Received: *1 May 2023* | *Revised:* *29 June 2023* | *Accepted:* *29 June 2023*
DOI: 10.37917/ijeee.19.2.14 *Vol. 19 | Issue 2 | December 2023*

Open Access

Iraqi Journal for Electrical and Electronic Engineering
Original Article

IJ EEE University of Basrah College of Engineering

Authentication Healthcare Scheme in WBAN

Abdullah Mohammed Rashid[1], **Ali A. Yassin** *[2], **Abdulla J. Y. Aldarwish**[2], **Aqeel A. Yaseen**[3], **Hamid Alasadi**[2], **Ammar Asaad**[2], **Alzahraa J. Mohammed**[2]

[1]Department of Computer, Education College for Human Science, University of Basrah, Basrah, Iraq
[2]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq
[3]Ministry of Education, Basrah, General Directorate of Education in Basrah, Iraq

Correspondance
*Ali A.Yassin
Computer Science,
College of Education for Pure Sciences,
University of Basrah, Basrah, Iraq
Email: aliadel79yassin@gmail.com

Abstract

A wireless body area network (WBAN) connects separate sensors in many places of the human body, such as clothes, under the skin. WBAN can be used in many domains such as health care, sports, and control system. In this paper, a scheme focused on managing a patient's health care is presented based on building a WBAN that consists of three components, biometric sensors, mobile applications related to the patient, and a remote server. An excellent scheme is proposed for the patient's device, such as a mobile phone or a smartwatch, which can classify the signal coming from a biometric sensor into two types, normal and abnormal. In an abnormal signal, the device can carry out appropriate activities for the patient without requiring a doctor as a first case. The patient does not respond to the warning message in a critical case sometimes, and the personal device sends an alert to the patient's family, including his/her location. The proposed scheme can preserve the privacy of the sensitive data of the patient in a protected way and can support several security features such as mutual authentication, key management, anonymous password, and resistance to malicious attacks. These features have been proven depending on the Automated Validation of Internet Security Protocols and Applications. Moreover, the computation and communication costs are efficient compared with other related schemes.

Keywords
WBAN, healthcare, sensitive data, mutual Authentication, AVISPA.

I. Introduction

With the rapid growth of the Internet, the Internet of Things (IoT), cloud computing, and the usage of wireless networks in the daily lives, life has become easier. IoT services are almost boundless, as they fuse the real and Internet worlds. The IoT has applications that can be found in several areas, such as smart cities, vehicle networks, and healthcare systems [1]. Currently, information technology plays the primary role in expense pressure, as keeping an eye on the health state of a patient remotely is now possible, thus avoiding hospitalization [2, 3]. A WBAN considers a part of a wireless sensor network that is applied in several areas, including comprehensive healthcare, according to its ability to observe the patient's health information to follow the health cases of a customer that leaves the health care center. However, the applications of WBAN are numerous in other fields, such as GPS and E-bank [4, 5, 6, 7]. Generally, a WBAN consists of biometric sensors suitable for collecting health information by measuring vital signals from the human body[8]. These biometric sensors can send vital signals to a personal device (a smart mobile phone or a portable computer), which connects to an authentication server. This server is able to take necessary actions in emergency situations as well as saves the patients' information on a secure database [9]. Figure 1 shows the central organization of a WBAN. Much like other wireless networks, the WBAN suffers from information security, data integrity, and availability challenges. The data of WBAN are transferred via a normal channel. Therefore, it is in jeopardy of security problems and privacy breaches [10]. In this context, security refers to the protection of data from illegal use while they are connected, transferred, processed, and saved. Privacy refers to the ability to maintain the confidentiality of a patient's personal information, such as his/her name and details about his/her health [11]. In 2018, Wei et al. [12] proposed a secure authentication scheme that depended on a low-entropy PIN. Their work can be more convenient for WBAN to apply on a simple-to-recall PIN. In 2019, Kompara et al. [13] presented a good authentication system for a two-hop WBAN with a confirmation on a pseudonym and nonchase merit. The performance and solidity of this system were elucidated utilizing an unofficial analysis, which was then officially confirmed. Koya and Deepthi [14] supported an authentication scheme based on physiological signals. The authors' opinion was that physiological value assistance was employed in protecting the scheme versus sensor node impersonation attacks. Wang et al. [15] proposed a swift authentication method for health contingencies; their work relied on decreasing authentication time to lug contingencies speedily without aiding a physician. Dodangeh et al. [16] suggested a good authentication scheme depended on the biometric merits of the human body. The authors offered two schemes for authentication and key agreement in WBAN. Their work applied biometric features, secure exchanged data, and an essay password to supply security. In 2019, Liu et al. [17] developed a modern authentication scheme that was distinguished using a dynamic password. The main aim of this research is to develop secure scheme for patient's health cases observation.

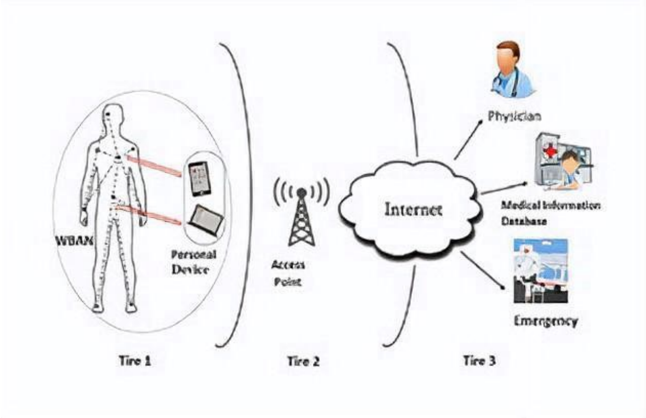


Fig. 1. WBAN organization

A. THE RESEARCH CONTRIBUTIONS

The contributions of the proposed scheme can be summarized in the following points:

- To keep the energy of the sensor, the time at which the pivotal signals are submitted from a sensor during categorizing the signals into two types, normal and abnormal, are specified. This classification includes all types of sensors used in this work, such as body temperature sensor.
- In the patient's health care part, an adequate scheme attached to the patient's device, which can analyze the class and type of the sensor's signal and perform suitable actions without demanding a physician, is proposed.
- This work is characterized by strong security and high confidentiality in terms of exchanging information between the basic parts of the components of the work environment.
- This proposed scheme is very important and can be used by patients, the elderly, athletes, and those interested in continuously monitoring the functions of their vital bodies.
- On the security side, the proposed scheme can resist familiar attacks such as insider attacks, MITM attacks, and DoS attacks. Moreover, AVISPA prove the security of the proposed scheme.

