Secure mHealth IoT Data Transfer from the Patient to the Hospital: A Three-Tier Approach

Elias Yaacoub, Khalid Abualsaud, Tamer Khattab, Mohsen Guizani, and Ali Chehab

Abstract

eHealth and mHealth applications are gaining increasing importance with advances in the IoT and the ubiquity of sensor deployments. Measured IoT mHealth data needs to be captured, transmitted, and stored securely, without having the security measures hinder or delay the response of medical personnel in case of emergency. In this article, we present a holistic framework for data transfer from the patient to the hospital. Three tiers are identified in the proposed framework. In each tier, suitable security measures are presented for securing the data and protecting the privacy of the patients. The proposed methods range from physical layer security techniques designed for low portable sensors deployed at the patient's home or body, to combining traditional encryption methods with additional security procedures at the cloud data center where the medical records are stored.

Introduction

Remote patient monitoring is becoming one of the important applications of the Internet of Things (IoT) [1], where wireless IoT sensors are attached to the patient in the form of a body area network (BAN) [2]. A closely related application is ambient assisted living (AAL), where technology is used to assist elderly or disabled people in their daily activities, generally by using IoT sensors deployed in a smart way in their homes or surrounding environment. The BAN/AAL network allows monitoring their health situation and detecting any changes in their condition [3]. Thus, the BAN sensors and the other AAL sensors deployed throughout the living environment help sense and monitor the daily activities of patients or elderly people, and permit the provision of immediate medical intervention whenever needed [4].

However, BAN/AAL sensors are generally small devices, with limited battery capacity and limited computational power. When these sensors send their data wirelessly, they are subjected to several threats. Indeed, their limited capabilities make them vulnerable to cyber attacks. The sources of cyber attacks are evolving from individual hackers to well-organized groups of cyber criminals, which poses additional challenges to protect the privacy of the patients and the security of the data. These attacks could affect any part of the path from the BAN and AAL sensors to the storage of medical data on the hospital or cloud servers [5].

Consequently, appropriate security measures should be implemented throughout this path, while taking into account the capabilities of the IoT healthcare devices. The efficiency of such measures will increase the trust of citizens in mHealth systems dedicated to remote patient monitoring. Several works in the literature, for example, [6], have outlined the security concerns in eHealth/mHealth systems, and indicated the need to find suitable solutions that can address these security issues.

This article addresses this problem by first presenting a holistic framework for mHealth IoT data transmission from the patient to the hospital. The framework comprises three tiers, where devices with different capabilities and resources are used at each tier. Thus, appropriate security measures for securing the data and protecting the patients' privacy at each tier are proposed and analyzed. The purpose of these measures is to meet the security challenges while adapting to the capabilities and constraints of the devices at each tier.

Proposed Framework

This section describes the framework presented in this article. It is illustrated in Fig. 1, and consists of the following components.

Body Area Network (BAN) and Ambient Assisted Living (AAL) Sensor Network: This network consists of various sensors measuring either bodily parameters corresponding to the patient's health condition (BAN sensors), or parameters corresponding to the living environment of the patient or elderly person (AAL sensors). For example, the AAL devices can measure temperature, humidity, fire/smoke detection, and even record surveillance videos in case the patient needs to be monitored visually. The BAN and AAL data is transmitted locally to one or more controllers that connect to an access point (AP). The AP can itself be the controller and aggregate the data from the sensors before forwarding it to the network.

Network Edge Server (NES): The NES receives the data from the AP and then performs additional processing such as data cleaning, feature extraction, anomaly detection, and so on. In case no risks are detected, the data is encrypted and stored on the cloud data center. Otherwise, the NES communicates with the medical response team to handle the situation. The presence of the NES at the network edge is important to avoid any delays in case of emergency. The measured data by the BAN/AAL sensors can be sent to the NES using, for example,

Digital Object Identifier:
10.1109/MWC.2019.1800590

Elias Yaacoub, Khalid Abualsaud, Tamer Khattab, and Mohsen Guizani are with Qatar University; Ali Chehab is with the American University of Beirut (AUB).

1536-1284/19/$25.00 © 2019 IEEE

5G massive machine type communications (mMTC). However, whenever an emergency is detected, the NES communicates with the medical team, and the team can communicate with the patient (or access the surrounding sensors, the patient's family, and so on) through the NES, using ultra reliability low latency communications (URLLC) [7].

Medical Center (MC): A medical facility where professional medical personnel resides, and where the monitored patient can be admitted for treatment whenever the need arises. The MC is responsible for preserving the privacy of the patients and the security and integrity of their health records.

Medical Response Team (MRT): Ccorresponds to the medical personnel located at the MC. The MRT receives alert notifications from the NES whenever it detects (or suspects) an emergency situation.

Cloud Data Center (CDC): The CDC corresponds to the storage of the health data on the cloud. It could correspond to a data center with an aggregation of servers, which can preferably be located at different cloud premises, under the control of the MC. Another possibility consists of storing the data on the cloud with one or more cloud providers (CPs). This relieves the MC from the burden of managing huge amounts of data, but it remains responsible for the privacy of its patients and the security of their stored data. Thus, it is preferable to store the data with different CPs using the approach described in this article for Tier 3.

In case of emergency, the MRT at the MC is notified by the NES, and it can then take appropriate action, for example, sending an ambulance to the patient's location, notifying the treating physician, contacting the patient and/or their family to take immediate measures until the ambulance arrives, and so on. The MRT can retrieve the patient's historical data from the CDC, and then this data can be combined with the real-time information received from the NES in case of emergency, in order to make a better assessment of the situation.

