Computer Networks 000 (2016) 1–11

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring

M. Shamim Hossain[a,*], Ghulam Muhammad[b]

[a] Software Engineering Department, College of Computer and Information Sciences, Riyadh 11543, Saudi Arabia
[b] Computer Engineering Department, College of Computer and Information Sciences, Riyadh 11543, Saudi Arabia

ARTICLE INFO

Article history:
Received 2 August 2015
Revised 6 January 2016
Accepted 8 January 2016
Available online xxx

Keywords:
ECG monitoring
IoT-driven healthcare
Cloud-assisted system
Signal watermarking
Healthcare Industrial Internet of Things (HealthIIoT)

ABSTRACT

The promising potential of the emerging Internet of Things (IoT) technologies for interconnected medical devices and sensors has played an important role in the next-generation healthcare industry for quality patient care. Because of the increasing number of elderly and disabled people, there is an urgent need for a real-time health monitoring infrastructure for analyzing patients' healthcare data to avoid preventable deaths. Healthcare Industrial IoT (HealthIIoT) has significant potential for the realization of such monitoring. HealthIIoT is a combination of communication technologies, interconnected apps, Things (devices and sensors), and people that would function together as one smart system to monitor, track, and store patients' healthcare information for ongoing care. This paper presents a HealthIIoT-enabled monitoring framework, where ECG and other healthcare data are collected by mobile devices and sensors and securely sent to the cloud for seamless access by healthcare professionals. Signal enhancement, watermarking, and other related analytics will be used to avoid identity theft or clinical error by healthcare professionals. The suitability of this approach has been validated through both experimental evaluation, and simulation by deploying an IoT-driven ECG-based health monitoring service in the cloud.

1. Introduction

Today we are witnessing the increased use of smart devices and communication apps in healthcare monitoring, and their influence on the activities of healthcare professionals (doctors, nurses, and hospital administrators), patients, and the healthcare industry. According to Gartner and Forbes, it is estimated that by 2020, the Internet of Things (IoT) will contribute $1.9 trillion to the global economy and $117 billion to the IoT-based healthcare industry [1]. Based on this estimate, it is expected that the Healthcare Industrial IoT (HealthIIoT) will be one of the main players in the Industrial Internet of Things (IIoT)-driven healthcare industry. IIoT has had a remarkable influence across many large and small healthcare industries. As a result, an increasing number of wearable IoT devices, tools, and apps are being used for different monitoring applications (e.g., glucose monitors, ECG monitors, and blood pressure monitors) to avoid preventable death due to hospital or other related errors. The errors may occur before, during, or after hospitalization.

Currently, HealthIIoT is still in its preliminary stages with regards to design, development, and deployment; however, IoT-based solutions are presently displaying a remarkable impact, and carving out a growing market in today's healthcare industry and tomorrow's emerging IIoT-based healthcare monitoring solutions. IIoT has the potential to save 50,000 people each year in the US by avoiding preventable deaths due to hospital error [2]. It

* Corresponding author. Tel.: +966 114676189.
E-mail addresses: mshossain@ksu.edu.sa (M.S. Hossain), ghulam@ksu.edu.sa (G. Muhammad).

http://dx.doi.org/10.1016/j.comnet.2016.01.009
1389-1286/

promises patient well-being and safety by coordinating critical patient information and synchronizing related resources (e.g., healthcare staff, facilities, wearable smart devices to capture real-time patient data such as vital signs, and patient-related electronic information) instantly through interconnected devices and sensors. Research reveals that IoT in the healthcare industry can facilitate better care with reduced costs, reduced direct patient-healthcare staff interaction, and ubiquitous access to quality care [3]. Mohammed et al. developed a remote patient monitoring system using web services and cloud computing [4]. Hassanalieragh et al. discussed the opportunities and challenges of health monitoring and management using IoT [5]. To date, however, no comprehensive study has been published about cloud-assisted IIoT-driven health monitoring.

