INTERNATIONAL JOURNAL OF BIOLOGY AND BIOMEDICAL ENGINEERING
DOI: 10.46300/91011.2022.16.26 Volume 16, 2022

Secure and Reliable ML-based Disease Detection for a Medical Wireless Body Sensor Networks

Mbarka Belhaj Mohamed[1], Amel Meddeb-Makhlouf[2], Ahmed Fakhfakh[3], Olfa Kanoun[4]

[1]Laboratory of Signals, Systems, Artificial Intelligence and Networks (SM@RTS), Digital Research Center of Sfax (CRNS), University of Sfax, National School of Engineers of Gabes (ENIG), Tunisia
[2]New Technologies and Telecom Systems Research Unit (NTS'COM), Engineering School of Electronics and Telecommunications of Sfax (ENET'com), Sfax, Tunisia
[3]Laboratory of Signals, Systems, Artificial Intelligence and Networks (SM@RTS), Digital Research Center of Sfax (CRNS), University of Sfax, Engineering School of Electronics and Telecommunications of Sfax (ENET'com), Sfax, Tunisia
[4]Measurement and Sensor Technology, Chemnitz University of Technology, Chemnitz, Germany

Received: June 18, 2021. Revised: January 3, 2022. Accepted: January 22, 2022. Published: February 28, 2022

Abstract: **The recent development of the Internet of Things (IoT) has enabled a significant technology that aids quick healthcare solutions through the use of smart wearables sensors. Indeed, undesirable events and network threats can appear in any physiological recording in Wireless Body Sensor Networks (WBSN), leading to a misdiagnosis. These events and threats are recognizable by experienced medical staff, thereby it is necessary to identify them before making any diagnosis. In this paper, a secure and energy efficient approach is proposed. For disease detection, our research provide insight into several physiological signals, including the ElectroCardioGram (ECG), ElectroMyoGram (EMG), and Blood Pressure (BP), where the security is achieved by the application of the Advanced Encryption Symmetric (AES) and the Secure Hash Algorithm (SHA). Similarly, to obtain a reasonable range of reliability, a classification procedure based on supervised Machine Learning (ML) techniques is used. The simulation results proved the accuracy and sensitivity of the system by 97% and 92%, respectively by enhancing a high level of security. Moreover, a suitable prototype is developed for medical staff to ensure the applicability of our proposal.**

Keywords: **Data aggregation, Data reliability, Security, WBSN.**

I. INTRODUCTION

A whole condition of physical, psychological, and social well-being, rather than only the absence of disease, is defined as health. As is well known, one of the most important aspects of people's desire for a better life is their health. Regrettably, conventional health systems have established a problem for the reason of some factors, including poor health care, large inequalities between rural and urban areas, physician and nurse unavailability during the most difficult times are only a few examples.

Indeed, a large number of individuals die each year because of cancer [1], cardiovascular disease [2], hypertension, neurological disease, epilepsy [3], and a variety of deadly illnesses [4]. IoT has improved almost every area of our everyday lives and intelligent applications as a result of the growth of smart objects. Smart healthcare [5], smart homes [6], smart agriculture [7], crowd sensing [8], and crowdsourcing [9] are some of these applications.

The prevalence of chronic diseases has made a renewed request for allowing serious healthcare facilities to the persons tracking [10]. The current investigations reveal the flaws in the traditional healthcare system, implying that hospitals and clinics alone will not be able to deal with the crisis. One of the most significant advantages of wearable sensors is their ability to retrieve information partnering with physical, behavioral and psychological health. Nonetheless, a difficult challenge in WBSN is transmitting the vast amount of generated data by wearables [11]. In fact, it may have a detrimental impact on the decision-making process. To address this problem, using secure data transmission and precise prediction has recently received a lot of attention.

The following are the details for each block of this WBSN-based platform:

(1) The Intra-BSN (Fig. 1 (a)): During this phase, wearable or implanted sensors are placed on the human body under the skin. Sensors such as ElectroEncephaloGram (EEG), ECG, EMG, and BP can be used and included. Then, the detected data is wirelessly transmitted to the Local Processing Unit

(LPU) and the LPU then passes the sensed data to the part (b).

(2) The Inter-BSN (Fig. 1 (b)): During this phase, data is sent from part (a) to part (b) by one of the transmission channels. This stage's data must be passed to the next stage (c).

(3) The Beyond-BSN (Fig. 1 (c)): In this phase, the data is saved and processed in order to make a health related decision. To this goal, data may be sent to doctors or hospitals, as well as to intermediary family members. Indeed, received data should be as precise and truthful as necessary [12].

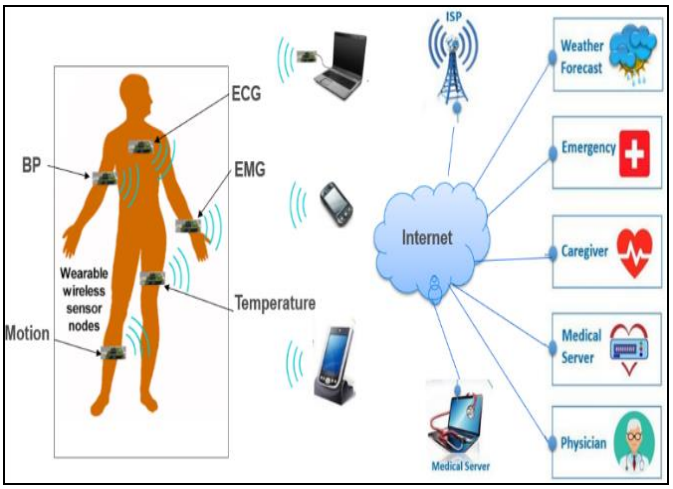

Figure 1. WBSN based platform for personal healthcare

There has been a surge in the use of WBSN-based methodologies to respond to a variety of healthcare applications. Routing [13], traffic engineering [14], resource allocation [15], anomaly detection [16], energy consumption [17] and classification [18], and other subjects are frequently discussed in WBSNs. In the IoT healthcare sector, however, there is a lack of focus on security and reliability for data analysis. Because the medical network transfers such a large amount of sensitive data, it is critical to ensure secure data transmission between patients and medical specialists. Furthermore, it is critical to evaluate the accuracy of incoming data in order to avoid unfavorable events that affect the quality of patient monitoring. To address this issue, a reasonable level of security and reliability need immediately to be enhanced.