It can be seen from the framework of Fig. 1 that the transmission of the measured mHealth data to the cloud goes through three communication tiers: (i) Tier 1 corresponds to the communication between BAN/AAL sensors to the AP; (ii) Tier 2 corresponds to the communications between the AP and the NES; (iii) Tier 3 corresponds to communications on the backbone network between the NES and the CDC, along with the data retrieval by the MRT from the CDC. The following sections describe physical layer and/or lightweight security measures to secure the data during communications through the three tiers of Fig. 1, that is, from the BAN/AAL to the AP, from the AP to the NES, and from the NES to the CDC.

Communications Between the Sensors and the AP

The main challenge to secure the transmissions of small sensor nodes (SNs) used for BAN or AAL data measurements is to design security solutions that consume little power, need low processing overhead, and are fast. The privacy of the information sent by these sensors should be protected from eavesdroppers, while the data should be transmitted with low delay and with low energy consumption.

An approach for low energy and fast transmission for sensor networks was proposed in [8]. With this approach, SNs with bad channel conditions on their long range (LR) SN-AP link find neighboring SNs with which they can communicate on the short range (SR) at higher data rates. They break their connection with the AP and communicate with a nearby SN. This SN, in turn, finds another SN to relay its data to the AP if it does not have high channel gain on its link with the AP; otherwise, it maintains its LR link with the AP. In this way, a multi-hop tree is built with few SNs connected to the AP on the LR, acting as cluster heads (CHs) relaying the data of the other SNs connected to them on the SR. This approach was shown in [8] to lead to large energy savings, and reduced transmission delay, since several SR multi-hop transmissions at high data rates can transmit the data faster than one LR link at low data rate. The approach of [8] can be extended to accommodate physical layer security by resorting to channel-aware encryption (CAE) with bit flipping [9].

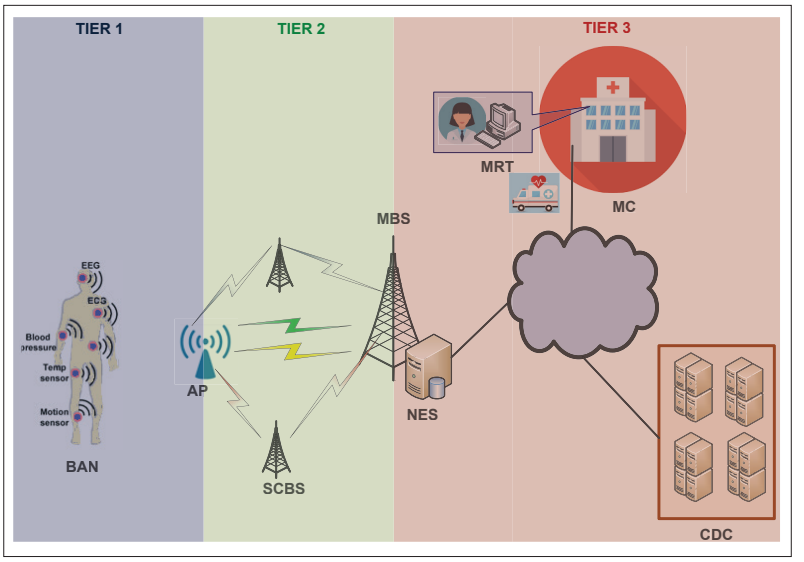

FIGURE 1. Proposed mHealth IoT framework.

With bit flipping, an SN estimates its channel gain on the SN-AP link , for example, through pilot signals transmitted by the AP. If the calculated channel state information (CSI) exceeds a certain threshold, the SN flips its transmitted data, thus sending a "1" instead of a "0," and vice-versa. If the CSI is below the threshold, the data is sent without flipping. Although the decision for flipping or not depends on the CSI on the SN-AP link, the actual data transmission occurs on the multi-hop SR links with the neighbor SNs or CHs, except on the CH-AP link since the CHs aggregate the data before sending it to the AP. To detect the flipping patterns, an eavesdropper must know the channel gains on each SN-AP link. Consequently, it will be hard for the eavesdropper to guess the flipping patterns, since they are dynamically changing with the channel conditions.

Figure 2 presents simulation results using Matlab. A rectangular area of size 25m x 25m is considered, where the distribution of the sensors is assumed to follow a uniform distribution. The origin (lower left corner) of this area is assumed to be located at a distance d_{LR} m from the AP and at a distance d_E from an eavesdropper. The thresholds are selected to be equal to −70dB and −80dB for d_{LR} = 30m and 50m, respectively. The channel model includes pathloss, with a pathloss constant of −128.1dB and a pathloss exponent equal to

3.76, in addition to lognormal shadowing with an 8dB standard deviation, and Rayleigh fading.

The flipping thresholds were determined by empirical evaluation; they correspond to approximately the average channel gain between the SNs and the AP at the specified distances d_{LR}. Results are averaged over 50 iterations. In each iteration, new random SN locations are determined and 50 slow fading (shadowing) realizations are considered. For each of these iterations, 50 fast fading realizations are assumed. Hence, the results are averaged over 50x50x50 = 125000 fading realizations.