B. Organization

This paper is organized as follows: Section 2 presents an architecture of WBAN's organization. Section 3 displays the proposed scheme. Section 4 demonstrates the formal analysis and the results of the experiment. Section 4 consists of a comparison with other related schemes. Section 5 presents the conclusions.

II. Architecture of WBAN

A. System Components of WBAN

The components of the WBAN system are sensors (S_i), personal devices (PD_i), and an authentication server (AS). Figure 2 presents the components of the WBAN system. Sensors (S_i): Sensors are considered limited resources, as they have the ability to collect patients' health data and send signals to personal devices via Bluetooth or Wi-Fi. Personal device (PD_i): A personal device is a communication tool that can connect biometric sensors, users, and an authentication server. A personal device can interpret the sensor's signals and send information to the server or notify the patient about his/her health condition through an application provided by the health institution. Authentication server (AS): An authentication server has many roles, including saving the sensitive information of the patients in a secure database, analyzing data, and processing and distributing data to the relevant people.

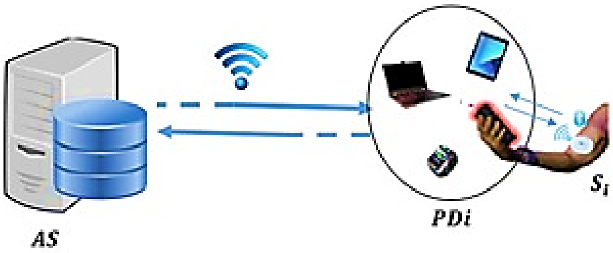


Fig. 2. Components of WBAN

B. System Model

The proposed scheme consists of biometric sensors (BS_i), personal devices (PD_i), and an authentication server (AS). The BS_i can collect vital signals from the human body, which have two types: normal and abnormal. A normal signal is sent to the PD_i every 12 hours, whereas any abnormal signal is sent immediately. This purpose is to conserve the sensor's energy, which is only used in critical situations. The personal device submits a complete report of the patient's health condition to the authentication server on the last day. This report contains the details of the patient's health status, such as the duration of his/her stable state, the number of critical incidents he/she experienced, and the number of times his/her medical practitioner was contacted. This report is carried out for archiving and the future study of the patient's condition. In the event of an abnormal signal, the PD_i either notifies the patient of his/her health condition if the patient is in a state of consciousness or sends information directly to the server so that the necessary action can be carried out. The AS sends the details of the patient's condition to the concerned people, such as his/her doctor and other practitioners responsible for the patient. The PD_i includes the health institution authority's application, through which the user is logged in. This application receives the sensor's signals, interprets them, and sends a warning message on the phone screen to the people concerned as well as a voice alert to notify the user. Additionally, all components exchange data securely based on strong security features such as mutual authentication, key management, and password anonymity.

C. Security Issues in A WBAN Environment

As the components of WBAN $(S_i, PD_i, and$ AS) exist in an unattended environment, the various ways an attacker can penetrate the network must be studied [7]. Below are some possible malicious attacks on WBAN components [18]:

- **MITM Attack**: An attacker has many attempts to disconnect the communication channel between a rightful patient (PD_i) and the remote server (AS) by embodying a rightful patient or server during a study attack's method.
- **DoS Attack:** A DoS attack is a type of malicious attack that aims to disrupt the services provided by the server by flooding the network with an inundation of fake login requests.
- **Stolen Personal Device:** An adversary has the ability to reproduce the user (PD_i)-sensitive data and then apply this information to impersonate a genuine patient to destroy the system.
- **Forged Sensor:** The main function of this attack comprises a fake sensor annoying to submit unfitting information using the patient's identity. It is hazardous to the health of the patient.

D. Security Requirements

Several security requirements are measured throughout the design progression of all authentication schemes [7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17]:

- Mutual Authentication: The main system components of WBAN should authenticate one another's identities as a first step and then exchange data as a second step to prevent the risks of attackers.
- User Anonymity: In the login and authentication phases, any proposed scheme should avoid eavesdropping or sniffing the exchanging information between components by applying this feature to their identities.
- Confidentiality: Sensitive patient information must be protected from attackers by using encryption techniques for all communication messages between system parties.
- Availability: The patient needs to use/access the resources of WBAN anytime and anywhere.
- Forward Secrecy: A session key allows the main parties to use WBAN's system and should only be used once to access the scheme.

III. The Proposed Scheme

This scheme has four main phases: setup, registration, authentication, and healthcare. The components of the proposed schemes are patient (P), Health Care Center (HCC), Authentication Server (AS), Personal Device (PDi), and sensors (S). The main difference between a HCC and AS in a WBAN is that the former is responsible for establishing trust between entities, while the latter is responsible for verifying the identity of devices.

A. Setup and Registration Phases

Symmetric encryption can be represented by the tuple of three main polynomial–time steps SKE =(Gen, Enc, Dec). Step Gen receives a secured factor λ and creates shared key K. Step Enc depends on K and plaintext m, and produces ciphertext c. Step Dec depends on K and ciphertext c to produce the real plaintext m. In the proposed scheme, the following steps are used:

- Key generation $Gen(1^{\lambda})$: The health care center (HCC) runs the key generation step. It uses security factor λ (where λ represents the length of the secured keys) and generates secret key Sh_{S_i}, Sh_{PDi}.
- The HCC is responsible for providing each patient (P_i) the personal device(PD_i) and set of sensors based on his/her case that is diagnosed by doctor (D_i). Moreover, HCC provides (Sh_{si}, Sh_{PDi}) to S_i and PD_i, respectively. PD_i may denote the patient's mobile phone.
- P_i registers on AS as the following steps:
  - The patient picks his identity (IDP_i) and password $(PWP_i\ )$.
  - (PD_i) computes $IDP_i = h(IDP_i,\ Sh_{PD_i})$ and $PWP_i = h(PWP_i,\ Sh_{PD_i})$. Then, it sends IDP_i and PWP_i to AS.
  - Upon receiving a registration request, AS determines from its database if P_i is previously recorded. If it holds, AS terminates the current phase. Otherwise, it adds the primary parameters $(IDP_i, PWP_i, Sh_{PDi}, Ph, andRel)$ of P_i to its database. Ph is the phone number of P_i, and Rel represents the main information of the patient's relatives (such as brothers, sisters, and friends).
  - HCC supports P_i in the set of sensors, and each one (S_i) should be registered in the AS by the HCC as follows:
    - ∗ The sensor's identity is computed based on its serial number (Se_{num_i}) attached from the industry company $ID_{S_i} = h(Se_{num_i} \oplus Sh_{S_i})$.
    - ∗ A password (PW_{S_i}) for S_i is selected.
    - ∗ $(\ ID_{Si},\ PW_{S_i})$ is sent to PD_i.