This paper's main contribution is to increase data reliability and security communication in WBSN. To eliminate data redundancy, the proposed methodology uses the aggregation technique [19], which reduces energy harvesting and increases the transmission time of sensed data. Meanwhile, various security criteria based on the AES and the SHA are employed. Following that, a data classification procedure based on numerous supervised machine learning algorithms is evaluated to establish data reliability on the receiving side. Finally, a developed prototype is used to evaluate the results.

The remaining part of this paper is organized as follows: Some relevant works are highlighted in section 2. The proposed approach is then described in detail in section 3. Section 4 discusses the experiments and their outcomes. In Section 5, the main conclusions are drawn.

II. Related Work

One of the key concerns of the WBSN is the safe and secure transfer of medical sensitive information to the intended destination. Many strategies have been proposed in the past to ensure secure data aggregation transmission. The proposed technique in [20] goes through various Privacy-Preserving Data Aggregation (PPDA) methods used in Wireless Sensor Networks (WSN) and IoT. The goal is to provide a better WBSN-specific privacy preserving data aggregation scheme. Because the WBSN is a specific sort of WSN, the proposed scheme keeps basic criteria such as data redundancy and the role of individual sensors.

The article [21] describes a novel data aggregation strategy for reducing network traffic and energy usage in WSN. The Extreme Learning Machine (ELM) is used in the proposed technique to efficiently fuse data at the cluster head before transmission to the sink. The Mahalanobis Distance-based Redial Basis Function (MDRBF) is utilized to set the model's parameters after the data filtering and clustering procedure, ensuring data processing. In fact, network traffic could be significantly reduced, extending the network's lifetime. The obtained results show that the proposed approach achieves data accuracy of 79% and energy efficiency of 80%.

For monitoring cardiovascular diseases, existing solutions record data through multiple channels at a high sampling rate, which results in the generation of a considerable amount of data. Thereby, it consumes a lot of energy and necessitates a lot of storage space. The study in [22] introduces a real-time encoding technique for ECG signals in this context. The approach is based on iterative thresholding and a wavelet coefficient approximation. The goal is to condense bio-signals while maintaining their essential characteristics. The results of a real-time-based IoT platform show a system-level energy rise of 96% with a 2% influence on signal quality.

Regardless of the options available for setting up a telemonitoring approach, the WBSN process is influenced by three major factors: Latency, energy usage, and reliability. The research presented in [23] tries to address these issues by employing a Time Division Multiple Access (TDMA) analysis technique that sends data at distinct time slots and removes unnecessary sensitive data. With a lower latency (0.635 ms) and lower power consumption, this approach was able to achieve a tolerable range of accuracy (31.5 %).

WBSNs have gained popularity as a result of recent developments in the IoT and remote health monitoring (eHealth) applications. The wide range of applications such as healthcare, military, entertainment, and so on highlights the need for more adaptable architectures and protocols. New Medium Access Control protocols (MACs), including as Bluetooth, IEEE 802.15.4, and IEEE 802.15.6 [24], have been proposed in this context to suit the Quality of Service (QoS)

criteria of WBSN architecture. The numerical findings demonstrate that the proposed approach outperforms the existing works by 21% in latency and 67% in energy consumption.

Recent research has put a lot of effort on adapting the sample rate of sensors in wireless sensor networks. For health monitoring in WBSNs, the paper [25] proposes the Adaptive Rate Energy-saving Data Collecting Technique (AREDaCoT). It consists of two stages: Local emergency detection (by reducing data redundancy and adjusting the sample rate) and global emergency detection (by removing data redundancy and adjusting the sampling rate). In fact, the obtained results show how AREDaCoT reduces the volume of data collected, resulting in a large energy saving (76%) while maintaining data correctness (70%) and integrity.

To the best of the authors' knowledge, most of the proposed solutions only deal with a single type of bio signals. They do not take into consideration sensors that are implanted in the legs, hands, fingers, brain or in any other body part. In case of need, the implanted sensor would be better able to detect internal body functioning for more accurate health analysis. To overcome these limitations, we proposed an accurate disease detection approach for medical WSNs based on three multivariate physiological signals. A developed prototype is designed, which is based on a data aggregation model for energy, reliability and security enhancement.

III. The Proposed Data Transmission Methodology

The main purpose of this research was to provide a secure and reliable data transmission mechanism for WBSN. As shown in Fig. 2, the suggested methodology is comprised of multiple steps. Each of the processes was thoroughly detailed in the subsections below

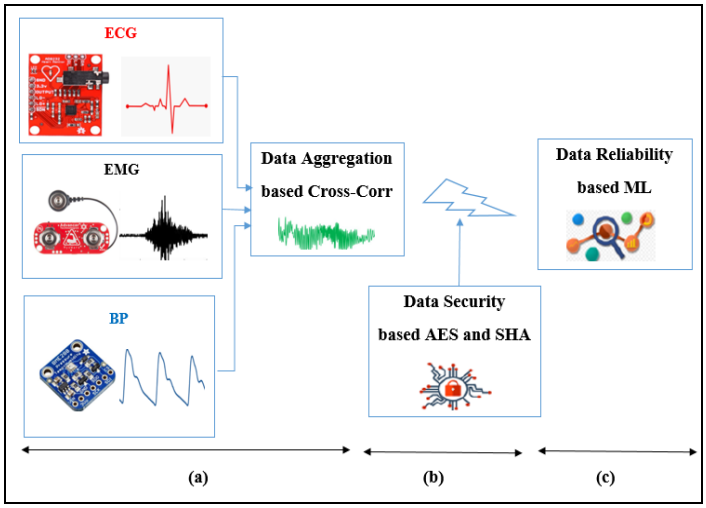

Figure 2. The proposed flowchart

The health condition of patients is supervised in WBSN via a set of tiny-powered sensor nodes that are subject to energy exploitation. According to various studies, retransmission processes are one of the main cause of resource exploitation in WBSN. In fact, channel fading causes a data collision and data loss. To address this problem, data aggregation strategies are being investigated. Furthermore, data reduction extends the network lifetime by maximizing the sensor nodes' resource utilization. Even, it is likely to decrease some service quality measures, such as data privacy and accuracy.