Figure 2 shows the percentage of SNs that the eavesdropper can correctly assume the status of their transmission, whether flipped or not. Since the eavesdropper cannot know the channel gain on a given SN-AP link, the only way to try to "guess" the flipping patterns is to consider the channel gain between the SN and the eavesdropper itself. The eavesdropper could estimate this CSI from the SN's transmissions, and compare it to the flipping threshold (assuming this threshold is known to the eavesdropper). If the channel gain of the SN-eavesdropper link is above the threshold, the eavesdropper would assume that the transmissions are flipped. Fig. 2 shows that the guessing percentage of the eavesdropper fluctuates between 48 percent and 53 percent, thus being very close to 50 percent.

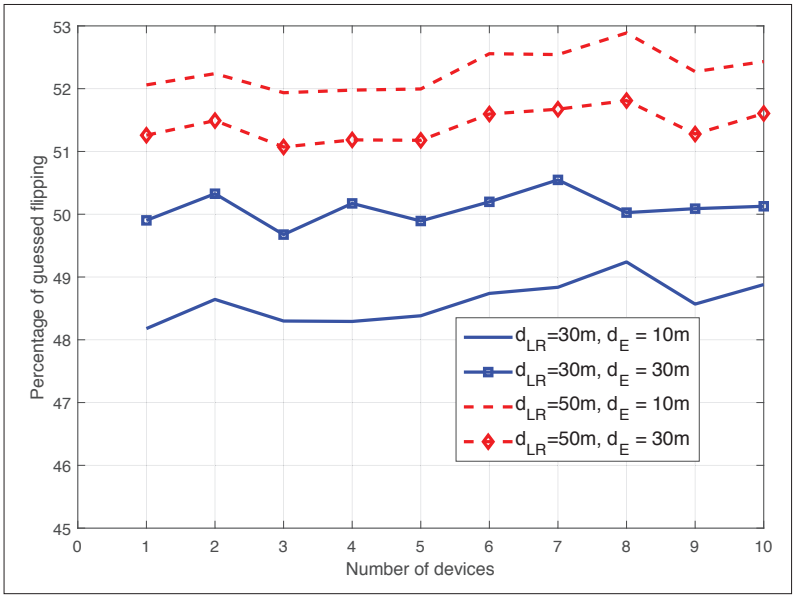

FIGURE 2. Percentage of correct flipping detections by an eavesdropper.

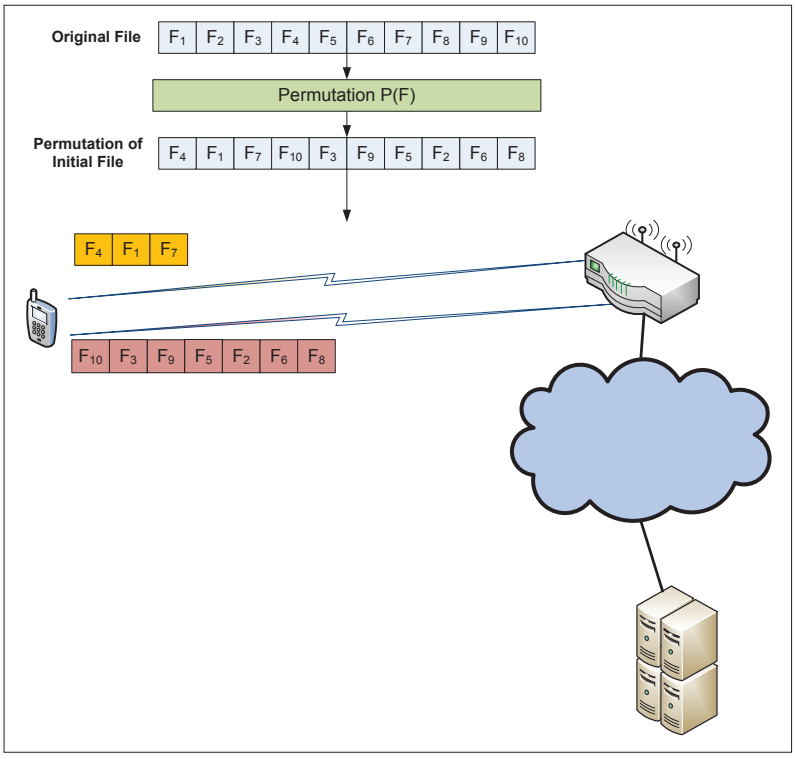

FIGURE 3. Illustrative example for transmitting data over two-resources with the proposed approach.

These results lead to maximum confusion for the eavesdropper. In fact, if the eavesdropper systematically fails to guess any of the transmissions, that is, the percentage of Fig. 2 is 0 percent, then the eavesdropper can systematically flip all the bits that it detected, hence obtaining a guessing percentage of 100 percent. Obviously, the other extreme with 100 percent guessing rate is ideal for the eavesdropper. Consequently, a flipping rate of 50 percent and a guessing rate of 50 percent lead to maximum confusion to the eavesdropper and maximum security for the transmitted data based on the channel-aware encryption physical layer security technique, since the eavesdropper cannot know which transmissions were guessed correctly and which were not.

Although in Fig. 2 fixed thresholds were assumed, the value of each threshold is different depending on the distance. In practice, the AP assists the SNs in order to know the threshold, so that approximately 50 percent bit flipping is achieved to confuse the eavesdropper. The AP can measure the average channel quality with the SNs, then it can determine the threshold and share it with the SNs. However, sending the threshold unencrypted can allow the eavesdropper to potentially capture it. Nevertheless, although the eavesdropper can estimate the channel state between itself and a given SN, it cannot know the CSI over each SN-AP link. Since the threshold is used for this latter link, knowing it at the eavesdropper does not change much. However, for added security, lightweight encryption can be used to encrypt the thresholds.

