Man-in-the-Middle Attack Mitigation in Internet of Medical Things

Osman Salem, Khalid Alsubhi, Aymen Shaafi, Mostafa Gheryani, Ahmed Mehaoua, and Raouf Boutaba, *Fellow, IEEE*

***Abstract*—The Internet of Medical Things are susceptible to Man-in-the-Middle (MitM) attack, which can identify healthcare emergency of monitored patients and replay normal physiological data to prevent the system from raising an alarm. In this article, we propose a framework to prevent a MitM from disrupting the operations and prohibiting the raise of alarms by the remote healthcare monitoring system. To reduce energy consumption for normal data transmission, and preserve the privacy of health data, our framework transmits a smaller size signature derived from acquired data with message authentication code, where the key is derived from received signal strength indication. Our experimental results for emergency detection show that our approach can achieve a high detection accuracy with a low false alarm rate of 3%.**

***Index Terms*—Anomaly detection, authentication, Bluetooth Low Energy (BLE), cyber-attacks, healthcare, Internet of Medical Things (IoMT), wireless body area networks (WBANs), wireless security.**

I. Introduction

THE Internet of Medical Things (IoMT) is a set of medical sensors used to collect physiological data from the body of a remotely monitored patient. As these sensors have restricted resources and limited transmission power, they transmit measured data to a local processing unit (LPU—such as tablet, smartphone, etc.) for processing. The LPU has more resources (i.e., processing power, energy, and transmission capability) than sensors, and facilitate data processing for emergency healthcare detection is running on LPU. When an emergency situation is detected, an alarm is transmitted to the healthcare professionals to take appropriate actions.

Several security mechanisms have been proposed to secure the communications between sensors and LPU, and offer confidentiality, integrity, and availability (CIA) triad in monitoring. Each mechanism has strengths and weaknesses (e.g., undisclosed or unpatched vulnerabilities), which can be exploited to circumvent security and perform Man-in-the-Middle (MitM) attacks.

The Bluetooth Low Energy (BLE) is widely implemented and leveraged in IoMT to exchange data with the LPU, where monitoring applications in portable medical devices require a short-range communication, low bandwidth, and delay. The Security Manager module in BLE uses protocols and algorithms to secure communications (AES with 128-b key) and provide protection against several attacks [1]. However, the security of BLE and data protection depends heavily on the I/O capability of sensor devices, display, and keyboard, which are used to confirm keys for communication end points. Furthermore, recent works [2]–[4] have pinpointed vulnerabilities in BLE-based IoT devices and conducted experiments to exploit them.

The MitM attack exploit the vulnerabilities and limited resources of sensors. Several publicly available tools (such as GATTacker, BtleJuice, Mirage [5], etc.) can be leveraged to launch MitM attacks. Though the normal radio range of BLE cannot exceed 100 m, these tools can be used with special radio adapters that allow an attacker to intercept BLE up to 1000 m.

We consider a realistic scenario in healthcare monitoring, where an attacker succeeds in MitM attack, despite the deployed security measures in the communication infrastructure. The attacker is able to intercept and decrypt the exchanged data between sensors and LPU. Therefore, the attacker can sniff the private data, and conduct analysis on captured data to detect heavy changes or healthcare emergency. To disrupt the monitoring system from raising an alarm when patient needs assistance, the MitM can modify abnormal data and transmit normal measurements to the LPU. In the same malicious spirit, a demonstration was conducted by Jay Radcliffe, where false commands were injected to prevent the Medtronic infusion pump from injecting or to overdose the diabetic patients with insulin [6].

In this article, we propose a framework to prevent a MitM from modifying the data and disrupting the function of the remote monitoring system. Mostly, the data transmitted by the sensor are normal with infrequent anomalies [7]. The data are processed by the LPU to identify heavy changes in measurements before

Manuscript received March 6, 2021; revised May 10, 2021; accepted June 8, 2021. Date of publication June 15, 2021; date of current version December 6, 2021. This work was supported by the Deanship of Scientific Research, King Abdulaziz University, Jeddah, Saudi Arabia, under Grant KEP-9-611-42. Paper no. TII-21-1094. *(Corresponding author: Osman Salem.)*

Osman Salem, Aymen Shaafi, Mostafa Gheryani, and Ahmed Mehaoua are with the Borelli Research Center, CNRS UMR, University of Paris, 75006 Paris, France (e-mail: Osman.Salem@parisdescartes.fr; aymen.shaafi@etu.parisdescartes.fr; mostafa.gheryani@etu.parisdescartes.fr; ahmed.mehaoua@parisdescartes.fr).

Khalid Alsubhi is with the Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21441, Saudi Arabia (e-mail: kalsubhi@kau.edu.sa).

Raouf Boutaba is with the David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: rboutaba@uwaterloo.ca).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2021.3089462.

Digital Object Identifier 10.1109/TII.2021.3089462

raising an alarm. Therefore, to prevent the MitM from getting access to private data, only the signature of acquired data is transmitted by the sensor. The change detection algorithm in the LPU takes the data signatures, which preserve the gap between measurements. We use the locality-sensitive hashing (LSH) to derive data signature, which is irreversible and prevents an attacker from deducing the private data or accessing it. On the other hand, the transmission of signatures instead of measurements significantly reduces the packet size and consequently the required energy for data transmission. To prevent modification attacks, a keyed Hash Message Authentication Code (HMAC) is transmitted with the message, where the initial value of the key is derived from the received signal strength indication (RSSI). The RSSI has been widely used in BLE for indoor geolocalization and its value depends on the distance between communicating devices. The MitM will not be located at the same distance as sensors, hence the corresponding RSSI value will differ from the RSSI value used to derive the authentication key.

In summary, our contributions are threefold, which are as follows.

1) We provide a method to reduce energy consumption for normal data transmission, where much smaller sized signatures derived from measured data are transmitted from the sensor to the LPU.
2) Based on the aforementioned signature, we prevent a successful MitM from accessing the measured data and preserve the privacy of health data.
3) Considering MitM's malicious intent of deterring alarms from the monitoring system, we prevent modification and replay attacks by using HMAC with the initial key derived by the communicating entities based on their RSSI.

The rest of this article is organized as follows. In Section II, we review the recent related work. In Section III, we present our proposed approach to prevent a MitM from accessing the data. In Section IV, we conduct a comprehensive analysis and comparative study to analyze the performance of our approach. Finally, Section V concludes this article.