A. $Cross_{Corr}$ -based data aggregation

According to the literature, there is a lot of interest in resolving energy consumption issues in the medical profession. Several proposed strategies, including as radio scheduling, control packet elimination, topology control, and data aggregation, are examined for this purpose. Data aggregation is one of the most well-proven solutions. It's worth remembering that sensor data contains noise, which reduces WBSN performance by a large amount of redundancy due to spatial and temporal correlations of the data. Thus, deleting these duplicated data is a necessary step in significantly reducing energy exploitation. The detected sensor readings are aggregated under the condition that a data aggregation technique is used.

This paper introduces a useful aggregation technique. This strategy takes advantage of temporal and spatial correlations to achieve its goal. As aggregation functions, several mathematical equations such as Average, Max, Min, Sum, Count, Median, and Cross-Correlation are used. A cross-correlation function (equation (1)) based on three multivariate physiological signals is used.

$$Corr_k = \frac{\sum_{i=1}^{N}((X_i)(Y_{i+k}))}{\sqrt{\sum_{i=1}^{N}(X_i)^2 \sum_{i=1}^{N}(Y_{i+k})^2}} \quad (1)$$

The proposed data aggregation technique's simulation results are shown in Fig. 3 below. The cross-correlation function between the ECG (Fig. 3 (a)) and the BP (Fig. 3 (b)) signals is used to compress data. The received data (Fig. 3 (d)) is then correlated with the EMG signal (Fig. 3 (c)), yielding fused data as observed in (Fig. 3 (e)) below. For example, when a sensor node is used to monitor heart rate on a patient (Fig. 3 (a)), the recorded values quickly become stable after 30 minutes or even an hour. Furthermore, if two additional sensor nodes are used for the same patient to monitor muscular activity (Fig. 3 (b)) or BP variation (Fig. 3 (c)), then the data collected by one node is often similar to neighboring node.

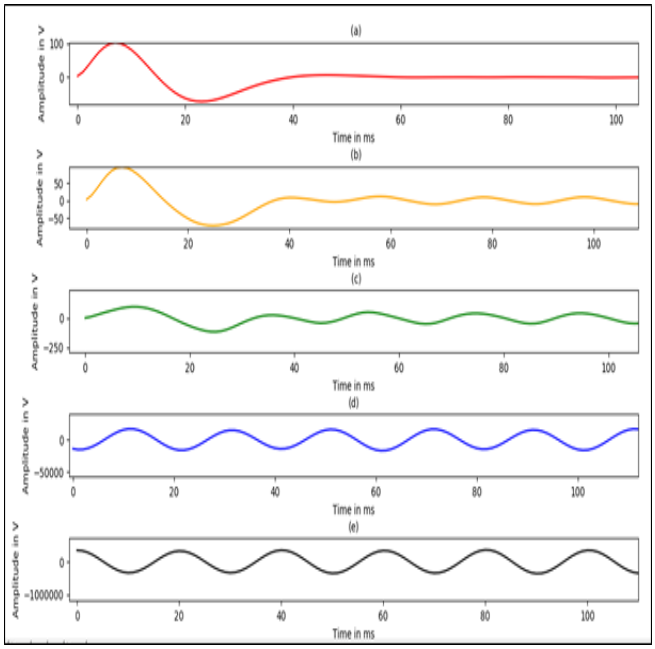

Figure 3. Data aggregation process: (a): Filtered ECG, (b): Filtered BP, (c): Filtered EMG, (d): Cross-Correlation (a)*(b), (e): Aggregated data

B. AES and SHA-based data security

Because wireless communications are sensitive, medical information are impacted by a variety of network threats and attacks. It is critical to establish a secure link between sensor nodes in this regard. Indeed, the security is achieved by verifying data authenticity. This means that data must be well-preserved in order to ensure that secret data is not falsified at the receiver's end and that data is delivered securely to the authorized entity.

These techniques are implemented utilizing the most secure AES [26] and SHA [27] algorithms for data encryption and authentication. The total security level was improved in this area while maintaining the core network criteria. The proposed secure algorithm presented in Fig. 4 contains four phases: Registration, Aggregation, Encryption, and Verification.

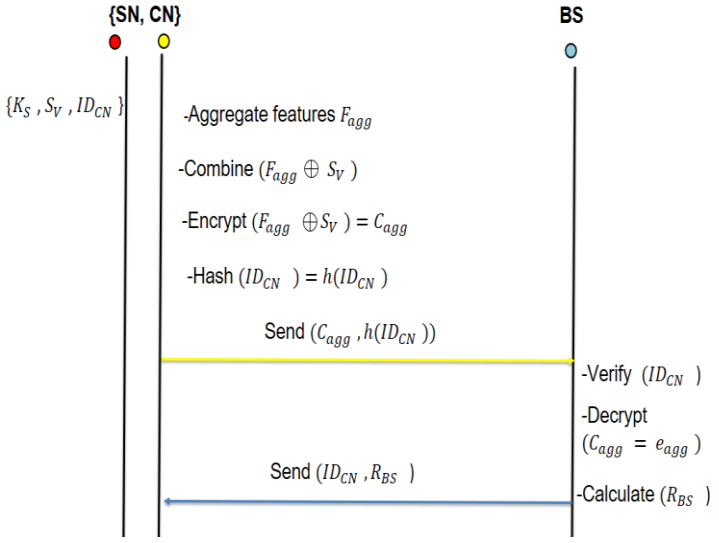

Figure 4. Proposed AES and SHA algorithm

During the registration phase, the process is designed to prompt and save a few key personal details. A secret key K_S is communicated between the Sensor Node (SN), the Control Node (CN), and the Base Station (BS). The observed sensed value, S_v, is wirelessly sent to the neighboring CN. Each CN has its own unique identifier, ID_{CN}, to prevent identity takeover. Following that, all of the data is sent to the BS.

The CN integrates the received extracted features into a single unit named F_{agg} during the aggregation phase. The features are then XORed after being regrouped using a sum transaction modulo S_v. The S_v and F_{agg} outputs of this operation are forwarded to the BS.

To improve data confidentiality during the encryption phase, the AES algorithm was proposed. To the best of knowledge, the AES is the most extensively utilized algorithm because to the several benefits it provides over other algorithms.

In step 3, the CN encrypts the combined F_{agg} and S_v to produce the cipher text C_{agg} determined in (2). It could be read by anyone who has access to the K_S sharing secret key.

$$Ciphertext_j^r = \text{Encrypt}\left((Agg_j^r, r), h(Agg_j^r, K_j)\right) \quad (2)$$

Where:

- $\mathbf{Agg_j^r}$: Aggregated sensed data by SNj at round r,
- $\mathbf{h(Agg_j^r, K_j)}$: hash function of compressed sensed data using K_j.