For example, the method proposed in [10] can be used. It is based on using channel information between sender and receiver to derive a secret key used for encrypting orthogonal frequency division multiplexing (OFDM) data specifically designed for IoT networks. The key changes dynamically as the channel conditions change between the sender and receiver. The approach of [10] can be used to encrypt the whole data, not just the flipping thresholds, whenever the capabilities of the devices allow the use of lightweight encryption.

Communications Between the AP and NES

This section discusses the communication between the AP and the NES and/or the nearest BS connected to a NES. Ideally, in a normal situation where no emergency seems imminent, the transmissions can be sent encrypted from the AP to the NES using traditional encryption methods. Whenever the data processing at the NES starts detecting a potential situation where the health of the patient could undergo a certain risk, different measures can be applied to speed up transmissions while maintaining the privacy of the patient and the security of the data. We

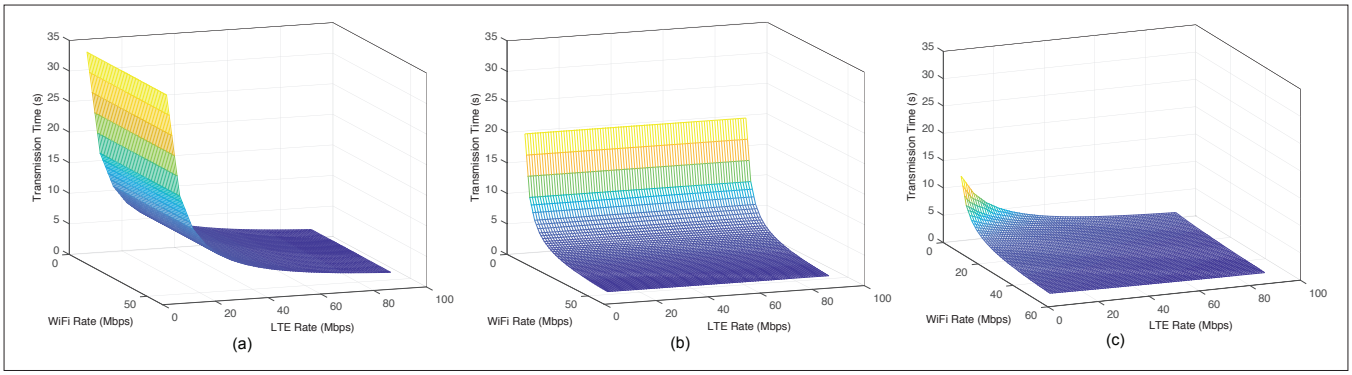

FIGURE 4. Transmission time of single versus two RATs: a) LTE transmission time; b) WiFi transmission time; c) transmission time with 2-RATs.

propose an approach based on "multi-resource" transmission with physical layer security and/or lightweight encryption. By multi-resource we refer to any of the following situations.

Multi-Channel: This corresponds to multiple resource blocks (RBs) in LTE/LTE-Advanced (LTE-A) for example, where each RB represents 12 consecutive orthogonal frequency division multiple access (OFDMA) subcarriers. In the general case, whenever "older" systems are used, "multi-channel" allocation could also correspond to multiple codes in a 3G code division multiple access (CDMA) system or multiple time slots (over the same or different carrier frequencies) in an EDGE system. In the LTE example, each RB would support a data rate that depends on the channel quality over that RB on the AP-BS link.

Multiple Small Cells or Relays: Several small cells could be deployed within the coverage area of a macro BS (MBS) co-located with the NES. In that case, the AP could rely on coordinated multipoint (CoMP) to be connected simultaneously to more than one small cell BS (SCBS), whenever good quality links are available with these SCBSs. Thus, the uplink data transmission can be split over channels provided by multiple SCBSs, who relay this data to the MBS where it is processed at the NES and communicated to the MRT and CDC. The presence of SCBSs and the MBS could be used to separate the uplink and downlink data transmission [11]. In fact, SCBSs can be used for the uplink, thus allowing the AP to achieve high data rates through communications with nearby SCBSs, whereas the control information can be sent directly through the MBS on the downlink, since the MBS generally has higher transmit power than the AP and is also directly connected to the NES.

Multiple Radio Access Technologies (Multi-RATs): Whenever there are multi-RATs available, and the AP can support communications over two or more RATs simultaneously, the data can be split over these RATs in a multihomed fashion, proportionally to the data rates achievable over each RAT, in order to optimize performance by minimizing the transmission time of the measured data. The overall data rate will be equal to the sum of the data rates achievable over each of the RATs [12].

To determine the splitting ratio, we can consider a multi-RAT scenario with two RATs for example, with R_1 and R_2 being the achievable data rates on RATs 1 and 2, respectively. If the size of the data to be transmitted is D bits, then the split that would minimize transmission time is to send $D \cdot R_1/(R_1 + R_2)$ bits over RAT 1 and $D \cdot R_2/(R_1 + R_2)$ bits over RAT 2 [12].