II. Related Work

Intrusion detection systems for IoT have received attention after volumetric attacks exploited the deployed sensors for distributed denial of service attack (e.g., Mirai [8]). Zuo *et al.* [9] hijack IoT connections using MiTM by exploiting the pairing mode in deployed BLE. In BLE authentication phase, the short-term key (STK) is used to encrypt the exchange of long-term keys, which in turn is used to encrypt data. In fact, we have two generation methods for STK in BLE, where the first is based on passkey display and depends on the input/output capabilities of IoT to enter the code, and the second is based on insecure exchange of unencrypted text and makes devices vulnerable to MitM attacks.

Data mining (DM) and machine learning (ML) approaches have been applied to identify malicious or compromised sensor. Nguyen *et al.* [10] apply deep neural networks to detect anomalous deviation in the data traffic. Kavousi-Fard *et al.* [11] propose an ML model to detect data integrity attack in wireless sensors, and they use the neural networks (NN) to derive the lower and upper band estimation of the prediction intervals to secure microgrid sensors from MitM attacks.

Hasan *et al.* [12] compare the performance of several ML algorithms used in the literature to detect anomalies and predict attacks in the IoT systems. They compare the performance of: logistic regression (LR), support vector machine (SVM), decision tree (DT), random forest (RF), and artificial NN (ANN) in terms of accuracy, precision, recall, and F-score. They found that RF achieves comparatively better than other algorithms (LR, SVM, DT, RF, and ANN), with comparable accuracy.

In the same spirit, Hafeez *et al.* [13] review recently proposed anomaly detection techniques, which are based on DM and ML for the detection of cyber-attacks in IoT, where any deviation from normal learned patterns is used to detect anomalous behavior. These algorithms consume a lot of time and resources and cannot achieve real-time analysis. Therefore, they proposed the use of fuzzy C-means and fuzzy interpolation to detect malicious traffic activity despite the huge amount of data collected and transmitted by devices. Their proposed framework (IoT keeper) restricts access to devices with normal network activity. They also identify five threats in IoT to detect and block in edge networks, where the injection and replay attacks by MitM are among them.

Koutras *et al.* [14] review recent related work on security in IoMT communications while focusing on medical applications. They classify communication protocols with respect to their usage in medical application and examine the inherent security characteristics, limitations, and implementation gaps in IoMT. For BLE, they identify the vulnerabilities and feasible attacks: sniffing, DoS, MitM, brute-force, device duplication attacks, etc. Therefore, their review confirms the ability to conduct MitM in BLE used in medical devices.

Asharaf *et al.* [15] review recent intrusion detection approaches for cyber-attack incidents against IoT. Most of the surveyed anomaly detection perform offline analysis and require training model. They also review IoT-based threats and attacks, where an attacker makes all IoT devices connect to the software enabled access point as it has a stronger signal than the actual LPU. Therefore, the MitM can eavesdrop and compromise all the communications despite the deployed security infrastructure. In the same spirit, Lawal *et al.* [16] analyze the security threat and pinpoint MitM through poisoning to eavesdrop or modify the exchanged data.

Guo *et al.* [17] propose a symmetric cryptosystem to support real-time healthcare monitoring applications in untrusted environment where data in transit are encrypted and the LPU processes received data without decryption. The spirit of their work is very similar to our proposed approach.

Jamming attack is a critical issue in IoT, where intentional malicious messages are sent by attackers to create interferences and prevent normal communications. Several channel hopping solutions [18] have been proposed to defend against jamming attacks, including proactive and reactive strategies. To cope with the jammer, a pseudorandom sequence is used to switch the channel periodically (each k seconds) in proactive solutions. In reactive solutions, a jamming detection mechanism is required

Fig. 1. MitM prevents raising alarms.

prior to channel switching. The main challenge is to derive the same channel number on the LPU and the sensor without explicit exchange, to prevent the attacker from following the sequence and jam continuously. Several mechanisms based on predefined, random, RSSI, and secret have been proposed as channel switching solutions to escape the jammer (see [18] and [19]). In our proposed approach, we use the RSSI to derive the distance between sender and receiver, and subsequently derive the same authentication keys used in HMAC to prevent data modification and injection.

Hence, recent existing works confirm the possibility to conduct MitM despite the deployed security framework. We want to add an additional security layer to prevent the attacker from accessing or modifying the transmitted data in case of successful MitM attack. To prevent such situation, a signature or bitmaps derived from the measured values are transmitted in the network instead of transmitting the raw physiological measurements. In case of successful attack, the MitM cannot see the data but only their irreversible signature. To prevent an attacker from modifying or replaying old signatures, an authentication key is derived by communicating devices based on the signal strength. This key is used in message authentication code sent along data or their acknowledgement to prevent the MitM from sending spoofed ACK.

III. Proposed Approach

In this section, we propose an approach to mitigate the impact of MitM attack. We assume a general deployment scenario for remote healthcare monitoring and a successful MitM attack. Despite the deployed security, the MitM in Fig. 1 is able to intercept the data transmitted by the inertial measurement unit to LPU. By running the same algorithm as in the LPU, the MitM can detect the fall and replay previous normal data to prevent the monitoring system from raising alarms for assistance.

In Fig. 2, we present the building blocks of our proposed system to mitigate the impact of successful MitM attack in the IoMT. The first block is the data acquisition, where several physiological parameters, such as heart rate (HR), pulse, blood pressure (BP), oxygenation ration (SpO_2), and temperature (T) are acquired by the sensors. These physiological data records are feed to the data preprocessing block that cleans the data and removes outliers by using median filter. Next, the LSH blocks derive the signatures or bitmaps from the records and append the calculated HMAC to the message before transmission to prevent modification or future replay attacks. Note that the sequence number of the packet is included in the HMAC.

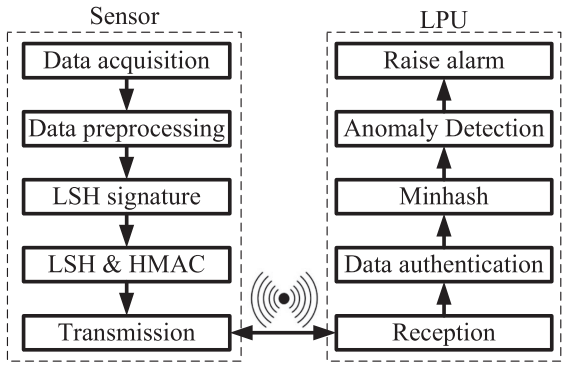

Fig. 2. Components of our proposed framework.