An updated key is required because of the human body's mobility. Equation (3) was used to perform an XOR binary operation between the hash values and the secret key.

$$K_j^r = K_j^{r-1} \oplus h\left(Agg_j^r\right), r = 1,2,3 \ldots. \quad (3)$$

The SHA is used to safeguard the CN's identity. The calculated results (ID_{CN}, C_{agg}) are then sent to the backend server. The BS must justify the data confidentiality and integrity of all senders during the verification process. When it receives the packet carrying the identification of the control node ID_{CN}, it checks it as a first step. The BS then decrypts the Cipher text C_{agg} and examines the plaintext e_{agg} received in the second phase. If the verification is successful, the BS believes this information to be from CN, and the data integrity is assured (e_{agg} is accepted). Finally, the BS sends to the CN a response R_{BS} containing the monitored patient's diagnostic.

C. ML-based data reliability

WBSNs should be able to transfer a large amount of data in a short amount of time to guarantee continuous healthcare monitoring. In order to detect harmful situations or death causes in patients, data must be obtained correctly, and hence reliability must be disposable.

Actual data prediction using Machine Learning (ML) algorithms has been a rising topic in artificial intelligence. ML algorithms are useful for data analysis, but experiments demonstrate that when a large amount of data is utilized for training and testing, reduces their performance [28]. A data classification technique for the obtained aggregated data (387*24) is used to avoid these flaws. The Support Vector Machine (SVM), K-Nearest Neighbors (K-NN), Random Forest (RF), Decision Tree (DT), Logistic Regression (LR), Gradient Boost (GB), and Naive Bayes (NB) algorithms are used in this procedure [29].

The training data set is downloaded in the first step from the "Kaggle" website (www.kaggle.com**)**, which provides powerful tools and resources. The total data classification in this case is based on the relevant features for each investigated signal, such as age, sex, height, weight, QRS, QRS duration, PR interval, QT interval, T interval, Heart Rate, Standard Deviation, Root Mean Square, Min, Max, Zero Crossing, Systolic and Diastolic.

Figure. 5 shows an ECG with seven different types of arrhythmias. A significant probability of above 64.8% is discovered as normal situation. As previously stated, this study is focused on a number of associated ECG illnesses. Indeed, 11.6% of the patients under observation may suffer ischemic alterations. This problem refers to a problem involving the brain's tiny blood vessels.

Furthermore, a myocardial infarction induced by irreversible heart muscle necrosis is noted. A reduction in blood flow to the heart owing to coronary artery obstruction causes this infraction. Thereby, two distinct types of myocardial infarction are discovered for both old anterior and inferior myocardial infarctions, with a lower probability equal to (4%). In addition, the cardiac rhythms tachycardia and bradycardia are known. The first occurs when the heart rate exceeds 100 BPM, while the second occurs when the sinus node emits an electrical charge at a slower rate than typical (60-100 BPM). Finally, (5.6%) represents the remaining probability, which is reserved for other diseases.

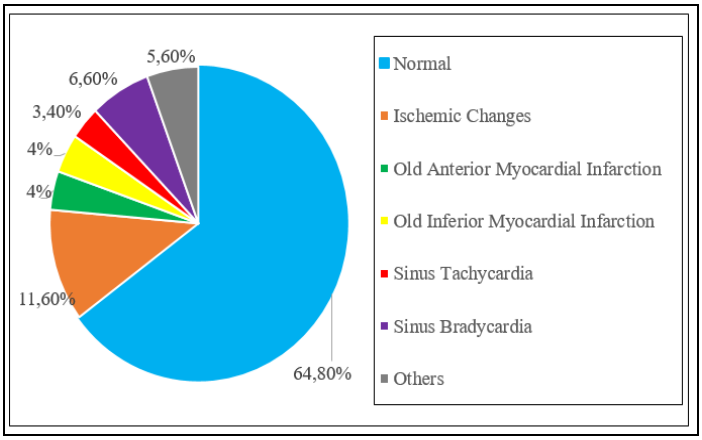

Figure 5. ECG diseases identification

The BP has been shown to be an important determinant in human health status in prior research. The numerous illnesses are characterized by unusually high BP on the artery lining, with four important outputs (see Fig. 6). To begin with, only 33.3% of the training data set represents a typical case. However, a highest detection probability (until 40%) of a prehypertension is detected, but also, two different hypertension stages with a detection ranges between 17% and 10% respectively. Hence, lifestyle have a strong effect in the health status of the persons. Under stress or during physical effort, for example, is one of the primary causes of hypertension.

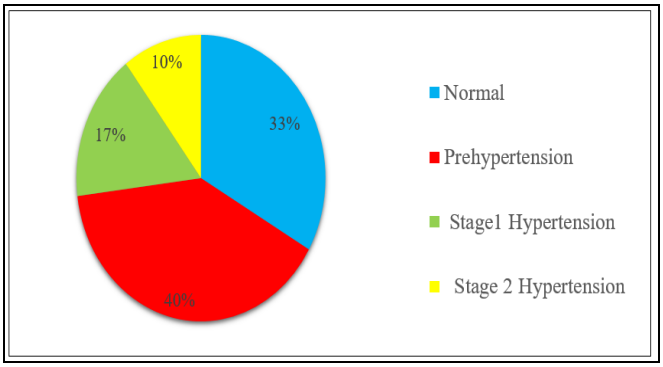

Figure 6. BP diseases identification

Likewise, the same procedure is used to determine whether or not a muscle contraction is conceivable. As previously indicated, two forms of EMG classification are investigated. Indeed, until 84.9% of contractions are produced by coordinated muscle cell problems, the highest probability is reached. However, the reset condition (normal state) is only referenced 15.1% of the time. Hence, these probabilities reveal the impact of cardiovascular and hypertensive problems on the observed patient's muscle activity.

IV. Real Experimentation

To prove the feasibility of our approach, we propose in this section a hardware implementation of our secure classifier. Indeed, it is necessary to consider CPU power, computing steps and memory in the overall energy balance phase.