Figure 3 shows an example of two resources where 30 percent of the total data rate is achievable over the first resource and 70 percent is achievable over the second resource. As mentioned previously, these resources could be two LTE RBs, two RATs, or two different paths to the MBS, for example, through two SCBSs or two relay stations. The 70-30 ratio example will change as the channel conditions change on the LTE RBs, on the wireless links of the RATs, or over the various AP-SCBS links. Fig. 4 shows an example where two RATs are available: LTE and WiFi. The achievable rates on each RAT vary depending on the channel conditions over that RAT. Considering a file of size 100 Mbits, Fig. 4 shows the transmission time needed when (a) LTE only is used, (b) WiFi only is used, and (c) both RATs are used simultaneously. Clearly, the multi-RAT case leads to significantly reduced delays.

In addition to splitting the data, Fig. 3 shows a scrambling of the transmitted data over multiple parts using a certain permutation vector, then sending the scrambled data over the multiple resources. This is a lightweight encryption approach as the measured data is grouped into a file and split into parts that are transmitted unencrypted. However, they are scrambled according to a certain permutation vector that needs to be exchanged between the AP and the NES. This vector can be transmitted encrypted, with the encryption keys exchanged using a three-way handshake as detailed in [12] for two RATs. Then, as long as the emergency situation persists, the data can be scrambled according to this vector, with the split varying dynamically over the multiple resources depending on the channel conditions. In this case, an eavesdropper would not only have to guess the permutation vector through brute force attack, but also has to determine the splitting ratio over the multiple resources. Since this ratio depends on the channel conditions between the AP and the receivers (whether SCBSs or the MBS), it will be very difficult for an attacker to guess it. In fact, an eavesdropper could determine the channel conditions between itself and the BSs, but it will not be able to determine these channel conditions between the AP and the BSs. Furthermore, the permutation vector can be changed periodically, which makes the eavesdropper's task even more difficult. Besides, as soon as the emergency situation is appropriately handled by the MRT, transmissions can revert to normal operation where more advanced cryptographic techniques are used.

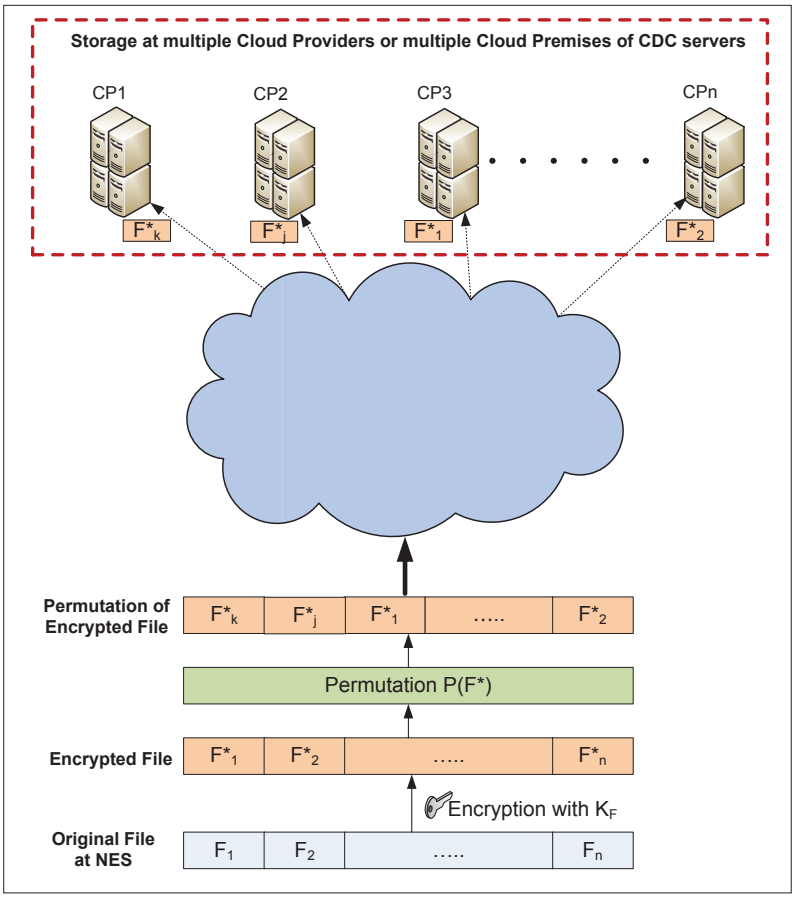

FIGURE 5. Storing a file on the cloud with the proposed approach.

A typical scenario where this approach can be implemented in AAL scenarios with video transmission is the subdivision of source coded video frames into I, P, or B frames that are generally transmitted according to a certain order as per the H.264/H.265 video coding standards. For example, P frames in a group of pictures (GOP) cannot be decoded without the I frame and the previous P frames. Using multiple resources for transmission along with scrambling of the various frames using a secret permutation vector would be an efficient approach to protect the privacy of the monitored patient.

Secure Storage and Retrieval at the CDC

This section discusses the storage of data received at the NES in the CDC, in addition to its retrieval from the CDC by the MRT. In the framework of Fig. 1, the data measured by the BAN/AAL sensors and received at the NES is processed, and in case no imminent risk is detected, it is stored on the cloud. This section presents a secure approach for cloud storage that maintains the privacy of the patients and the integrity of the data regardless of the measures that are usually taken by cloud providers. In addition, as discussed in the previous section, whenever an emergency occurs, NES communicates directly with the MRT and provides real-time measurements with lightweight encryption. Nevertheless, a copy of this information can be stored temporarily at the NES and then stored later in the CDC, when the emergency ends, using the approach described in this section.