B. Login and Authentication Phases

The login and authentication processes between S_i and PD_i are executed as below:

- S_i selects a random integer value $r_i \in Z^*$ and calculates $PW'_{S_i} = h(PW_{S_i},\ r_i)$ and $E_{S_i} = Enc_{Sh_{S_i}}(r_i)$.
- S_i sends $<ID_{Si},\ PW'_{S_i}, E_{S_i}>$ to PD_i.
- Upon receiving the sensor's request, PD_i checks the validity of S_i by decrypting function $r_i = Dec_{Sh_{S_i}}(E_{S_i})$. Then, PD_i computes $PW''_{S_i} = h(PW_{S_i},\ r_i)$ and compares PW''_{S_i} with PW'_{S_i}. If the results match, the sensor is ready to send its signals; otherwise, PD_i terminates this phase.
- The above steps are performed once for preserving the energy of the sensor.

  PD_i needs to login the system via AS for exchanging data between. PD_i and AS as follows:

- PD_i generates an integer random number $R_A < q$; computes $V_A = g^{R_A}\ mod\ q$; where q is a prime number, and is g a primitive root modulo q; and computes $PWP^{'}_{i} = h(PWP_i||\ Sh_{PD_i}||\ R_A)$ and $E_{PD_i} = Enc_{Sh_{PD_i}}(V_A)$. Then, it sends $<IDP_i,\ PWP^{'}_{i},\ E_{PD_i}>$ to AS.
- Upon receiving $<IDP_i,\ PWP^{'}_{i},\ E_{PD_i}>$, AS ensures from received information by computing the following:
- E_{PD_i} is decrypted using $V'_A = Dec_{Sh_{PD_i}}(E_{PD_i})$. $R'_A = \sqrt[g]{V'_A}$ and $PWP^{''}_{i} = h(PWP_i||\ Sh_{PD_i}||\ R'_A)$ are computed.
- $PWP^{''}_{i}$ is compared with $PWP^{'}_{i}$. If the result is a match, AS generates an integer random number $R_B < q$; computes $V_B = g^{R_B}\ mod\ q$, computes $E'_{PD_i} = Enc_{Sh_{PD_i}}(V_B,\ Ch)$; $Ch \in \{1,\ 0\}$ where AS rebuilds shared secret key $Sh_{PD_i} = Sh_{PD_i} \bigoplus (V'_A * R_B)$ for the next going request session and sends a challenge (Ch) to tell PD_i to compute a new key for a new login request.
- Then, it sends $<E'_{PD_i}>$ to PD_i.
- Upon receiving $<E'_{PD_i}>$, PD_i retrieves $V^{'}_{B}$, Ch based on $Dec_{Sh_{PD_i}}(E'_{PD_i})$ and then generates a fresh key for the next login request $Sh_{PD_i} = Sh_{PD_i} \bigoplus (V^{'}_{B} * R_A)$. The main function of Ch provides a pulse to compute a new Sh_{PD_i}.

Figure 3 explains the organization of the current phases.

C. Healthcare Phase

In the proposed scheme, three kinds of S_i are used: a blood pressure sensor, a body temperature sensor, and an oxygen sensor. The following points explain how sensors work, and the body temperature sensor is taken as an example:

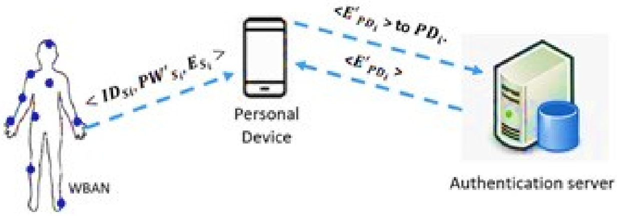


Fig. 3. Login and authentication phases

- The body temperature sensor has the ability to obtain the temperature of the patient and redirects the values to the PD_i based on the following conditions:
  - Normal: If the value of the temperature signal >= 36.5 and the temperature signal <= 37.2, the case of the patient is normal, and then the result is sent to PD_i every 12 hours while the normal case is continuous [8].
  - Abnormal: If the value of the temperature signal is greater than 37.2, this result is sent to PD_i directly. PD_i observes the reaction of P_i and his detailing with the warning message via PD_i. If the interaction of P_i is negative, PD_i submits the medical information of P_i to AS for the necessary action to be taken. Then, AS retrieves the phone numbers of the doctors and relatives of the patient to tell them about their emergency.
- Finally, (PD_i) sends a medical report of the patient to AS at the end of the day. This report is saved in the database of AS to be used by doctors or authors in the future.

IV. Formal Analysis

A. Security Analysis

This work can enjoy several security features as follows.

Correctness

- The fast authentication of S_i is proven below:
  - PW'_{S_i} is calculated based on decrypted E_{S_i} to obtain r_i via secret key Sh_{S_i}, so the password process of a sensor S_i is correct:
  - $$PW''_{S_i} = \; h(PW_{S_i},\, r_i) = PW'_{S_i}$$
  - As a result, the authentication phase is proven correct from S_i to PD_i.
- The fast authentication of PD_i is confirmed as below:

$$PWP''_i = h(PWP_i||\; Sh_{PD_i}||\; R'_A)$$

$$= h(PWP_i||\; Sh_{PD_i}||\sqrt[g]{V'_A})$$

$$= h(PWP_i||\; Sh_{PD_i}||R_A)$$

$$= PWP'_i$$

The left side (PWP'_i) is matched with the right side in the above proof. Therefore, the authentication phase is verified from PD_i to AS.

