the context of WMSNs.

According to informal examination, the schema has a satisfactory level of security and functionality when compared to other contemporary alternatives. As a result, we accept the null hypothesis.

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

Specifically, the suggested protocol *(PP)* is attack resilient *(AR)* against a variety of well-known threats, i.e. $(AR)_{PP}$equals the hypothesized attack resilience $(AR)_{PPH0}$when utilizing multifactor authentication, resulting in secure WMSNs.

V. CONCLUSION

This chapter addresses a crucial requirement in healthcare applications that utilize WMSNs. The proposed solution involves a robust three-factor user authentication schema, which leverages a smart card, a password, and the biometrics of health professionals (users). A comprehensive comparison was conducted between the suggested schema and various state-of-the-art user authentication techniques. The results demonstrate that the proposed schema exhibits robustness against a wide range of common attacks while offering superior functionality compared to existing alternatives. The findings from this study suggest that the proposed schema is highly suitable for diverse healthcare applications that rely on WMSNs, as depicted in Figure 3. Furthermore, the study provides insightful recommendations for future research. These suggestions include incorporating biometric updating mechanisms and dynamic addition stages for medical sensor nodes. With such enhancements, the proposed protocol can be adapted to other domains. In summary, the proposed three-factor user authentication schema offers a secure and functional solution for healthcare applications in WMSNs. Its potential for further expansion and adaptation to other critical domains makes it a valuable contribution to the field of WSNs and opens doors to even broader applications.

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.