Storing Data in the CDC

The NES receives the data from the AP, and collects the measurement data from each of the transmitting sensors. Whenever this data is retrieved and processed, it is stored into data files and encrypted. Afterwards, the various parts of the file are scrambled according to some pseudorandom permutation vector. Finally, each part is stored at servers located at different CPs. The data storage process is shown in Fig. 5. It should be noted that in Figs. 5 and 6, the term "CP" is used to denote either a "cloud provider" or "cloud premise." The former scenario corresponds to offloading the management of large amounts of data to cloud providers, with the MC still being responsible for the privacy of its patients. The latter case corresponds to a data center owned and controlled by the MC, with an aggregation of servers, that can preferably be located at different cloud premises, to avoid the risks of storing the data at a single location. The CPs can store all the health records of the patient (medical history, X-Ray images, and so on), that can be uploaded by the MC/MRT, and not just the data sent by the NES.

In both cases, the main objective is to spread the risk over multiple servers at different data centers on the cloud. Even if cloud providers implement various security features to protect their clients' data , the MC is still responsible for its patients' privacy, and thus can adopt the approach described in this section as an additional security layer. It should be noted that this approach does not incur additional storage costs. However, redundancy can be incorporated into the encryption process for additional protection, through the secret sharing approach. With this approach, the correct retrieval of $k < n$ parts of the file can lead to the correct recovery of the whole file, even if $(n - k)$ parts were lost at certain CPs [13]. The method in Fig. 5 can be implemented with and without secret sharing, at the cost of having a larger number of parts to store and thus larger storage space when secret sharing is used [14].

Retrieving Data from the CDC

When a user at the MC wants to retrieve the medical records stored at the CPs, it navigates through the appropriate software to select a given filename. Then, the different parts of the file are retrieved from the CPs, sorted in the correct order, and decrypted. However, to be able to implement these steps, the system needs to know the encryption key (assumed symmetric and also used for decryption) and the permutation vector. This information is stored securely in two separate tables that can be located in two different servers controlled by the MC. The process is described in Fig. 6. For added security, the filename is stored in hashed format. The first table contains the encryption key. The second table contains the permutation vector (encrypted with the key stored in the first table), along with hashed versions of the file H(F) and the encrypted file H(F*), used to check the integrity of the file's data after retrieval from the CPs.

To access these parameters in the two tables, the corresponding entry is identified through the hash of the filename entered by the user. The first table contains the hash of the filename concatenated with the character string "Table 1", whereas

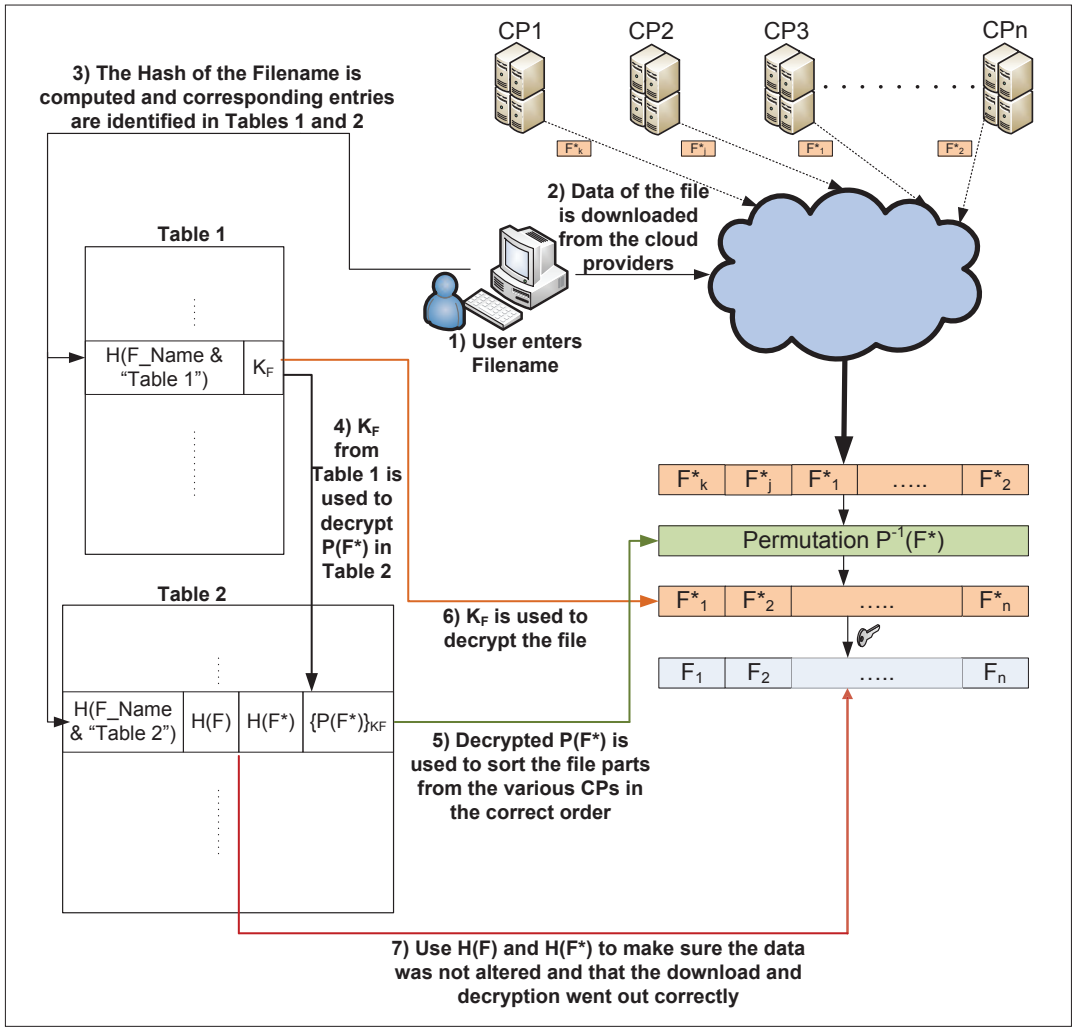

FIGURE 6. Retrieving a file from the cloud with the proposed approach.