- Providing Key Agreement and Key Freshness: The key agreement depends on main components and secure parameters $<S_i\;, PD_i\;, AS\;, Sh_{S_i}, Sh_{PD_i}>$ in the proposed scheme. The first one is connected with S_i and PD_i, where the secret key is Sh_{S_i}. The second fold depends on Sh_{PD_i} used by components PD_i and AS, and Sh_{PD_i} is generated once for each login request. The following steps illustrate the mechanism of generating a key:
  - PD_i generates an integer random number $R_A < q$ and computes $V_A = g^{R_A}\; mod\; q$.
  - PD_i sends $E_{PD_i} = \; Enc_{Sh_{PD_i}}(V_A)$ to AS.
  - AS generates an integer random number $R_B < q$ and computes $V_B = g^{R_B}\; mod\; q$ and $E'_{PD_i} = Enc_{Sh_{PD_i}}(V_B)$. Then, it sends $<E'_{PD_i}>$ to AS.
  - PD_i computes $Sh_{PD_i} = Sh_{PD_i} \bigoplus\, (V'_B * R_A)$.
  - AS computes $Sh_{PD_i} = Sh_{PD_i} \bigoplus\, (V'_A * R_B)$. Consequently, the proposed scheme supports key freshness for each login session.
- Providing Anonymity and Untraceability: Assume the attacker (Ã) can capture the important parameters such as PW'_{S_i}, PWP'_i in the communication channel between components. On the side of S_i, employing the random r_i in the login message demand $< ID_{Si},\; PW'_{S_i}, E_{S_i} >$ refers to the generation of the message one time for each demand. λ faces difficulties to obtain (r_i) from E_{S_i}.

  On the other side, Ã fails to trace or obtain a one-time password PWP'_i between PD_i and AS. In each login phase, PD_i computes anonymous password $PWP_i^{'} = h(PWP_i|| \, Sh_{PD_i}|| \, R_A)$ that is generated once based on R_A. AS can ensure the validity of $PWP_i^{'}$ because it owns Sh_{PD_i}, g to compute R'_A and then obtains $PWP_i^{''} = h(PWP_i|| \, Sh_{PD_i}|| \, R'_A) = PWP_i^{'}$.

Hence, the present scheme supports anonymity and untraceable metrics.

- Withstanding MITM Attacks: Assume an attacker (A) has gained a requested demand from S_i to PD_i $< ID_{Si}, \, PW'_{S_i}, E_{S_i} >$, and from PD_i to $AS < IDP_i, PWP_i^{'}$, $E_{PD_i} >$ and vice versa, any attempt to change these messages by A fails to verify from the other side, as the changed parameters do not match with the original parameters. Additionally, A cannot obtain pivot parameters such as $Sh_{PD_i}, R_A, \, R_B, \, g, \, and \, Sh_{S_i}$. Moreover, the exchanged messages between components are only produced once for each sign-in demand.

- Withstanding Eavesdropping, Traffic, Black Hole Attacks: Suppose (Ã) attempts to quote information to implement the current attack, and these messages comprise the exchange of information between all components (S_i, PD_i, AS), as shown below:

$$S_i \quad \overset{<ID_{Si}, \, PW'_{S_i}, \, E_{S_i}>}{\rightarrow} \quad PD_i$$

$$S_i \quad \overset{<pivotal \; signals>}{\rightarrow} \quad PD_i$$

$$PD_i \quad \overset{<IDP_i, \, PWP_i^{'}, \, E_{PD_i} \, >}{\rightarrow} \quad AS$$

$$AS \quad \overset{<E'_{PD_i} \, >}{\rightarrow} \quad PD_i$$

$$PD_i \quad \overset{Message \; to \; renew \; Sh_{PD_i}}{\rightarrow} \quad AS$$

$$PD_i \quad \overset{<Case \; emergency \; of \; P_i \, >}{\rightarrow} \quad AS$$

Previously, all the above messages have been generated once. Consequently, A cannot apply the eavesdropping and traffic attacks. Furthermore, the above security analysis shows the proposed scheme can protect from a Forged S_i and resist DoS and replay attacks. Furthermore, a Black Hole Attack can also occur in Wireless Body Area Networks (WBANs), which are small, low-power networks that connect wearable devices to a central hub. In a WBAN, a malicious node can launch a Black Hole Attack by falsely advertising itself as having a stronger signal or a shorter path to the central hub, causing other nodes to route their data through it. The malicious node then discards or modifies the incoming data, potentially compromising sensitive medical information. In the proposed work, the secure communication based on encryption (E_{PD_i}, E'_{PD_i}, E_{S_i}) and mutual authentication ($< ID_{Si}, \, PW'_{S_i}, \, E_{S_i} >$, $<IDP_i, \, PWP_i^{'}, \, E_{PD_i} >$, $<E'_{PD_i} >$), can be used to protect the transmitted data.

- Resisting Replay Attacks: Assuming that an adversary (A) intercepts request messages $< ID_{Si}, \, PW'_{S_i}, E_{S_i} >$ or $<IDP_i, \, PWP_i^{'}, \, E_{PD_i} >$ and attempts to use these messages to allow A to use the services of the system, these parameters are generated once due to R_A and r_i so A cannot resend a message request. Furthermore, A cannot access any other value of the system's components because it does not know keys Sh_{S_i} and Sh_{PD_i}. Therefore, the proposed scheme is secure against replay attacks.

- Resisting DoS Attacks: In the proposed scheme, all requested messages are linked to random values R_A and r_i. In normal cases, messages must be variable and not fixed. Therefore, repeating the same message without any alteration reveals the attack, and the repeated message is rejected. In this scheme, all exchanged messages within the system's components are unique and generated once during the login and authentication phases. This feature can be considered a part of the message validation. Therefore, the scheme resists DoS attacks.

- Protecting from Stolen PD_i Attack: If a (PD_i) is stolen, all the saved information $(ID_{Si}, PW_{si}, PW_{Si}$, $SH_{ki})$, and (Sh_{Si}) would be available to an adversary (A). However, A cannot resend older messages because this scheme is resistant to replay attack, and they cannot create new medical information because this information contains the patient's location. Owing to these above reasons, A would not benefit from a stolen PD_i and access the system. Therefore, the proposed scheme is protected from instances of stolen personal devices. Unlinkability: Any two visible system components' connection cannot be specified. Various acts can be changed privately and randomly without everyone else knowing the connection between them.

- Smart Factor: The login to the system as a smart factor makes the system available permanently. This process reduces the login efforts in applications, is performed after the first login to the system or application, and adds efficiency and flexibility to the proposed scheme.