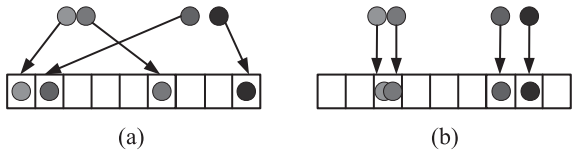

Fig. 3. Comparison between HF and LSH. (a) Universal HF. (b) Local sensitivity hashing.

In the reception block on the LPU, the authenticity of received signature is verified before conducting anomaly detection to identify healthcare emergency and raise an alarm for assistance.

In Fig. 2, the sensor transmits the LSH of data along with the HMAC. As the data are not readable by MitM, our system provides confidentiality. Furthermore, the HMAC provides authentication and integrity (authenticity) using the sequence of authentication keys, as shown in Section III-C.

A. Locality Sensitive Hashing

LSH is used to identify nearest neighbors (NN) in ML and DM, where it performs dimensionality reduction through the generation of hash value (or bitmap) that preserves the similarity between data points. The LSH is a random projection function that maximize collisions for similar points by generating the same hash value for two similar input, as shown in Fig. 3(b).

In contrast to cryptographic hash function (shown in Fig. 3(a)) that reduces collisions in the derived fingerprint, by generating very different outputs even for near or similar inputs, the LSH preserves the distance between input values, where similar measurements produce similar (same or near) hash values (see Fig. 3), whereas deviated measurements have hash values far from each other. Therefore, the rationale behind using LSH is to identity abnormal or deviated measurements from the hash values.

For a data record V_i of length n (the record contains n physiological measurements), we use a k spherically symmetric random vector U_i of length n to derive the bitmap $(h_k(V_i))$, as given in the following:

$$h_k(V_i) = \begin{cases} 1 \text{ if } & U_k.V_i \geq 0 \\ 0 \text{ if } & U_k.V_i < 0 \end{cases}. \quad (1)$$

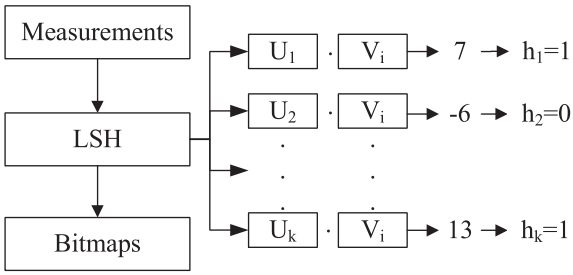

Fig. 4. Derived bitmaps from LSH.

Fig. 4 shows the derived bit h_k as the result of the product of $U_k = [u_{1k}, u_{2k}, \ldots, u_{nk}]$ and the record $V_i = [v_{1i}, v_{2i}, \ldots, v_{nt}]$. As the result of each vector product is 1 b h_k, the use of k random vector U_k results in a bitmap of k bits $(h(V_i) = [h_1 h_2 \ldots h_k])$, denoted by hash table or LSH signature of the record.

For two given records V_i and V_j, the resulting bitmaps satisfy the following equation:

$$\begin{aligned} &\text{if } \text{dist}(V_i, V_j) \le R \Rightarrow P\left(h(V_i) = h(V_j)\right) \ge p_1 \\ &\text{if } \text{dist}(V_i, V_j) \ge cR \Rightarrow P\left(h(V_i) = h(V_j)\right) \le p_2 \end{aligned} \tag{2}$$

where $c > 1$ and $p_1 > p_2$. The LSH tend to produce the same hash (or signature) for similar records. Therefore, the probability P is high if V_i and V_j are close to each other, whereas the probability is low when V_i and V_j are far apart. The use of LSH is twofold. First, it reduces the size of transmitted record, where only the signature LSH is transmitted instead of the n physiological data in the record. Second, the signature is used to measure the similarity between measured records and conduct anomaly detection.

Various techniques for deviation detection in the derived LSH signature have been proposed, such as Euclidian, χ^2 and Hamming distance, cosine similarity, etc. In our implementation, we calculate the MinHash similarity to identify deviating records.

B. MinHash for Anomaly Detection

To detect changes between received signatures in the LPU, we used the MinHash similarity, which provides an estimation of Jaccard similarity (JS)

$$\text{JS}(V_i, V_j) = \frac{|V_i \cap V_j|}{|V_i \cup V_j|} = P\left(h(V_i) = h(V_j)\right). \tag{3}$$

The JS was formulated by Tanimoto similarity for bitmaps as

$$\text{TS}(V_i, V_j) = \frac{V_i . V_j}{\|V_i\| + \|V_j\| - V_i . V_j} = \frac{\sum_{k=1}^{n} |V_{ik} \wedge V_{jk}|}{\sum_{k=1}^{n} |V_{ik} \vee V_{jk}|} \tag{4}$$

where $\wedge$ and $\vee$ denote the bitwise *AND* and *OR* operators, and $\|V_i\|^2$ is the magnitude of V_i

$$\|V_i\|^2 = \sum_{k=1}^{n} v_{ki}^2. \tag{5}$$

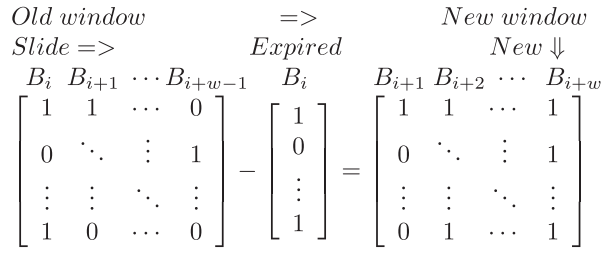

Fig. 5. Sliding window.

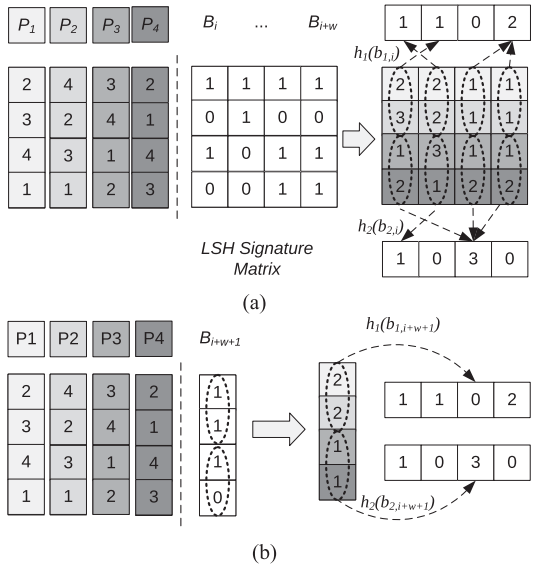

Fig. 6. Detection of deviations in signature. (a) MinHash permutation. (b) Anomaly detection.