the second table contains the hash of the filename concatenated with "Table 2". The purpose of the concatenation is to have the entries of the same file look different in the two tables. (Thus, any predefined strings can be concatenated with the filename.) In this way, in the unlikely event where the servers containing both tables are compromised, the attacker would not be able to identify the entries corresponding to the same file, which leads to increased protection. The attacker needs to know both the key from Table 1 and the permutation vector from Table 2, and has to be able to retrieve the file parts from the various CPs.

Conclusions and Security Analysis of the Proposed Methods

In this article, a holistic framework for data transfer from the patient to the hospital in mHealth IoT systems was presented, and subdivided into three tiers. In each tier, appropriate measures were proposed for securing the data and protecting the privacy of the patients. The proposed methods were analyzed and discussed. They range from physical layer security techniques designed for low portable sensors, to combining traditional encryption methods with additional procedures at the cloud data center where the medical records are stored.

At Tier 1, the bit flipping approach is used to combat eavesdropping and thus protect confidentiality of the data and privacy of the patients. Jamming attacks are hard to perform since the jammer has to determine the location of the AP inside the home to jam it; nevertheless, they can still be mitigated by directing the main beam of the AP antenna toward the sending SNs (through beamforming). In addition, sensor measurements generally include the measurement time, so replay attacks are rendered useless in this case. The SNs generally authenticate themselves with the AP using existing techniques, thus preventing impersonation attacks by attackers sending fake data to the AP.

Similarly, at Tier 2, the proposed approach over multiple resources mitigates eavesdropping, and the impact of jamming attacks at the BS can be reduced by beamforming between the BS and the transmitting AP. Replay attacks can be mitigated by appending a timestamp or nonce to the permutation vector exchanged between the AP and BS. In addition, authentication using existing methods precedes communication between the AP and BS, which should allow the BS to verify the authenticity of the AP.

The approach provided at Tier 3 for securing the data at CDC ensures confidentiality through encryption and permuted storage at different CPs, integrity through the use of hash values of the file to make sure the data has not been changed, and

For added security, the filename is stored in hashed format. The first table contains the encryption key. The second table contains the permutation vector (encrypted with the key stored in the first table), along with hashed versions of the file H(F) and the encrypted file H(F*), used to check the integrity of the file's data after retrieval from the CPs.

The proposed approach is implemented by the MC on top of all the security measures implemented by CPs, in order to maintain control over its patients' data and protect their privacy. Thus, this approach is very robust and makes it hard for any attacker to tamper with the data.

availability since authorized personnel having the appropriate access rights can access the data after logging in and being authenticated. Although it can be implemented in a private cloud at the MC or in a public cloud, it is mostly convenient in the public cloud case. Privacy issues in private or public clouds have been addressed in the existing literature, for example, [15]. However, the proposed Tier 3 approach can be implemented in addition to any security measures implemented by CPs. Each CP can provide security services to its customers by encrypting the data, providing backup storage, adding redundancy, deploying intrusion detection systems and firewall, and so on. The proposed approach is implemented by the MC on top of all the security measures implemented by CPs, in order to maintain control over its patients' data and protect their privacy. Thus, this approach is very robust and makes it hard for any attacker to tamper with the data. In fact, if an attacker manages to access the data at one of the CPs, it is extremely difficult to access it at all others, access the two tables with the hashed file name, and get the correct decryption keys! The worst that could happen is the loss of data when an attacker manages to penetrate a CP's network and deletes the data, but privacy is not compromised in this case. This can be resolved by adopting the secret sharing method (e.g., see [13]) that can be used in conjunction with the proposed approach to provide redundancy (as mentioned in the discussion of Fig. 5).

Acknowledgment

This work was made possible by NPRP grant No. 10-1205-160012 from the Qatar National Research Fund (a member of the Qatar Foundation). The statements made herein are solely the responsibility of the authors. The authors would like to thank the editor and the reviewers for their comments that helped to enhance the quality and clarity of the article.

References

[1] P. Kumar and H.-J. Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," *Sensors,* 2012, no. 12, pp. 55–91, doi: 10.3390/s120100055.

[2] K. Abualsaud, A. Mohamed, and M. Mahmuddin, "Survey on Wireless Body Area Sensor Networks for Healthcare Applications: Signal Processing, Data Analysis and Feedback," *Proc. 3rd Int'l. Conf. Computing and Informatics, ICOCI2011*, Indonesia, 8–9 June, 2011.

[3] J. Wan *et al.*, "Internet of Things for Ambient Assisted Living: Challenges and Future Opportunities," *Proc. Int'l. Conf. Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pp. 354357, Nanjing, China, Oct. 2017.