B. AVISPA

Focus is on an official investigation called AVISPA to check whether the proposed scheme is protected. This protocol depends on High-Level Protocol Specification Language (HLPSL) [19, 20, 21], whose translated file is an intermediate format.

On the security side, AVISPA provides four back-end analyzers, OFMC, CL-AtSe, SAT-based Model-Checker, and Tree Automata-based Protocol Analyzer, as shown in Fig. 4. The same basic symbols in Table I are used to implement the proposed scheme in HLPSL and then check the validity of our work with the AVISPA result. Figures 5, 6, 7, 8, and 9 denote implementing the proposed scheme in AVISPA and prove the security features.

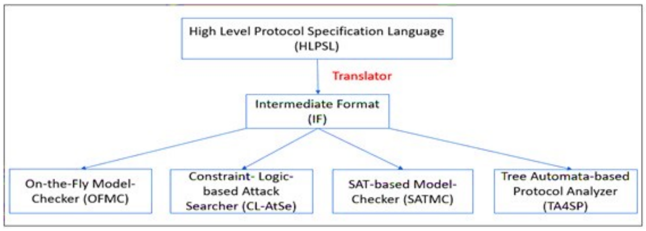
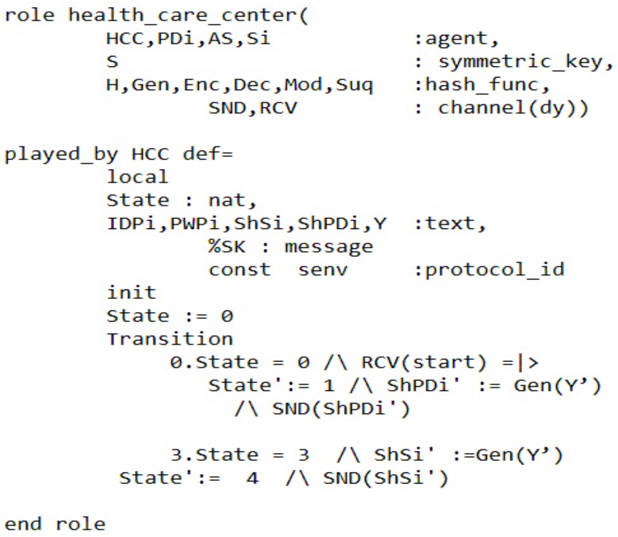

High Level Protocol Specification Language (HLPSL)
Translator
Intermediate Format (IF)
On-the-Fly Model-Checker (OFMC)
Constraint- Logic-based Attack Searcher (CL-AtSe)
SAT-based Model-Checker (SATMC)
Tree Automata-based Protocol Analyzer (TA4SP)

Fig. 4. AVISPA structural design

TABLE I.
SYMBOLS USED IN THIS PAPER

Symbols	Description
P_i	User, which may be a patient or their relatives
D_i	The doctor is responsible to check patient
S_i	Any sensor that is connected to the patient
PD_i	Special device of each patient
AS_i	Remote Authorized server
ID_{si}	The identity of S_i
PW_{si}	The password of S_i
IDP_i	The identity of patient
h	Salt hash function
PWP_i	The password of patient
SH_{ki}	Shared key between S_i and AS
Sh_{si}	Shared key of encrypted information between S_i and PD_i
Sh_{PDi}	Shared key of encrypted information between PD_i and AS
Medical information	**Includes the patient's information, medical state, and location**



```
role health_care_center(
        HCC,PDi,AS,Si                :agent,
        S                            : symmetric_key,
        H,Gen,Enc,Dec,Mod,Suq        :hash_func,
                SND,RCV              : channel(dy))

played_by HCC def=
        local
        State : nat,
        IDPi,PWPi,ShSi,ShPDi,Y  :text,
                %SK : message
                const  senv         :protocol_id
        init
        State := 0
        Transition
             0.State = 0 /\ RCV(start) =|>
                State':= 1 /\ ShPDi' := Gen(Y')
                  /\ SND(ShPDi')

             3.State = 3  /\ ShSi' :=Gen(Y')
         State':=  4  /\ SND(ShSi')

end role
```

Fig. 5. Specification of health care center in HLPSL

In practical terms, by using AVISPA, the proposed authentication scheme for a WBAN can ensure that the scheme is secure and meets the necessary requirements for protecting sensitive medical information. Figure 5 explains the main role of the health care center (HCC) in distributing the setup parameters to the WBAN components (P , PD_i , S_i , AS) . The login of sensors in the proposed scheme can be applied in AVISPA by using Fig. 6. Figure 7 denotes the login and authentication phase on the side of sensors (S_i) and personal device (PD_i) up to the sending of the main authentication parameters from $PD_i$to AS. Figure 8 plays more attention for checking the validity of $PD_i$and then sends challenge in encrypted manner to $PD_i$for achieving to mutual authentication between $PD_i$and AS. Figure 9 is responsible for the contracting and running main session of proposed scheme.

V. COMPARISON WITH SIMILAR SCHEMES

The main comparison relies on the security features of proposed scheme with some previous authentication schemes, as shown in Table II. However, the proposed scheme has many security features such as smart factor, unlinkability, and resistance to well-known attacks like protection from a stolen $\mathbf{PD_i}$ attack. Table III focuses on a comparison using the computational cost with other previous schemes.

T_h : denotes the specific time of hash.

$T_{\oplus}$: denotes the specific time of XOR.

T_{Enc} : denotes the specific time of encryption.

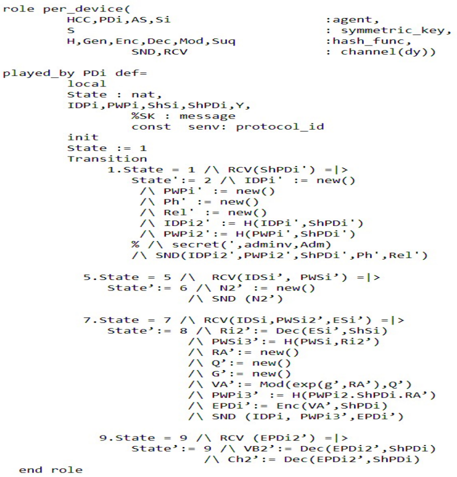
T_{Dec} : denotes the specific time of decryption.