A. System design

The main purpose of this paper is to provide continuous healthcare monitoring. For that, the proposed method is divided into three stages: (1) Data collection, (2) Data preprocessing, and (3) Data storage and diagnosis. Wearable sensors are used in the first stage to collect data from the patient's body, where three physiological signals, including ECG, EMG, and BP, are gathered. After that, the sensors are connected to an ESP32 processor unit. The Raspberry Pi 3 receives sensor data and transfers it via GPIO pins, where the proposed aggregation technique is used. The resulting fused data is forwarded to the web server. Open Signals is used for the graphical interpretation and display of collected findings on the online user interface. The HTML protocol allows a Wi-Fi module and a web server to communicate easily. The HTML user interface is updated every 20 s to ensure real-time patient tracking.

Figure. 7 shows the designed platform. To collect data, all wearable sensors are placed on the patient's body. The sensors are connected to an ESP32 processor unit. It serves as the system's core by connecting these (heartbeat, muscle, and blood pressure) sensors. The ESP32 collects sensor data before sending it to the Raspberry Pi 3. Following that, the sensor output is connected to the IoT website. The medical data is then accessible via any supported device. The data is graphically exposed via a secure connection, which requires a password. Following the verification of authentication, the previously proposed secure technique is used to ensure data privacy.

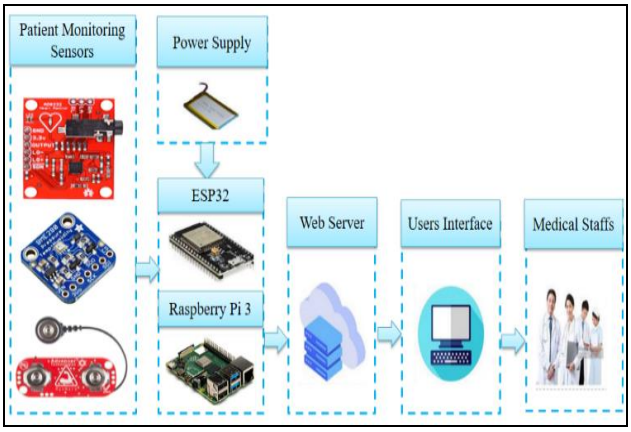

Figure 7. Proposed healthcare monitoring architecture

B. Implementation details

For a better understanding, the system is built around the association of the previously described hardware and software components, as shown in Fig. 8. Physical pins connect the ECG, EMG, and BP sensors to the ESP32. Because it features a built-in wifi module, the ESP32 is employed as a processing device. The ECG sensor's output pin is attached to the ESP32's D34 pin for a single patient. Myoware's data pin is represented by the microcontroller's D25 pin (ESP32). The data pin of the BME280 is connected to the ESP32's D1 for blood pressure variation.

The Lolin32 is connected to a Raspberry Pi via USB connection in the second stage. However, it is vital to double check that the ESP32 module uses a serial connection, which is really simple to set up. The RX pin on the Pi, GPIO 15, is connected to the TX pin on the ESP32. The ESP32's RX pin is connected to the Pi's TX pin, GPIO 14. The ESP32's Vin and grounds are connected to a 5 V pin on the Pi. As a result, use caution while working with 5 V lines, as the GPIO pins can only take 3.3 V and are subject to damage at higher voltages. The proposed prototype is shown in Fig. 8, which shows how the system is evaluated with just one user. Indeed, ECG electrodes are placed on the user's heart, and EMG (Myoware) and BP (BME280) sensors are placed on one user's hand. The web server receives all of the sensed data for additional analysis.

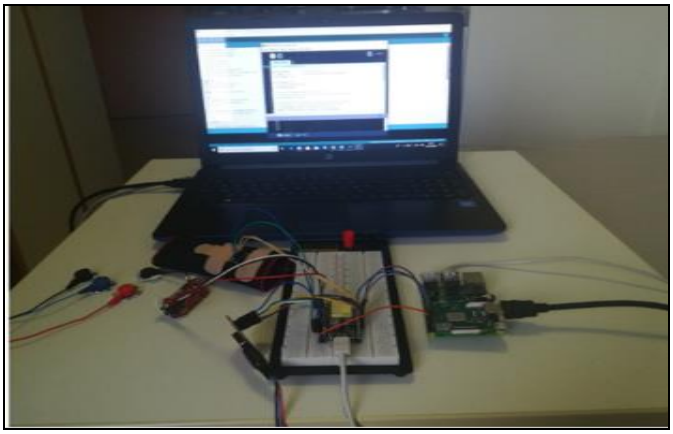

Figure 8. Overall architecture of healthcare monitoring systems

V. Evaluation of the Obtained Results from the Real Prototype

This section evaluates the suggested prototype's performance in terms of security, reliability, and energy reduction.

A. Achieved security requirements

The proposed security approaches prove four key features:

Data Authentication: This service verifies that sensor nodes, control nodes, and the base station are all authenticated before allowing access or disclosing any data.

Data Privacy: This service prevents control node identities from being usurped ID_{CN}. The hash function is applied to the node identity to achieve this.

Data Confidentiality: The security system ensures that personal health information sent over the internet is only seen by the intended recipients. The usage of AES ensures that the information is kept private.

Data Integrity: Integrity is ensured by a predetermined Hash function $h(Agg_j^r, K_j)$, which is calculated and appended to each piece of data, demonstrating its originality. The Hash is calculated with a private key that only the source knows about.

B. Achieved reliability improvement

It is required to justify the impact of the proposed aggregation and security procedures on data reliability after they have been implemented. However, in our work, decision-making is based on various supervised machine learning algorithms. To do this, a suitable classification model is used on the reception side to verify whether the data was received correctly.

When learning algorithms are utilized, there are a few key metrics that must be represented properly based on the mathematical expressions of accuracy (4) and sensitivity (5). Tables 1 and 2 show the final results for each training model.

$$\text{Accuracy}_{\text{Score}}(\%) = \frac{TP+TN}{TP+FP+TN+FN} \quad (4)$$

$$\text{Sensitivity}_{\text{Score}}(\%) = \frac{TP}{TP+FP} \quad (5)$$

Where:

- **TP:** True Positive, prediction is positive and patient is with disease,
- **FP:** False Positive, prediction is positive and patient is healthy,
- **TN:** True Negative, prediction is negative and patient is healthy,
- **FN:** False Negative, prediction is negative and patient is with disease.