Safe and high-quality healthcare service is of paramount importance to patients. Accordingly, healthcare data security and patients' privacy are important issues that will have a great impact on the future success of HealthIIoT [17]. One of the major issues in the IIoT-based healthcare system is the protection of privacy. In general, a healthcare service provider receives data from its users (such as patients) and shares them with registered clinics or healthcare professionals. The provider may also distribute the data to health insurance companies and pharmaceutical companies. Moreover, patient data can be vulnerable to hackers during cloud transfer or synchronization with interconnected devices.

Therefore, we need to protect this information from unauthorized access, which may result in the posting of personal information in the public domain, or in interference with essential medical equipment, such as a pacemaker. A security breach of a patient's monitoring devices and data may cause the patient social embarrassment, mental disorders, or adverse physical effects such as a fatal heart attack. Hence, data protection in the form of watermarking and authentication is very important in an IIoT-based healthcare system.

To this end, this paper describes an IIoT-based health monitoring framework, where health monitoring signals are authenticated. As a case study, we have used electrocardiogram (ECG) monitoring, as ECG is an important assessment tool. By continuously monitoring an ECG signal, a healthcare professional can diagnose disease and prescribe medications to avoid preventable death. ECG signals are recorded via portable ECG recording devices at home or outdoors, and sent to smartphones or desktops via Bluetooth technology. On the client side, a smartphone app or desktop software removes unwanted noise from the recorded signal, and embeds a watermark for security and authentication purposes; heartbeat is also monitored using a simple algorithm. The watermarked ECG signal is then transmitted to a cloud server, where temporal and spectral features are extracted and classified using a one-class support vector machine classifier. The classification decision, along with the watermarked ECG, is passed to the desired healthcare professional for analysis. The professional then sends back a decision and prescription to the cloud server. The cloud then notifies the patient. The contributions of the paper are as follows:

- the introduction of a watermark into the ECG signal on the client side, to avoid a security breach in the cloud
- the introduction of a user identification code to provide customized protection of data
- the introduction of a one-class support vector machine classifier in the cloud

The rest of this paper is organized as follows. Section 2 reports some related studies. Section 3 outlines the HealthIIoT ecosystem, followed by a high-level data flow architecture for the HealthIIoT monitoring value chain, and the details of a cloud-supported HealthIIoT-enabled monitoring framework. Section 4 describes a proposed health monitoring approach by considering ECG as healthcare data. Section 5 presents the experimental results and evaluations. Section 6 concludes the paper.

2. Related studies

The IIoT is an innovative technology, directly interconnecting a set of sensors and devices (such as smartphones) to collect, record, transmit, and share data for possible analysis. The IoT has a wide range of emerging applications [4–16]. Among them, the most revolutionary potential application is healthcare monitoring, where patient healthcare data are collected from a number of sensors, analyzed, delivered through a network and shared with healthcare professionals for evaluation of patient care [4–6,10,11,13]. A more comprehensive survey of IoT for healthcare applications can be found in [7]. IoT-enabled healthcare applications, including IoT-driven ECG monitoring, are discussed in the following studies [6,10]. Li et al. [10]. presents a health monitoring service as a platform for ECG monitoring using adaptive learning analysis model to detect abnormalities.

Mohammed et al. developed a remote patient monitoring system using web services and cloud computing [4]. In particular, they designed an Android application for ECG data monitoring and analysis. Data can be further analyzed by third-party software if needed; however, there is no option for the cloud server to extract features and classify the signal to assist the health professional at the time the signal is received. In our proposed framework, the cloud server extracts features and classifies the signal, so that a preliminary analysis decision from the cloud can be sent to the healthcare professionals to facilitate good patient care.

Hassanalieragh et al. discussed the opportunities and challenges of health monitoring and management using IoT [5]. Some challenges include slow processing, handling big data, presence of too much heterogeneous data, and data integrity. In our proposed framework, the ECG signal is watermarked on the client side before transmitting through the Internet to authenticate against any attacks. Data processing is also distributed between the client side and the cloud side to make the overall processing faster.