$T_{||}$: denotes the specific time of concatenation.

Based on [22], T_h is 0.0023 ms, and $T_{\oplus} - T_{||}$ is ignored due to its negligible time. In terms of communication

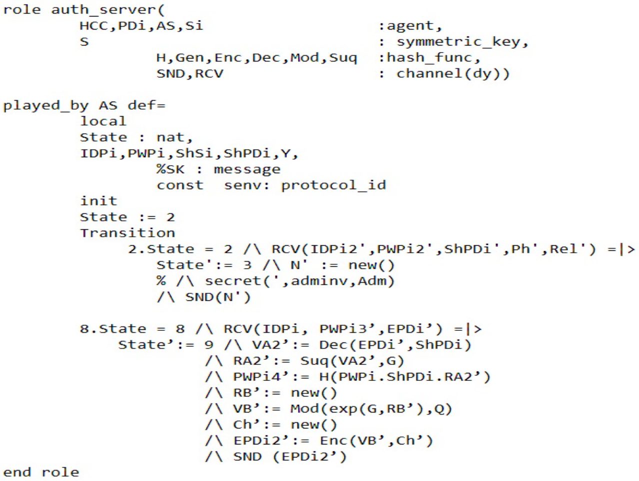
cost, the size of the identity, password, key, and hash value is assumed 128 bits for the authentication phase. The value of 32 bits is connected with the computed parameters. Each of the random numbers and timestamps has a size equal to 8 bits. The total communication cost of scheme and other similar schemes is compared in Table IV.

Table III shows the total computation cost of scheme is approximately 0.0161 ms, which is less than the cost of previous



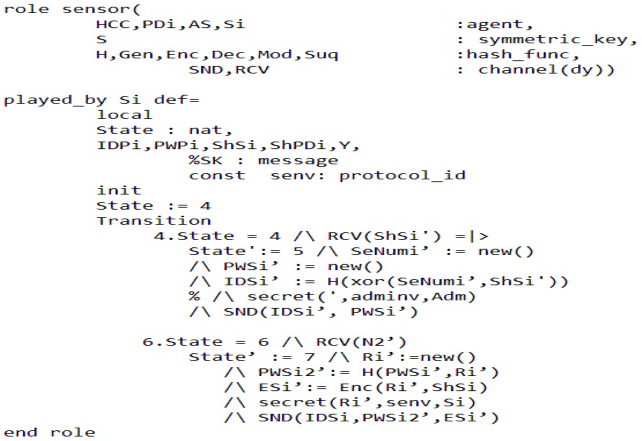
```
role per_device(
        HCC,PDi,AS,Si                            :agent,
        S                                        : symmetric_key,
        H,Gen,Enc,Dec,Mod,Suq                    :hash_func,
                SND,RCV                          : channel(dy))

played_by PDi def=
        local
        State : nat,
        IDPi,PWPi,ShSi,ShPDi,Y,
                %SK : message
                const  senv: protocol_id
        init
        State := 1
        Transition
             1.State = 1 /\ RCV(ShPDi') =|>
                State':= 2 /\ IDPi' := new()
                 /\ PWPi' := new()
                 /\ Ph' := new()
                 /\ Rel' := new()
                 /\ IDPi2' := H(IDPi',ShPDi')
                 /\ PWPi2':= H(PWPi',ShPDi')
                % /\ secret(',adminv,Adm)
                /\ SND(IDPi2',PWPi2',ShPDi',Ph',Rel')

          5.State = 5 /\  RCV(IDSi’, PWSi’) =|>
             State’:= 6 /\ N2’ := new()
                        /\ SND (N2’)

          7.State = 7 /\ RCV(IDSi,PWSi2’,ESi’) =|>
             State’:= 8 /\ Ri2’:= Dec(ESi’,ShSi)
                        /\ PWSi3’:= H(PWSi,Ri2’)
                        /\ RA’:= new()
                        /\ Q’:= new()
                        /\ G’:= new()
                        /\ VA’:= Mod(exp(g’,RA’),Q’)
                        /\ PWPi3’ := H(PWPi2.ShPDi.RA’)
                        /\ EPDi’:= Enc(VA’,ShPDi)
                        /\ SND (IDPi, PWPi3’,EPDi’)

            9.State = 9 /\ RCV (EPDi2’) =|>
                State’:= 9 /\ VB2’:= Dec(EPDi2’,ShPDi)
                          /\ Ch2’:= Dec(EPDi2’,ShPDi)
  end role
```

Fig. 6. Specification of sensor role in HLPSLL



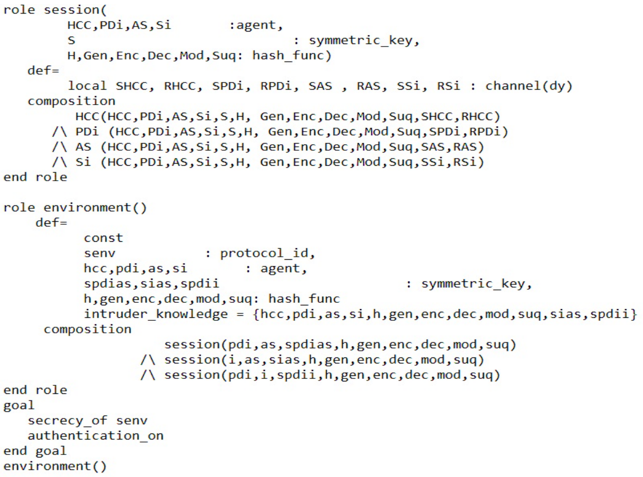
```
role auth_server(
        HCC,PDi,AS,Si                            :agent,
        S                                        : symmetric_key,
                H,Gen,Enc,Dec,Mod,Suq            :hash_func,
                SND,RCV                          : channel(dy))

played_by AS def=
        local
        State : nat,
        IDPi,PWPi,ShSi,ShPDi,Y,
                %SK : message
                const  senv: protocol_id
        init
        State := 2
        Transition
              2.State = 2 /\ RCV(IDPi2',PWPi2',ShPDi',Ph',Rel') =|>
                State':= 3 /\ N' := new()
                % /\ secret(',adminv,Adm)
                /\ SND(N')

        8.State = 8 /\ RCV(IDPi, PWPi3’,EPDi’) =|>
           State’:= 9 /\ VA2’:= Dec(EPDi’,ShPDi)
                       /\ RA2’:= Suq(VA2’,G)
                       /\ PWPi4’:= H(PWPi.ShPDi.RA2’)
                       /\ RB’:= new()
                       /\ VB’:= Mod(exp(G,RB’),Q)
                       /\ Ch’:= new()
                       /\ EPDi2’:= Enc(VB’,Ch’)
                       /\ SND (EPDi2’)
end role
```