To reduce false alarms, we do not base our analysis on the comparison between the latest two received bitmaps, instead we take a sliding window containing the latest w received bitmap into consideration, as shown in Fig. 5.

To measure the similarity between the latest received bitmap with past bitmaps in the sliding window, we apply the MinHash that uses D random permutations (using vector P_1, P_2, P_3, and P_D) on the raw index of the past w bitmaps. The random permutations on bitmap is used to determine a nonzero bit that will be placed in the first position of each permutation. The result of such HF is the index of the first element in the permuted B_i, which has value 1

$$h_j(B_i) = \min_{j \in B_i} \left(P_j\left(B_i\right)\right). \tag{6}$$

The resulted MinHash signature matrix from the random permutations is used to measure the similarity of newly received bitmaps (B_{i+w+1}) with past w bitmaps in LSH signature matrix $([B_i, B_{i+1}, \ldots, B_{i+w}])$. For clarification, Fig. 6(a) presents a simple example of MinHash with four permutations, which is used to derive the MinHash signature matrix. As one bitmap is derived from several physiological parameters, we divide the signature matrix into b bands with r rows per band. Each band (b_i) is hashed using the universal HFs and the associated buckets in the hash table is incremented by one.

The main idea behind the use of MinHash is to have an HF that is sensitive to distances. In other words, if two measurements are close to each other, the probability that this function hashes them to the same bucket is high. Conversely, if the points are far apart, the probability that they get hashed to the same bucket is low.

The MinHash provides a fast and unbiased estimation of the JS between two sets. As the MinHash can be computed in linear time $O(m)$ on the size of the bitmap B_i, the pairwise similarity estimation between w bitmaps (wxB_i) leads to substantial savings in running time compared to doing a full comparison of the members of each bitmap.

To distinguish between normal changes in the monitored physiological parameters caused by daily activities, and those induced by health emergency, the spatial correlation between parameters is exploited, where at least r attributes must simultaneously deviate to reflect such correlated changes before raising a medical alarm.

A family of HFs $H = \{h_i : U \to 0, \ldots, m-1\}$ is called universal if the collision probability for two different bands (i.e., b_i and b_j) through two different hash is at most $1/m$, where m is length of the hash table

$$\forall b_i, b_j \in U,\ b_i \neq b_j : P\left[h(b_i) = h(b_j)\right] \leq \frac{1}{m}. \tag{7}$$

When a new signature (B_{i+w+1}) is received, the same permutation is applied to derive the MinHash signature, as shown in Fig. 6(b), and each band is hashed to verify the value of the associated bucket in the hash table. If the associated value is not zero, the band is similar and considered as normal. In Fig. 6(b), the MinHash of the last received bitmap is derived and divided into two bands, with two rows per band in this simple scenario. The first part maps to an empty bucket (dissimilar) and the second part maps to the bucket with value 3 (similar). When the similarity is lower than a predefined threshold h (75% in our implementation) in terms of band, an alarm is raised for healthcare emergency.

After the decision is made, the oldest bitmap is removed from the LSH and MinHash signature matrix. It is also removed from the universal hash tables, where the associated buckets are reduced by one for indexes generated by applying the HFs on this bitmap.

C. Data Authentication

The RSSI is the power measurement of the received signal. The BLE RSSI has been recently used in tacking the spread of coronavirus (COVID-19), proximity detection and infectiousness risk [20]. Several research [20]–[22] addresses the fluctuation in this signal and proposes methods to compensate the biased RSSI measurements.

In our approach, we use the RSSI signal to derive the initial authentication key and change it based on the distance between LPU and sensors. In fact, both sender and receiver derive their distance from corrected RSSI signal. As the attacker is not located at the same distance, its measured RSSI value is not the same and consequently cannot derive the same key.

The basic idea is to accept measurements from sensors within nearest locations using the RSSI, where sensors are near as they are deployed on the body of the monitored patient, and to refuse data from other far away sensors as their RSSI deviates from the majority. The RSSI is continuously decreasing with the distance from the other device, and the intensity attenuation model is described as

TABLE I
VARIATION OF RSSI WITH DISTANCE

Distance (m)	RSSI (dBm)	Dist (m)	RSSI (dBm)	Distance (m)	RSSI (dBm)
0.5	-63	3	-73	5.5	-76
1	-66.50	3.5	-73.75	6	-76.5
1.5	-69	4	-74.5	6.5	-77
2	-70.50	4.5	-75	7	-77.5
2.5	-72	5	-75.5	7.5	-78

$$\mathrm{RSSI}_d = \mathrm{RSSI}_{d_0} - 10\gamma \log_{10}\left(\frac{d}{d_0}\right) + x_\sigma \tag{8}$$

where RSSI_{d_0} is the RSSI value at the reference distance d_0 ($d_0 = 1$ in our experiments), RSSI_d is the measured value at the distance d, γ is the path loss exponent related to distance, and x_σ denotes a Gaussian random variable with zero mean induced by shadowing. At distance 1 m, the measured RSSI_{d_0} is -66.50 dBm, and for simplification, x_σ is set to 0 in our experiments, where the distance is derived using (9). The path loss exponent γ is 1.25 and determined by fitting the acquired data. Table I shows the measured values of RSSI at a distance interval of 0.5 m

$$d = 10^{(\mathrm{RSSI}_{d_0} - \mathrm{RSSI}_d)/10\gamma}. \tag{9}$$

Therefore, to establish communication between sensor and LPU in the initial phase, they must measure the same distance to derive the same key. A Password-Based Key Derivation Function (PBKDF) is used to derive a sequence of authentication keys, each key of length 32 B. The PBKDF is used for key stretching, where it makes the password cracking resistant to dictionary attacks and much more difficult to find.

To check the initial key, the LPU sends the universal hash of PBKDF(d) to the sensor, which must acknowledge the correctness and installation of the key. Otherwise, the sensor sends NACK and the devices retry to derive the distance from the newly measured RSSI. In fact, during the initial phase, the sender and receiver are near to each other and have an accurate RSSI and derived distance.