Table 1. Accuracy score for each model

Model name	ECG	BP	EMG
RF	0.7631	1.0000	0.9736
SVM	0.7368	0.9605	0.9473
LR	0.7105	0.8157	0.9342
DT	0.6973	1.0000	0.9605
KNN	0.6842	0.9342	0.9605
GB	0.6842	1.0000	0.9736
NB	0.5789	0.9078	0.9342

Table 2. Sensitivity score for each model

Model name	Sensitivity
RF	0.9122
SVM	0.8859
LR	0.8596
DT	0.8859
KNN	0.8815
GB	0.8201
NB	0.8069

According to this research, the Random Forest (RF) outperforms the Support Vector Machine (SVM), Logic Regression (LR), Decision Tree (DT), k-Nearest Neighbors (KNN), Gradient Boost (GB), and Naive Bayes (NB) in terms of accuracy (76%, 97% and 100% for ECG, EMG, and BP, respectively) and sensitivity (91.22%) (see Table 2). Furthermore, the GB algorithm achieves a high accuracy score of 97.36%, especially when it comes to the classification of EMG signals. DT and GB have been shown to be good classifiers for the BP signal (until 100%).

The SVM, DT, and KNN algorithms, on the other hand, achieve a high sensitivity of up to 88%. Thus, these numerical findings show that the fused decision obtained was accurate. As a result of the aggregation operation, data redundancy is eliminated, and signal quality at the receiving end is unchanged. This indicates that the decision-making signal/output can be replicated.

C. Evaluation of the energy consumption

The energy consumption is a significant challenge in WBSNs. An energy model has been utilized to calculate the energy required by sensor nodes based on numerous previous research efforts.

A measurement technique in terms of exploited Voltage (V) and Intensity (I) of each component for further justification. The sensing process consumes a lower voltage and intensity in the region of (1.5V and 0.05A). This reduction demonstrates the effectiveness of the chosen wearable sensors. Furthermore, a significant amount of resource is set aside for the treatment process using both the ESP32 and Rasp Pi 3 microcontrollers (3.3V and 0.06A). These variables are used to determine total spent energy, which is the sum of all energy amounts in a variety of scenarios, as explained in (6):

$$E_{total} = \sum_i E_{TX} \quad (6)$$

With:

$$E_{TX} = V * I_{Tx} * \Delta_{TX} \quad (7)$$

Where:

- E_{TX}**:** Energy consumption in one iteration (J),
- V: Supply Voltage (V),
- I_{Tx}: Current consumption (A),
- Δ_{TX} : State duration (s),
- E_i : Energy in each state (J),
- E_{total} : Total consumed energy (J).

The energy consumption for each node is calculated. In fact, the nodes in the real scenario attained a numerical value of 2.912 mJ. This efficiency demonstrates the proper proposed hardware platform in one part and the suggested data aggregation process in the other part, which reduces resource usage.

Our goal of eliminating data redundancy is well achieved with this strategy. The low energy usage ensures data security and reliability. To demonstrate the system efficiency, the findings were compared to other proposed systems from literature (see Table 3).

Table 3. Comparative results

Related works	Energy (%)	Accuracy(%)

[21], 2020	80	79
[22], 2020	96	92
[23], 2020	50	31.5
[24], 2020	67	62
[25], 2020	76	70
Proposed approach,	87.32	80.53

In terms of energy saving, the proposed approach outperforms the Extreme Learning Machine [21], Enhanced Reliability, Energy-Efficient and Latency (EREEAL) algorithm [23], IEEE 802.15.6 [24], and AREDaCoT [25] algorithms by up to 87.32%. Using a single type of medical signal (ECG), the ERREEAL algorithm [22] achieves a crucial energy reduction (96%) and a high accuracy score over 92%. This study, on the other hand, is based on three multivariate signals. This demonstrates the effectiveness of the suggested aggregating method. Furthermore, AREDaCoT verifies that data accuracy is greater than 70%. The proposed approach is marginally more accurate (80.53%) than [21] (79%), [23] (31.5%), [24] (62%) and [25] (70%). The numerical results show that energy is saved with greater precision than previous methods.

VI. Conclusion

Technology advancements and healthcare devices provide a wide range of services in IoT applications. Although certain innovations in this field are exhaustive, they should be widely adopted due to concerns about data security and privacy.

The emission of compromised data not only wastes time but also lowers the performance of the data aggregation technique. Furthermore, due to the resource constraints of IoT devices, traditional security solutions are not a viable option. Developing a lightweight and energy efficient data aggregation algorithms that are not only secure but also reliable is an essential topic that needs to be looked.

A secure and reliable approach for multiple health signals is provided in this paper. To evaluate decision making on the receiving side, the suggested method necessitates the use of numerous supervised machine learning algorithms. However, an effective data aggregation procedure was performed to lower the energy consumed. The required results reveal the Random Forest algorithm's efficiency in terms of accuracy (97%) and sensitivity (92%) with a high level of security and low energy consumption.

Furthermore, a real implementation of the Random Forest classifier and security algorithms in WBSN is a future research path.

Acknowledgement

This research framework is within a collaboration between the National School of Engineering of Gabes, the Digital Research Center of Sfax (CRNS), Tunisia and Chemnitz University of Technology, Germany. The authors would like to thank DAAD for the support of the joint cooperation. They draw up many thanks to the European exchange program for supporting their work.

References

[1] M. M. Islam, H. Iqbal, M. R. Haque and M. K. Hasan, "Prediction of breast cancer using support vector machine and K-nearest neighbors," IEEE Region 10 humanitarian technology conference (R10-HTC), p. 226-9, 2017.

[2] M. B. Mohamed, A. M. Makhlouf and A. Fakhfakh, "Correlation for efficient anomaly detection in medical environment," *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2018, pp. 548-553, doi: 10.1109/IWCMC.2018.8450283.

[3] A. Djemal, D. Bouchaala, A. Fakhfakh and O. Kanoun, "Tonic-myoclonic epileptic seizure classification based on surface electromyography," 18th International Multi-Conference on Systems, Signals & Devices (SSD), 2021, pp. 421-426, doi: 10.1109/SSD52085.2021.9429401, 2021.

[4] S. Islam Ayon and Md. Milon Islam, "Diabetes prediction: a deep learning approach," Int J Inf Eng Electron Bus. 2019; 11:217. https :// doi.org/10.5815/ijiee b.2019.02.03, 2019.