Fig. 7. Specification of the personal device of each patient role in HLPSLL



```
role sensor(
        HCC,PDi,AS,Si                           :agent,
        S                                       : symmetric_key,
        H,Gen,Enc,Dec,Mod,Suq                   :hash_func,
                SND,RCV                         : channel(dy))

played_by Si def=
        local
        State : nat,
        IDPi,PWPi,ShSi,ShPDi,Y,
                %SK : message
                const  senv: protocol_id
        init
        State := 4
        Transition
            4.State = 4 /\ RCV(ShSi') =|>
                State':= 5 /\ SeNumi’ := new()
                /\ PWSi’ := new()
                /\ IDSi’ := H(xor(SeNumi’,ShSi’))
                % /\ secret(',adminv,Adm)
                /\ SND(IDSi’, PWSi’)

           6.State = 6 /\ RCV(N2’)
                State’ := 7 /\ Ri’:=new()
                   /\ PWSi2’:= H(PWSi’,Ri’)
                   /\ ESi’:= Enc(Ri’,ShSi)
                   /\ secret(Ri’,senv,Si)
                   /\ SND(IDSi,PWSi2’,ESi’)
end role
```

Fig. 8. Specification of authentication server role in HLPSLL



```
role session(
        HCC,PDi,AS,Si        :agent,
        S                            : symmetric_key,
        H,Gen,Enc,Dec,Mod,Suq: hash_func)
   def=
        local SHCC, RHCC, SPDi, RPDi, SAS , RAS, SSi, RSi : channel(dy)
   composition
         HCC(HCC,PDi,AS,Si,S,H, Gen,Enc,Dec,Mod,Suq,SHCC,RHCC)
      /\ PDi (HCC,PDi,AS,Si,S,H, Gen,Enc,Dec,Mod,Suq,SPDi,RPDi)
      /\ AS (HCC,PDi,AS,Si,S,H, Gen,Enc,Dec,Mod,Suq,SAS,RAS)
      /\ Si (HCC,PDi,AS,Si,S,H, Gen,Enc,Dec,Mod,Suq,SSi,RSi)
end role

role environment()
    def=
          const
          senv           : protocol_id,
          hcc,pdi,as,si        : agent,
          spdias,sias,spdii                        : symmetric_key,
          h,gen,enc,dec,mod,suq: hash_func
          intruder_knowledge = {hcc,pdi,as,si,h,gen,enc,dec,mod,suq,sias,spdii}
     composition
                     session(pdi,as,spdias,h,gen,enc,dec,mod,suq)
                  /\ session(i,as,sias,h,gen,enc,dec,mod,suq)
                  /\ session(pdi,i,spdii,h,gen,enc,dec,mod,suq)
end role
goal
   secrecy_of senv
   authentication_on
end goal
environment()
```

Fig. 9. Specification of session and environment role in HLPSL

work[13, 15, 22, 23, 24].

VI. Conclusion

In this paper, a robust, lightweight authentication scheme for WBAN, which provides additional security and is based on symmetric encryption, hash function, and key management, is proposed. Preserving the sensor’s energy is suggested. The vital signals should be divided into normal and abnormal signals so that the personal device can determine certain cases without referring to a doctor. The comparisons with related schemes show that our proposed scheme is cost effective in terms of computational and communication costs. Additionally, the scheme’s security analysis based on the AVISPA tool verifies the security of the presented scheme that can resist malicious attacks (such as MITM, replay, and eavesdropping) and supports security features such as mutual authentication and anonymous password. Each work includes a limitation. The limitation of our work is summarized by the energy efficiency enhancement of sensors as well as the quality of sensors, intersensor communication, and power efficiency of sensors. In the future, our work could be applied in different fields such as sports, where sensors can be used to measure navigation, time, distance, pulse rate, and body temperature; military, where sensors can be used for communication between soldiers and sending information about attacking, retreating, or running to their base commander; and lifestyle and entertainment, where sensors can be used in wireless music players and making video calls. There are the major limitations of authentication schemes in Wireless Body Area Networks (WBANs) and healthcare systems are scalability and complexity. As the

TABLE II.
COMPARISON OF SECURITY FEATURES

Mutual Authentication	[22]	[13]	[15]	[23]	[22]	[11]	Proposed Scheme
Anonymous Untraceable	√	√	√	×	×	√	√
Forward Secrecy	√	√	√	√	√	√	√
Unlinkability	×	√	×	√	√	√	√
Impersonal attack	×	×	√	√	√	√	√
Protected from a Stolen PD_i Attack	×	×	×	×	×	×	√
Insider Attack	×	√	√	√	√	√	√
Key Agreement and Freshness	×	×	×	√	√	√	√
MITM Attack	√	√	√	√	√	√	√
Replay Attack	√	√	√	√	√	√	√
DoS Attack DDos	×	×	×	×	√	√	√
Eavesdropping Attack	√	√	√	×	×	×	√
Forged Sensor	√	√	√	×	×	×	√
Smart Factor	×	×	×	×	×	×	×
Healthcare	×	×	×	√	√	×	√

TABLE III.
COMPARISON OF COMPUTATIONAL COST

Scheme	Registration Phase	Login and Authentication Phases	Total Cost
[22]	$2T_h$+ $1T_\oplus$	$13T_h$+$6T_\oplus$	$15T_h$+$7T_\oplus$ ≈0.0345
[13]	$1T_h$+ $2T_\oplus$+$1T_{\|\|}$	$8T_h$+$13T_\oplus$+$16T_{\|\|}$	$9T_h$+$15T_\oplus$+$17T_{\|\|}$ ≈0.0207
[14]	$2T_h$+ $6T_\oplus$	$16T_h$+$29T_\oplus$	$18T_h$+$35T_\oplus$ ≈ 0.0414
Our	$3T_h$+ $T_\oplus$	$4T_h$+$2T_\oplus$+$2T_{\|\|}$	$7T_h$+$3T_\oplus$+$2T_{\|\|}$ ≈ 0.0161

TABLE IV.
COMMUNICATION COST

Communication Link	[22]	[13]	[14]	Proposed Scheme
$S_i \rightarrow PD_i$	192 bits	200 bits	232 bits	384 bits
$PD_i \rightarrow$ AS	320 bits	328 bits	232 bits	384 bits
AS$\rightarrow PD_i$	320 bits	320 bits	192 bits	128 bits
$PD_i \rightarrow S_i$	192 bits	192 bits	192 bits	-
Total	1024 bits	1040 bits	848 bits	896 bits

number of devices and users grows, it becomes increasingly difficult to manage and maintain the authentication infrastructure. The complex is a difficult for users to understand and implement them. This can lead to a low adoption rate and a lack of trust in the system.