In the operation phase, when the distance measured by the LPU increases or decreases by at least 0.5 m during 1 min, i.e., the change in the value of distance must be greater than 0.5 m during six consecutive measurements (each of 10 s), the LPU initiates a key change procedure with the sensor. The LPU sends the universal hash value of the second key (derived in the initial phase) and waits for confirmation before installing and using the new key. It is important to note that the key change is triggered by a change in the value of RSSI and the initial key derivation is based on distance. The key change is triggered by a change in the distance of at least 0.5 m.

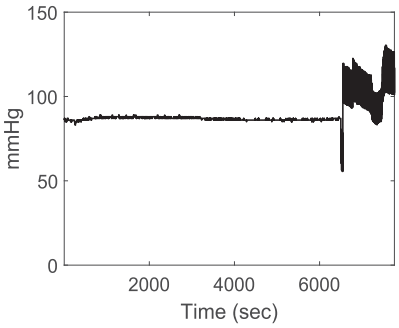

Fig. 7. Blood pressure for patient 1.

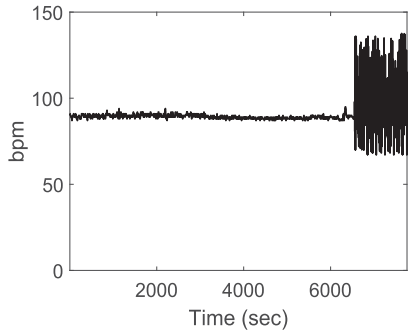

Fig. 8. Heart rate for patient 1.

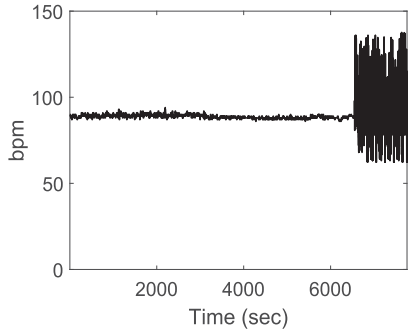

Fig. 9. Pulse.

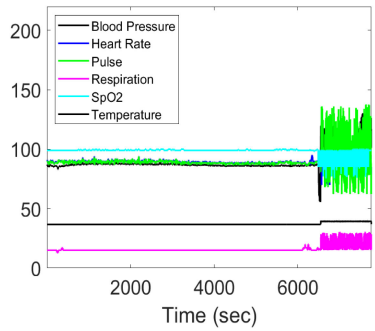

Fig. 10. Six attributes.

IV. Experimental Results

In this section, we present our experimental results conducted on Raspberry Pi, with the e-Health sensors platform [23] used as prototype for the implementation of our approach. A Raspberry Pi 4 is used as an interface to transmit the measured data by the e-Health sensors, which are connected directly to the human body. Though this realistic prototype is able to acquire and process physiological data in real time, we conduct performance analysis on a dataset with abnormal measurements, i.e., the annotated Multiple Intelligent Monitoring in Intensive Care database from the PhysioNet [24] website. A chunk of patient dataset (records 55 and 259) is stored in a file on Raspberry Pi and records are loaded and transmitted using BLE to the LPU while respecting the difference between their time stamps. We downloaded and configured the open source Bluetooth stack (BlueZ), as described in [25].

Both records (55 and 259) contains 12 attributes, including systolic arterial BP, diastolic arterial BP, mean arterial BP, cardiac output, mean pulmonary artery pressure, systolic PAP, Diastolic PAP, HR, PULSE, respiration or breathing rate, oxygen saturation or oxygenation ratio (SpO_2), and body temperature T°. Out of these attributes, we focus on six attributes, i.e., BP, HR, PULSE, RESP, SpO_2, and T°. We start the first set of our experiments on data record 55 by displaying the variation of monitored physiological parameters and the raised alarms by our system, which are triggered by heavy changes in the physiological measurements.

We start by showing, in part, the variations of the physiological parameters from the first record. Fig. 7 shows the variation of the BP, where notable changes occur at the end of the acquired values. The variations of the HR and pulse are presented in Figs. 8 and 9, respectively. Both parameters present similar variations with the same values, and both are measured in beats per minutes (b/min). As physiological parameters are heavily correlated, pulse exhibits heavy changes in the same time period as the changes in HR.

To prove the correlation between physiological parameters, where a change occurs in several parameters in the same interval, the variations of the six monitored physiological attributes are presented in Fig. 10. The first curve in Fig. 10 (from the bottom) represents the variations of the respiration rate in terms of respirations per minute, where an increase is visible at the end of the capture. The second curve presents the variation of body temperature T° in degree Celsius, where it also increases with the respiration rate.

The first curve from the top of Fig. 10 presents the variation of the oxygenation ratio SpO_2, which is the percentage of oxygen in the blood and its normal value must be greater than 95%. When the value of SpO_2 is lower than 95%, a respiratory assistant and ventilators are required to prevent asphyxia, lack of oxygen, and heart disease. In fact, as the SpO_2 decreases at the end of the capture, the respiration rate of the monitored patient increases along the HR and pulse. We can clearly see a zone of correlated change. The change in physiological data are correctly identified by the LSH and MinHash for similarity analysis. The raised alarms by our approach are presented in Fig. 11.

In the second set of experiments, we present our results on data record 259, which has more variations than the previous dataset. Fig. 12 shows BP with several zones of variations. Fig. 13 shows the variations in HR, where HR and pulse have similar but

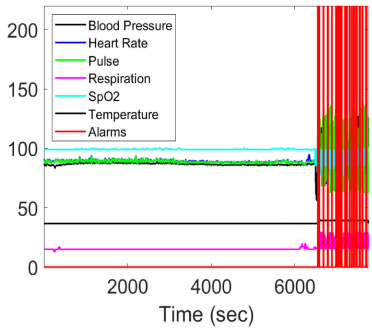

Fig. 11. Data with raised alarms.

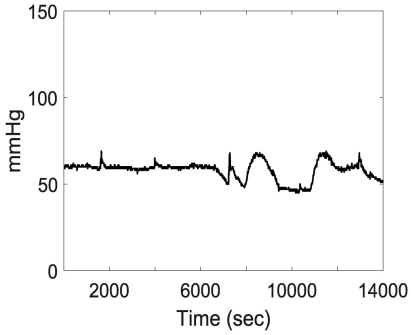

Fig. 12. Blood pressure for patient 2.