[4] S. Sindhu, S. Vashisth, and S.K. Chakarvarti, "A Review on Wireless Body Area Network (WBAN) for Health Monitoring System: Implementation Protocols," *Communications on Applied Electronics (CAE)*, Foundation of Computer Science FCS, New York, USA, vol. 4, no. 7, Mar. 2016, pp. 16–20.

[5] S. M. R. Islam *et al.*, "The Internet of Things for Health Care: A Comprehensive Survey," *IEEE Access*, vol. 3, June 2015, pp. 678–708.

[6] H. Subedar and K. El-Khatib, "Privacy and Security Concerns for Health Data Collected Using Off-the-Shelf Health Monitoring Devices," *Proc. IEEE 11th Int'l. Conf. Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2015.

[7] ITU-R M.2083, IMT Vision — Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond, ITU Recommendation, 2015.

[8] E. Yaacoub and A. Abu-Dayya, "Multi-Hop Routing for Energy Efficiency in Wireless Sensor Networks," Chapter 8 in the book: *Wireless Sensor Networks — Technology and Protocols*, Ed.: M. Matin, InTech, ISBN 979-953-307-825-9, Sept. 2012.

[9] H. Jeon *et al.*, "Channel Aware Encryption and Decision Fusion for Wireless Sensor Networks," *IEEE Trans. Information Forensics and Security*, vol. 8, no. 4, Apr. 2013, pp. 619–25.

[10] R. Melki *et al.*, "An Efficient OFDM-Based Encryption Scheme Using a Dynamic Key Approach," *IEEE Internet of Things J.*, vol. 6, no. 1, Feb. 2019, pp. 361–378.

[11] F. Boccardi *et al.*, "Why to Decouple the Uplink and Downlink in Cellular Networks and How To Do It," *IEEE Commun. Mag.*, vol. 54, no. 3, Mar. 2016, pp. 110–17.

[12] R. Diba *et al.*, "A Simple Approach for Securing IoT Data Transmitted over Multi-RATs," *Proc. IEEE Int'l. Wireless Commun. Mobile Computing Conf. (IWCMC 2018)*, Limassol, Cyprus, June 2018.

[13] D. Pal *et al.*, "Multilevel Threshold Secret Sharing in Distributed Cloud," *Proc. Int'l. Symposium on Security in Computing and Communication (SSCC2015)*, Kerala, India, Aug. 2015, pp. 13–23.

[14] A. Sakr *et al.*, "A Secure Client-Side Framework for Protecting the Privacy of Health Data Stored on the Cloud," *Proc. IEEE Middle East & North Africa COMMunications Conf. (MENACOMM 2018)*, Jounieh, Lebanon, Apr. 2018.

[15] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," *Proc. IEEE Inte'l. Conf. Dependable, Autonomic and Secure Computing (DASC 2009)*, Chengdu, China, Dec. 2009, pp. 711–16.

Biographies

Elias Yaacoub [S'07, M'10, SM'14] received the B.E. degree in electrical engineering from the Lebanese University in 2002, the M.E. degree in computer and communications engineering from the American University of Beirut (AUB) in 2005, and the Ph.D. degree in electrical and computer engineering from AUB in 2010. Between 2010 and 2014, he worked as a research scientist/R&D expert at the Qatar Mobility Innovations Center (QMIC). Then, he worked at the Arab Open University and as a freelance researcher/consultant before joining Qatar University as associate professor. His research interests include wireless communications, IoT, and physical layer security.

Khalid Abualsaud [M'14, SM'15] received the B.Sc. degree in computer engineering from Al-Azhar University, Egypt, and the M.Sc. and Ph.D. degrees in 2010 and 2015, respectively, from University Utara Malaysia, Malaysia. He is currently with the Department of Computer Science and Engineering, Qatar University. He teaches courses in hardware and software systems. He has more than 25 years of professional experience in information technology. His research interests include health systems, cloud computing, computer network protocols, wireless sensors for Internet of Things applications, and cybersecurity.

Tamer Khattab [M'94, SM'18] received the B.Sc. and M.Sc. degrees in electronics and communications engineering from Cairo University, Giza, Egypt, and the Ph.D. degree in electrical and computer engineering from The University of British Columbia, Vancouver, BC, Canada, in 2007. He joined Qatar University (QU) in 2007, where he is currently an associate professor of electrical engineering. His research interests include physical-layer transmission techniques in optical and wireless networks, information theoretic aspects of communication systems, and MAC layer protocol design and analysis.

Mohsen Guizani [S'85, M'89, SM'99, F'09] received the B.S. (Hons.) and M.S. degrees in electrical engineering and the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He was a professor and the ECE Department Chair with the University of Idaho, USA. He was the Chair of the Computer Science Department, Western Michigan University, and the Computer Science Department, University of West Florida. He is currently a professor with the Department of Computer Science and Engineering, Qatar University. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid.

Ali Chehab received the bachelor's degree in EE from American University of Beirut (AUB) in 1987, the master's degree in EE from Syracuse University in 1989, and the Ph.D. degree in ECE from the University of North Carolina at Charlotte in 2002. From 1989 to 1998, he was a lecturer with the ECE Department, AUB. He rejoined the ECE Department, AUB, as an assistant professor in 2002, and became a full professor in 2014. His research interests include wireless communications security, cloud computing security, multimedia security, trust in distributed computing, low energy very large scale integration (VLSI) design, and VLSI testing.