[5] P. Kumar and L. Chouhan, "A secure authentication scheme for IoT application in smart home," Peer-to-Peer Netw. Appl. 14, 420-438, https://doi.org/10.1007/s12083-020-00973-8, 2021.

[6] M.M. Islam, A. Rahaman and M.R. Islam, Development of smart healthcare monitoring system in IoT environment," SN Computer Science, https://doi.org/10.1007/s42979-020-00195-y, 2020.

[7] K. Haseeb, I. Ud Din, A. Almogren and N. Islam, "An energy efficient and secure IoT-based WSN framework: an application to smart agriculture," Sensors, 20, 2081, https://doi.org/10.3390/s20072081, 2020.

[8] Y. Ren, T. Wang, S. Zhang. et al, "An intelligent big data collection technology based on micro mobile data centers for crowd sensing vehicular sensor network," Pers Ubiquit Comput (2020), https://doi.org/10.1007/s00779-020-01440-0, 2020.

[9] Y. Yu, L. Guo, S. Liu, J. Zheng and H. Wang, "Privacy protection scheme based on CP-ABE in crowd sourcing-IoT for smart ocean," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10061-10071, doi: 10.1109/JIOT.2020.2989476, Oct. 2020.

[10] J.J. Jijesh, Shivashankar and Keshavamurthy, "A supervised learning based decision support system for multi-sensor healthcare data from wireless body sensor networks, " Wireless Pers Commun 116, 1795{1813, https://doi.org/10.1007/s11277- 020-07762-9, 2021.

[11] A. Alsiddiky, W. Awwad, K. bakarman, H. Fouad, A. S. Hassanein and A. M. Soliman, "Priority-based data transmission using selective decision modes in wearable sensor based healthcare applications," Computer Communications, Volume 160, Pages 43-51, ISSN0140-3664, https://doi.org/10.1016/j.comcom.2020.05.039, 2020.

[12] S. G. Mavinkattimath, R. Khanai and D.A. Torse, "A survey on secured wireless body sensor networks,"

International Conference on Communication and Signal Processing, April 4-6, 2019.

[13] T. Rashid, S. Kumar, A. Verma et al. "Co-REERP: cooperative reliable and energy efficient routing protocol for intra body sensor network (Intra-wbsn)," Wireless Pers Commun 114, 927–948, https://doi.org/10.1007/s11277-020-07401-3, 2020.

[14] S. Murtaza Rashid Al Masud, M. ul Hassan, Kh. Mahmood and M. Akram, "An M/M/1 preemptive queue based priority mac protocol for wbsn to transmit pilgrims' data," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 10, 2020.

[15] N. Badri, L. Nasraoui, L. A. Saidane and N. Brinis, "Auction-based time resource allocation for energy harvesting wban," International Wireless Communications and Mobile Computing (IWCMC), pp. 764-769, doi: 10.1109/IWCMC48107.2020.9148274, 2020.

[16] M. B. Mohamed, A. Meddeb-Makhlouf and A. Fakhfakh, "Intrusion cancellation for anomaly detection in healthcare applications," *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2019, pp. 313-318, doi: 10.1109/IWCMC.2019.8766592.

[17] N. Zahid, A. H. Sodhro, M. S. Al-Rakhami, L. Wang, A. Gumaei and S. Pirbhulal, "An adaptive energy optimization mechanism for decentralized smart healthcare applications," IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), pp. 1-5, doi: 10.1109/VTC2021-Spring51267.2021.9448673, 2021.

[18] W. Li, Y. Chai, F. Khan et al., "A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system," Mobile Netw Appl 26, 234-252, https://doi.org/10.1007/s11036-020-01700-6, 2021.

[19] A. Dehkordi, S. Farajzadeh, K. Rezazadeh, J. et al., "A survey on data aggregation techniques in IoT sensor networks," Wireless Netw 26, 1243{1263, https://doi.org/10.1007/s11276-019-02142-z, 2020.

[20] K. Kishan Sehra and M. Dave, "Privacy preserving data aggregation in wireless body sensor network," International Conference on IoT, Social, Mobile, Analytics Cloud in Computational Vision Bio-Engineering (ISMAC-CVB 2020), Available at SSRN: https://ssrn.com/abstract=3734802 or http://dx.doi.org/10.2139/ssrn.3734802, November 21, 2020.

[21] I. Ullah and H. Y. Youn, "Efficient data aggregation with node clustering and extreme learning machine for WSN," Journal of Supercomputing, 76:10009{10035, https://doi.org/10.1007/s11227-020-03236-8, 2020.

[22] A. Ghosh, A. Raha and A. Mukherjee, "Energy efficient IoT-health monitoring system using approximate computing," Internet of Things, Volume 9, 100166, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2020.100166, 2020.

[23] R. Anirudh Reddy and N. V. Ram, "Data aggregation and precedence by delay sensitivity (DAP-DS): data transmission over wireless body sensor networks," Microprocessors and Microsystems, Volume 77, 103165, ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2020.103165, 2020.

[24] A. S. H. Altamimi, O. R. K. Al-Dulaimi, A. A. Mahawish, M. M. Hashim and M. S. Taha, "Power minimization of WBSN using adaptive routing protocol," Indonesian Journal of Electrical Engineering and Computer Science, Vol. 19, No. 2, pp. 837 846, ISSN: 2502-4752, DOI: 10.11591/ijeecs. v19.i2. pp837-846, August 2020.

[25] A. S. Jaber and A. K. Idrees, "Adaptive rate energy-saving data collecting technique for health monitoring in wireless body sensor networks," International Journal of Communication systems, Volume33, Issue17 https://doi.org/10.1002/dac.4589, 21 August 2020.

[26] G. Shanmugavadivel, B. Gomathy and S. M. Ramesh, " An enhanced data security and task flow scheduling in cloud-enabled wireless body area network," Wireless Pers Commun, https://doi.org/10.1007/s11277-021-08493-1, 2021.

[27] B. Khadem, A. M. Suteh, M. Ahmad, A. Alkhayyat, M. S. Farash and H. S. Khalifa, "An improved wbsn key-agreement protocol based on static parameters and hash functions," in IEEE Access, vol. 9, pp. 78463-78473, 2021, doi: 10.1109/ACCESS.2021.3083708.