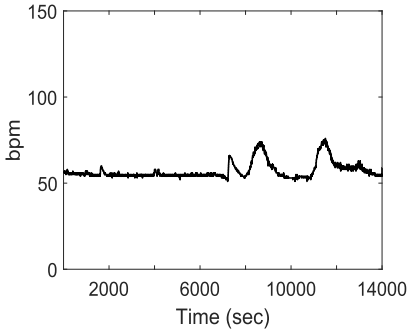

Fig. 13. Heart rate for patient 2.

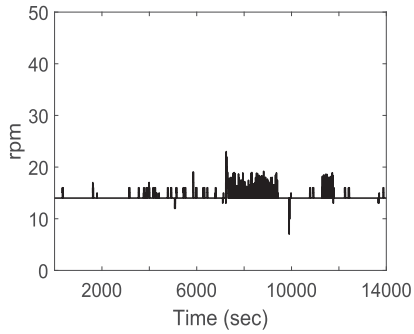

Fig. 14. Respiration rate.

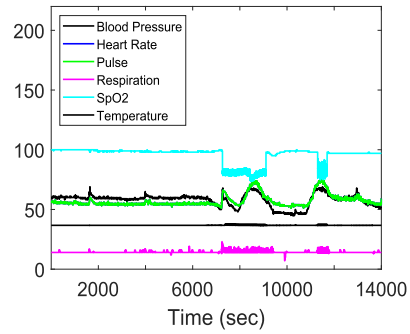

Fig. 15. All data.

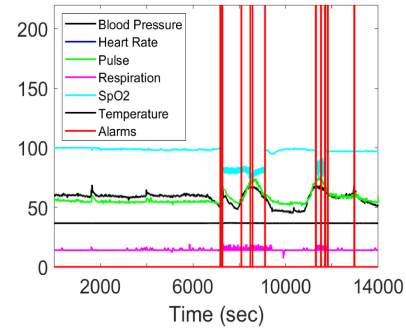

Fig. 16. Raised alarms.

several variations. Fig. 14 highlights the variation in respiration rate with an increase during the changes in other physiological parameters. The variations in SpO_2 and body temperature are shown in Fig. 15 (second and top curves). The oxygenation rate decreases during two times interval with a correlated increase in the respiration rate, where the body of the monitored patient tries to acquire oxygen. Fig. 15 depicts the variation of all parameters to visually localize the correlated zone of changes. The raised alarms by our similarity analysis approach are presented in Fig. 16.

In the third set of experiments, we analyze the impact of the parameters on the performance of the proposed framework. In our implementation, a bitmap of 32-b replaces the transmission of n physiological parameters, to reduce the energy consumption and prevent MitM from getting access to or analyzing medical data. We set the length of the bitmap $k = 32$, the rows per band $r = 4$, the number of bands $b = 8$, and the threshold $h = 75\%$. The probability that two records (R_1 and R_2) with 75% of similarity will hash in one bucket for any of the eight bands ($h = 1 - 8/32 = 0.75$) is $0.75^4 = 0.316$. Fig. 17 shows the variation in probability when changing the value of r from [1,10], where Figs. 18–20 show the variations in probability to map in the same bucket while varying the value of b from [1,10] for $r = 1$, $r = 4$, and $r = 8$, respectively.

We investigate the impact of MitM, where an attacker is located between the LPU and the sensor. The attacker can eavesdrop on all transmitted traffic between the target sensor and LPU, and will try to acquire several information from the exchanged data. The attacker may wait until the sensor connects (pairing) to the LPU and capture a pcap file containing whole exchanged information (pairing, bounding, data exchanges, etc.).

Even though the MitM does not have access to private medical data, the attacker still able to detect deviations from signatures and tries to replay old signatures. The MitM fails to produce a

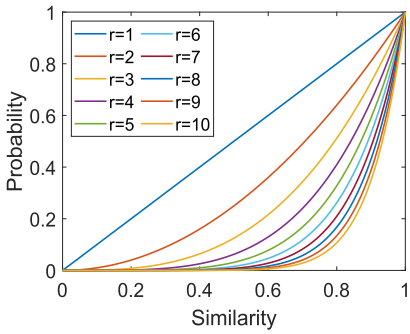

Fig. 17. $r = 1..10$ and $b = 1$.

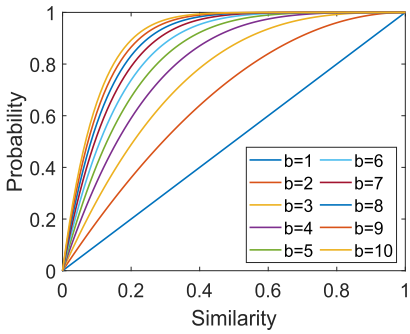

Fig. 18. $r = 1$ and $b = 1..10$.

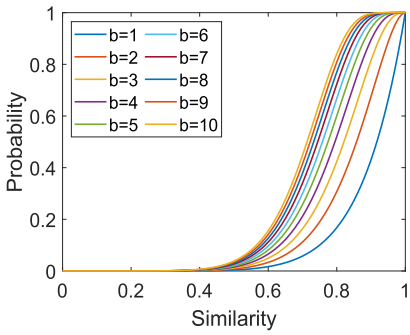

Fig. 20. $r = 8$ and $b = 1..10$.

valid HMAC with the new sequence number and the replayed data will be rejected in the LPU. Furthermore, the change in the RSSI of received data by the LPU induces a request to change the authentication password. On the other hand, the reliable transmission of data and the required authenticated ACK let the sensor raises a disconnection alert to notify the user of connectivity loss. The MitM fails to achieve replay, injection, and black hole attacks. In short, the proposed scheme mitigates exposure of information from the MitM and provides a second layer of security by preventing additional attacks by the MitM.

Afterward, we conduct performance analysis of our proposed approach to measure the accuracy in terms of true positive rate (TPR) and false alarm rate (FAR). The receiver operating characteristic (ROC) is used to study the impact of the similarity threshold on the accuracy of the system. The TPR and FAR are

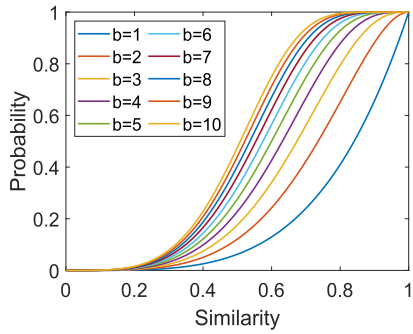

Fig. 19. $r = 4$ and $b = 1..10$.