CONFLICT OF INTEREST

The authors have no conflict of relevant interest to this article.

REFERENCES

[1] O. Ali, M. K. Ishak, M. K. L. Bhatti, I. Khan, and K.-I. Kim, “A comprehensive review of internet of things: Technology stack, middlewares, and fog/edge computing interface,” *Sensors*, vol. 22, no. 3, p. 995, 2022.

[2] L. Babangida, T. Perumal, N. Mustapha, and R. Yaakob, “Internet of things (iot) based activity recognition strategies in smart homes: A review,” *IEEE Sensors Journal*, vol. 22, no. 9, pp. 8327–8336, 2022.

[3] V. Mohindru, S. Vashishth, and D. Bathija, “Internet of things (iot) for healthcare systems: A comprehensive survey,” *Recent Innovations in Computing: Proceedings of ICRIC 2021, Volume 1*, pp. 213–229, 2022.

[4] C. Bayılmış, M. A. Ebleme, Ü. Çavuşoğlu, K. Kücük, and A. Sevin, “A survey on communication protocols and performance evaluations for internet of things,” *Digital Communications and Networks*, vol. 8, no. 6, pp. 1094–1104, 2022.

[5] J. Iqbal, M. Adnan, Y. Khan, H. AlSalman, S. Hussain, S. S. Ullah, N. u. Amin, and A. Gumaei, “Designing a healthcare-enabled software-defined wireless body area network architecture for secure medical data and efficient diagnosis,” *Journal of Healthcare Engineering*, vol. 2022, pp. 1–19, 2022.

[6] S. M. Mousavi, A. Khademzadeh, and A. M. Rahmani, “The role of low-power wide-area network technologies in internet of things: A systematic and comprehensive review,” *International Journal of Communication Systems*, vol. 35, no. 3, p. e5036, 2022.

[7] Y. Perwej, N. Akhtar, N. Kulshrestha, and P. Mishra, “A methodical analysis of medical internet of things (miot) security and privacy in current and future trends,” *Journal of Emerging Technologies and Innovative Research*, vol. 9, no. 1, pp. d346–d371, 2022.

[8] M. Kaur *et al.*, “A review on classification of data in wban,” in *2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS)*, vol. 1, pp. 1434–1438, IEEE, 2022.

[9] A. Behura and S. Nandan Mohanty, “Application of the internet of things (iot) in biomedical engineering: Present scenario and challenges,” *Internet of Things and Its Applications*, pp. 151–169, 2022.

[10] M. Trnka, A. S. Abdelfattah, A. Shrestha, M. Coffey, and T. Cerny, “Systematic review of authentication and authorization advancements for the internet of things,” *Sensors*, vol. 22, no. 4, p. 1361, 2022.

[11] T.-Y. Wu, Q. Meng, S. Kumari, and P. Zhang, “Rotating behind security: A lightweight authentication protocol based on iot-enabled cloud computing environments,” *Sensors*, vol. 22, no. 10, p. 3858, 2022.

[12] F. Wei, P. Vijayakumar, J. Shen, R. Zhang, and L. Li, “A provably secure password-based anonymous authentication scheme for wireless body area networks,” *Computers & Electrical Engineering*, vol. 65, pp. 322–331, 2018.

[13] M. Kompara, S. H. Islam, and M. Hölbl, “A robust and efficient mutual authentication and key agreement scheme with untraceability for wbans,” *Computer networks*, vol. 148, pp. 196–213, 2019.

[14] A. M. Koya and P. Deepthi, “Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network,” *Computer Networks*, vol. 140, pp. 138–151, 2018.

[15] C. Wang, W. Zheng, S. Ji, Q. Liu, and A. Wang, “Identity-based fast authentication scheme for smart mobile devices in body area networks,” *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[16] P. Dodangeh and A. H. Jahangir, “A biometric security scheme for wireless body area networks,” *Journal of Information Security and Applications*, vol. 41, pp. 62–74, 2018.

[17] X. Liu, R. Zhang, and M. Zhao, “A robust authentication scheme with dynamic password for wireless body area networks,” *Computer Networks*, vol. 161, pp. 220–234, 2019.

[18] M. Soni and D. K. Singh, “New directions for security attacks, privacy, and malware detection in wban,” *Evolutionary Intelligence*, pp. 1–18, 2022.

[19] D. Hammood and A. Alkhayyat, “An overview of the survey/review studies in wireless body area network,” in *2020 3rd International Conference on Engineering Technology and its Applications (IICETA)*, pp. 18–23, IEEE, 2020.

[20] M. H. Alzuwaini and A. A. Yassin, “An efficient mechanism to prevent the phishing attacks.,” *Iraqi Journal for Electrical & Electronic Engineering*, vol. 17, no. 1, 2021.

[21] A. J. Mohammed and A. A. Yassin, “Efficient and flexible multi-factor authentication protocol based on fuzzy extractor of administrator’s fingerprint and smart mobile device,” *Cryptography*, vol. 3, no. 3, p. 24, 2019.

[22] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid, and V. Odelu, “Secure anonymous mutual authentication for star two-tier wireless body area networks,” *Computer methods and programs in biomedicine*, vol. 135, pp. 37–50, 2016.

[23] C. Vorakulpipat, S. Pichetjamroen, and E. Rattanalerdnusorn, “Usable comprehensive-factor authentication for a secure time attendance system,” *peerJ computer science*, vol. 7, p. e678, 2021.

[24] A. Alghamdi, “A verification system for multi-factor authentication for e-healthcare architectures,” *Arab Journal for Scientific Publishing (AJSP)*, vol. 2663, p. 5798, 2021.