[28] M. B. Mohamed, A. Meddeb-Makhlouf, A. Fakhfakh and O. Kanoun, "Intrusion detection based on correlation of multiple health signals in wbsn," 2020 17th International Multi-Conference on Systems, Signals & Devices (SSD), 2020, pp. 372-377, doi: 10.1109/SSD49366.2020.9364227, 2020.

[29] M. B. Mohamed, A. Meddeb-Makhlouf, A. Fakhfakh and O. Kanoun, (2021), "Wireless body sensor networks with enhanced reliability by data aggregation based on machine learning algorithms," 10.1007/978-3-030-71225-9_4, 2021.

Mbarka Belhaj Mohamed is PhD student in electrical engineering at National School of Engineers Gabes (***ENIG***), Tunisia. She received the Master degree in communications (in 2015), and from the High School of Engineering in Electronics and Communications (***ENET'com***). Their master project presented and published at the 2016 IEEE Global Communications Conference in Washington DC. She is member of the Laboratory of signals, systems, artificial intelligence and networks (***SM@RTS***), in the digital research center of Sfax (***CRNS***). In her research, she focuses on wireless sensor networks; healthcare applications; medical signal processing; decision making; network security; sensors and energy harvesting. She is author in a lot of international conferences. In 2020, she had the best paper

award in the international multi-conference on systems, signals and devices (SSD). She has a very rich experience in higher education: In 2017, she works as a temporary teacher at ***ESPin Sfax*** ; and in 2018 at ***ESIP Gafsa***, (course: network and security). Then, she works as a contractual teacher in telecommunication at ***ISSAT Kasserine***; and at ***SUPtech Sousse***, in 2020, 2021 and 2022 respectively. Also, she works as a temporary teacher at ***ISSAT Sousse***; and ***ESSTHS Sousse*** in 2021 and 2022. She was a supervisor more than 8 end of studies project in fields of telecommunication, network security, signal preprocessing and smart health. These experiences enrich their knowledge in various technological domain.

Amel Meddeb-Makhlouf is currently a Post-Doctoral Fellow at the High School of Engineering in Electronics and Communications (***ENET'com***), Sfax, Tunisia. She received the engineering degree (in 2001), the Master degree in communications (in 2003), and the Ph.D. degree (2010) from the Engineering School of Communications (***SUP'COM***, Tunisia). From September 2001 to August 2004, she worked as a project chief of the certification unit in NDCA (National Digital Certification Authority), the root certification authority in Tunisia, where she participates to the establishment of the Tunisian public key infrastructure. She also collaborates in the security audit projects. From September 2004 to September 2010, she worked as a teacher assistant in telecommunications in the Engineering School of Communications (***SUP'COM***, TUNISIA), where she teaches security courses and supervised Engineer projects. Since September 2010, she work as an assistant professor in the Engineering School of Electronics and Telecommunications of Sfax (***ENET'com***), where she supervised more than 40 projects. She is a member of ***NTS'COM*** Laboratory in ***ENET'com***. He was a supervisor of more than 20 master projects and 9 PH.D thesis in fields of security of cloud computing, security of body sensor networks, security of 5G networks and the security of aeronautic networks. Since September 2018, she is responsible of the security branch in ***ENET'com*** and a head of the committee of research masters. She published 4 chapters and co-authored more than 40 papers that have been published in international journals and refereed conferences. Her research interests are in the area of network security with special emphasis on security of vehicular networks, security of cloud networks, authentication protocols and security of Body Sensor networks.

Ahmed Fakhfakh is professor for Engineering-of-Electronic-and-Communication-Systems at ***ENET'com*** Sfax, Tunisia. He has obtained his engineering degree in electrical engineering from ENIS in 1997, his DEA and PhD thesis in electronics both from ***Bordeaux university*** respectively in 1998 and 2002. In 2009, he has obtained the HDR diploma in electrical engineering from ***ENIS***. From 2002 to 2016, he was member of the Laboratory of Electronics and Information Technologies (***LETI***) in ENIS. In 2012, he is the director at ***ENET'com***. Since 2016, he is member of the Laboratory of [1]Laboratory of signals, systems, artificial intelligence and networks (***SM@RTS***), in the Digital research center of Sfax (***CRNS***) and head of the research team "Design and implementation of communicating systems". He was a supervisor of 20 PH.D thesis in fields of smart grid, vehicular communications and wireless sensor network applications. He published more than 25 papers that have been published in international journals and refereed conferences.

Olfa Kanoun is professor for measurement and sensor technology since 2007 at ***TU Chemnitz, Germany***. She graduated in electrical engineering at the ***Technische Universität München*** from in 1996, where she specialized in the field of electronics. Her PhD at the ***University of the Bundeswehr*** in Munich was awarded in 2001 by the Commission of Professors in Metrology (AHMT e. V.) in Germany. In 2015 she was awarded by the Tunisian ministry of social affairs for her scientific excellence and outstanding achievements. In her research she focuses on sensors, measurement systems and measurement methods. Since 2001 she is developing new sensors and measurement solutions based on impedance spectroscopy in the fields of battery diagnosis, bio-impedance spectroscopy, inductive sensors, capacitive sensors, conductivity sensors and material testing. She has a deep expertize in the field of energy harvesting and energy transmission and develops since many years *successfully flexible nanocomposite sensors for force, temperature and humidity measurements. As* ***senior IEEE member****, she volunteers for the* the Instrumentation and Measurement Society and for IEEE. In 2004 she founded an IEEE IM Chapter and in 2014 she initiated a student branch at TU Chemnitz. She serves as co-chair of the Technical

Committee on nanotechnology in instrumentation and measurement (TC 34). In 2001 she was co-founder of the international multi-conference on systems, signals and devices (***SSD***) and in 2008 she initiated the annual International Workshop on Impedance Spectroscopy (***IWIS***). She is author or co-author of 7 books, 52 papers in international journals with peer review, 110 papers in proceedings of international conferences and 6 journal special issues. She is member of the editorial board of Technisches Messen (***De Gruyter***) and associate editor of the journal on Digital Signals and Smart Systems (***IJDSSS, Inderscience***).

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Mbarka Belhaj Mohamed carried out the simulation and the evaluation of the proposed contributions and the redaction of the paper.

Amel Meddeb-Makhlouf has verified the results of Section 3. *A. AES and SHA-based data security.*

Ahmed Fakhfakh has validated the proposed prototype Section. IV. REAL EXPERIMENTATION.

Olfa Kanoun was responsible for the paper organisation.