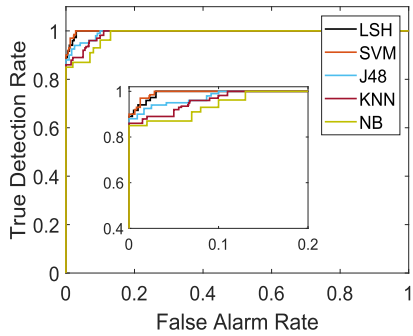

Fig. 21. Receiver operating characteristic.

given by the following equations:

$$\text{TPR} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{10}$$

$$\text{FAR} = \frac{\text{FP}}{\text{FP} + \text{TN}} \tag{11}$$

where TP is the number of true positives, FP is the number of false positives, FN is the number of false negatives, TPR is the percentage of true medical alarms that are raised as alarms, TN is the number of true negatives, and FAR is the percentage of misclassified normal data. The set of true medial alarms was reported in [24].

The ROC reflects the relationship between TPR and FAR, where a TPR closer to 100% indicates good performance in emergency detection, whereas a lower TPR indicates under performance in anomaly detection. A lower value of FAR is also desirable to achieve a good performance. To prove the effectiveness of our approach, we compare its accuracy with existing works [12], [26]. We present the performance results of four supervised classification algorithms: SVM, DT (J48), K-nearest neighbor (KNN), and naïve Bayes (NB).

The ROC curve presented in Fig. 21 shows that our approach achieves a TPR of 100% with 3% FAR. We found that the SVM slightly outperforms our approach with a TPR of 100% and a 2.8% FAR. The KNN, J48, and NB achieve a TPR of 100% with a FAR of 10%, 11%, and 13%, respectively. However, the required computational complexity to derive the SVM classification model in the sensor device is prohibitive and makes it impractical. The required computational complexity to derive the classification model in SVM is $O(n^3)$, where n is the number

TABLE II
NETWORK PERFORMANCE ANALYSIS

Metric	With HMAC		Without HMAC	
Goodput (kbps)	88.60	± 1.52	90.46	± 2.423
Latency (TCP)(ms)	0.44	± 0.004	0.39	± 0.003
Latency (UDP)(ms)	0.4	± 0.003	0.37	± 0.003

of records in training phase. The computational complexity to derive the model in other algorithms are: $O(1)$ for KNN (with $k = 3$), $O(2n)$ for NB, and $O(n\log(n))$ for J48. However, the accuracy of these algorithms is inversely proportional to their complexity to derive the model in the training phase, where J48 achieves better performance than KNN, which in turn performs better than NB. Obviously, our proposed approach for anomaly detection is fast—of the order of $O(1)$ requiring significantly less resources.

The results are more interesting when we start considering the memory requirements and CPU usage in the LPU and Raspberry Pi. The additional modules to perform LSH and RSSI estimation to derive the authentication keys consume less than 5 MB of the total available 4-GB RAM in Raspberry Pi 4, along with a few bytes from the virtual memory size. The memory consumed in the LPU is 12 MB to store previous signatures and achieve similarity comparison, where we keep only a fixed amount of data in the memory. The induced increase in the CPU usage is 12% in the CPU of the LPU and 5% in Raspberry Pi. The usage of the CPU can be explained by the required processing to verify the integrity, compare the signatures, remove the oldest signature, and insert the recent one inside the MinHash matrix. It is important to note that these statistics are derived by monitoring the memory and CPU usage before and after running our experiment.

We also investigate the network throughput and the impact of authenticated ACK. We used several tools to compare the throughput of authenticated versus disabled unauthenticated transmission. The required authenticated ACK, used to prevent black hole and data modification by the MitM, does not induce significant deterioration in network performance, in comparison to the baseline performance achieved using the same hardware, as shown in Table II. It is also important to note that our testbed uses nonoptimized implementation and hardware. As a result, network performance may vary and will potentially be better on different hardware and software stacks than the one used in our implementation.

V. CONCLUSION

In this article, we introduced an efficient and effective approach to enforce security in IoMT and mitigate the impact of MitM attack. We successfully addressed three important aspects: the privacy of physiological data, reliability of health monitoring system, and energy consumption. To prevent the MitM from getting access to private data, the LSH signature was transmitted instead of physiological value. To prevent modification, replay and black hole attacks, an HMAC was used with a key based on the RSSI value measured on both sensor and LPU. Our approach does not require labeled training data and does not need a classification model to detect heavy changes in the physiological parameters of monitored patient. Our experiments demonstrated that the proposed framework can achieve high detection accuracy with low false alarm rate (3%), when compared to supervised classification algorithms applied on the same annotated public dataset. In the future work, we will investigate the impact of jammer and the channel hopping solution using the derived authentication key as seed for pseudorandom function.

REFERENCES

[1] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd, and T. Hayajneh, "Security vulnerabilities in Bluetooth technology as used in IoT," *J. Sensor Actuator Netw.*, vol. 7, no. 3, 2018, Art. no. 28.

[2] M. E. Garbelini, C. Wang, S. Chattopadhyay, S. Sumei, and E. Kurniawan, "SweynTooth: Unleashing mayhem over Bluetooth low energy," in *Proc. USENIX Annu. Tech. Conf.*, 2020, pp. 911–925.

[3] A. Lahmadi, A. Duque, N. Heraief, and J. Francq, "MitM attack detection in BLE networks using reconstruction and classification machine learning techniques," in *Proc. 2nd Workshop Mach. Learn. Cybersecur.*, 2020, pp. 1–16.

[4] K. Lounis and M. Zulkernine, "Bluetooth Low Energy makes 'just works' not work," in *Proc. 3rd Cyber Secur. Netw. Conf.*, 2019, pp. 99–106.

[5] R. Cayre, J. Roux, E. Alata, V. Nicomette, and G. Auriol, "Mirage: Un framework offensif pour l'audit du Bluetooth Low Energy," in *Proc. Symp. sur la Sécurité des Technol. de l'Inf. et des Commun.*, 2019, pp. 229–258.

[6] A. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," 2020, *arXiv:2005.07359*.

[7] S. Gupta, N. Muthiyan, S. Kumar, A. Nigam, and D. A. Dinesh, "A supervised deep learning framework for proactive anomaly detection in cloud workloads," in *Proc. 14th IEEE India Council Int. Conf.*, 2017, pp. 1–6.

[8] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[9] C. Zuo, H. Wen, Z. Lin, and Y. Zhang, "Automatic fingerprinting of vulnerable BLE IoT devices with static UUIDs from mobile apps," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2019, pp. 1469–1483.

[10] T. Nguyen, S. Marchal, M. Miettinen, M. Dang, N. Asokan, and A.-R. Sadeghi, "DÏoT: A crowdsourced self-learning approach for detecting compromised IoT devices," 2018, *arXiv:1804.07474*.

[11] A. Kavousi-Fard, W. Su, and T. Jin, "A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 650–658, Jan. 2021.

[12] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet Things*, vol. 7, 2019, Art. no. 100059.

[13] I. Hafeez, M. Antikainen, A. Ding, and S. Tarkoma, "IoT-KEEPER: Detecting malicious IoT network activity using online traffic analysis at the edge," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 1, pp. 45–59, Mar. 2020.

[14] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in IoMT communications: A survey," *Sensors*, vol. 20, no. 17, 2020, Art. no. 4828.

[15] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in Internet of Things: Challenges, solutions, and future directions," *Electronics*, vol. 9, no. 7, 2020, Art. no. 1177.

[16] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, "Security analysis of network anomalies mitigation schemes in IoT networks," *IEEE Access*, vol. 8, pp. 43355–43374, 2020.

[17] C. Guo, P. Tian, and K. R. Choo, "Enabling privacy-assured fog-based data aggregation in E-healthcare systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 3, pp. 1948–1957, Mar. 2021.

[18] S. Djuraev and S. Y. Nam, "Channel-hopping-based jamming mitigation in wireless LAN considering throughput and fairness," *Electronics*, vol. 9, no. 11, 2020, Art. no. 1749.

[19] Q. Zhou, Y. Li, and Y. Niu, "Intelligent anti-jamming communication for wireless sensor networks: A multi-agent reinforcement learning approach," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 775–784, Feb. 2021.

[20] J.-M. Gorce, M. Egan, and R. Gribonval, "An efficient algorithm to estimate COVID-19 infectiousness risk from BLE-RSSI measurements," Inria Grenoble Rhône-Alpes, Grenoble, France, Tech. Rep. RR–9345, 2020.
[21] D. Cannizzaro *et al.*, "A comparison analysis of BLE-based algorithms for localization in industrial environments," *Electronics*, vol. 9, no. 1, 2020, Art. no. 44.
[22] R. C. Luo and T. Hsiao, "Indoor localization system based on hybrid Wi-Fi/BLE and hierarchical topological fingerprinting approach," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 10 791–10806, Nov. 2019.
[23] X. Hu, A. M. Abdulghani, M. Imran, and Q. H. Abbasi, "Internet of Things (IoT) for healthcare application: Wearable sleep body position monitoring system using IoT platform," in *Proc. Int. Conf. Comput., Netw. Internet Things*, 2020, pp. 76–81.
[24] PhysioNet, 2000. [Online]. Available: http://www.physionet.org/physiobank/database/mimicdb
[25] *Argenox—Bluetooth Low Energy Devices With a Raspberry Pi*. 2020. [Online]. Available: https://www.argenox.com/library/bluetooth-low-energy/using-raspberry-pi-ble/
[26] A. A. Toor, M. Usman, F. Younas, A. C. M. Fong, S. A. Khan, and S. Fong, "Mining massive E-health data streams for IoMT enabled healthcare systems," *Sensors*, vol. 20, no. 7, 2020, Art. no. 2131.

Osman Salem received the M.Sc. and Ph.D. degrees in computer science from Paul Sabatier University, Toulouse, France, in 2002 and 2006, respectively, and the Habilitation À Diriger des Recherches degree in anomaly detection in wireless body area networks for reliable healthcare monitoring from the University of Paris, Paris, France, in 2016.

From 2006 to 2008, he was with the Department of Computer Science, Telecom Bretagne, Brest, France, as a Postdoctoral Research Fellow. Since September 2008, he has been an Associate Professor with the University of Paris. His research interests include security and anomaly detection in medical wireless body area networks.

Khalid Alsubhi received the B.Sc. degree from King Abdulaziz University (KAU), Jeddah, Saudi Arabia, in 2003, and the M.Math. and Ph.D. degrees from the University of Waterloo, Waterloo, ON, Canada, in 2009 and 2016, respectively, all in computer science.

He is currently an Associate Professor of computer science with KAU. His research interests include network security and management, cloud computing, and security and privacy of healthcare applications.

Aymen Shaafi received the B.Sc. degree in electrical and electronic engineering from Tripoli University, Tripoli, Libya, in 2003, and the M.Sc. degree in computer engineering from EPITA Paris, Paris, France, in 2016. He is currently working toward the Ph.D. degree in secure and reliable monitoring of elderly using wireless body sensors with the Department of Mathematics and Computer Science, University of Paris, Paris.

His research interests include machine learning and classification, network security, cloud computing, and security and privacy of healthcare applications.

Mostafa Gheryani received the B.Sc. degree in electrical and electronic engineering from Tripoli University, Tripoli, Libya, in 2000, and the M.Sc. degree in computer engineering in 2016 from the University of Paris, Paris, France, where he is currently working toward the Ph.D. degree in automated epileptic seizures detection using wireless body sensors with the Department of Mathematics and Computer Science.

His research interests include biomedical signal processing, epilepsy, and pattern recognition and classification.

Ahmed Mehaoua received the M.Sc. and Ph.D. degrees in computer science from the University of Paris, Paris, France, in 1993 and 1997, respectively.

He is currently a Full Professor of computer networking with the University of Paris, and the Head of the Artificial Intelligence for Data Science and Cybersecurity Group, CNRS BORELLI Research Center, Paris, a governmental mathematics and computer science research center. His research interests include security and resource management in wireless medical sensor networks, wireless body area networks design and optimization, and quality of service management in IP multimedia networks.

Raouf Boutaba (Fellow, IEEE) received the M.Sc. and Ph.D. degrees in computer science from Sorbonne University, Paris, France, in 1990 and 1994, respectively.

He is currently a University Chair Professor and the Director of the David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, Canada. He also holds an INRIA International Chair in France.

Dr. Boutaba was the Founding Editor-in-Chief for the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT from 2007 to 2010 and the current Editor-in-Chief for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He is a Fellow of the Engineering Institute of Canada, the Canadian Academy of Engineering, and the Royal Society of Canada.