Jara et al. [8] present a remote monitoring framework using IoT by proposing a protocol, called YOAPY, to create a secure and scalable fusion of multi-modal sensors to record vital signs. A cloud-based speech and face recognition framework was developed to monitor a patient's state remotely [26]. Xu et al. [9] developed a ubiquitous data

Please cite this article as: M.S. Hossain, G. Muhammad, Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.01.009

accessing method in an IoT-based system for emergency medical scenarios. They proposed a semantic data model to store data, and a resource-based data access method to gain control of the data ubiquitously, concluding that their method could be significant to assist decision-making in emergency medical situations.

Zhang et al. [12] introduced an architecture of mobile healthcare networks, incorporating privacy-preserving data collection and secure transmission. The privacy-preserving data collection was achieved using cryptography with secret keys and private keys. Secure transmission was gained using attribute-based encryption, where only authorized users would have access to the data. These methods are generally worthwhile; however, the main problem is computation complexity.

Granados et al. [14] proposed web-enabled gateways for IoT-based eHealth with an option for wired or wireless services. To take advantage of wired gateways in terms of power-efficiency and low cost, the authors used the wired gateways in a small room or building, where movement is restricted. Radio frequency identification (RFID)-based eHealthcare systems were proposed in [15,16]. In [15], the authors proposed a system that would capture the patient's environmental conditions, such as temperature and humidity, by RFID, and transmit them to the cloud for a more detailed understanding of ambient conditions. Catarinucci et al. [16] proposed an IoT-aware architecture to monitor and assess a patient's situation automatically by integrating ultra-high-frequency RFID functionality.

Sawand et al. [18] identified three types of threats in an eHealthcare monitoring system. These are identity threat, where the identity of the patient is lost or stolen, access threat, where an intruder can access the system illegally, and disclosure threat, where confidential medical data are opened via malware or file sharing tools intentionally or unintentionally. They offered some solutions to these threats, including biometric cryptography and an advanced signal processing scheme; however, the authors did not implement these solutions in their paper.

In [19,21], emotion-aware or affective mobile computing frameworks have been proposed, and the authors investigated an architecture named "emotion-aware mobile cloud" (EMC) for mobile computing. Authors in [20] proposed another framework, affective interaction through wearable computing and cloud technology (AIWAC). Recently, Hu et al. [6] introduced the Healthcare Internet of Things (Health-IoT), attempting a bridge between intelligent health monitoring and emotional care of the patient.

To date, we have found no comprehensive study on cloud-assisted IIoT-driven ECG monitoring, where (i) the ECG signal is watermarked on the client side before transmission through the Internet to the cloud, and (ii) the cloud server extracts features and classifies the signal to assist healthcare professionals in providing quality patient care.

3. Proposed cloud-assisted HealthIIoT-enabled monitoring framework

HealthIIoT can revolutionize today's healthcare industry with affordable and quality patient care by adopting a large number of interconnected machines, wearable things (devices and sensors), and cloud-computing technologies to collect patient data in a seamless manner. This HealthIIoT technology will play an important role in a number of health monitoring applications, to form a Healthcare Industrial IoT ecosystem. Fig. 1 describes a comprehensive IIoT-driven healthcare ecosystem. As shown in Fig. 1, one type of stakeholder (e.g., patient with IoT devices and sensors, healthcare professional, hospital or medical research center, social media and family) is connected to another type of stakeholder (e.g., emergency response services, drug industries and pharmacies, smart medical devices and 'Things' industries, environmental and home control services) to form a complex HealthIIoT ecosystem. It also dispatches emergency services to the patient when needed, and orders pharmacy refills. In this ecosystem, interconnected 'Things' (medical devices and sensors) are coordinated. It allows fast transfer of patient information among the stakeholders in a secured manner, such that specific patient data are available only to a designated authorized healthcare team. Finally, cloud-based big data analytic enables analyzing, storing, closely monitoring, and securely sharing the data for further review and medical recommendations, aimed towards fulfilling the promise of Industrial IoT in regard to quality patient care, real-time patient monitoring, and avoiding hospital error.

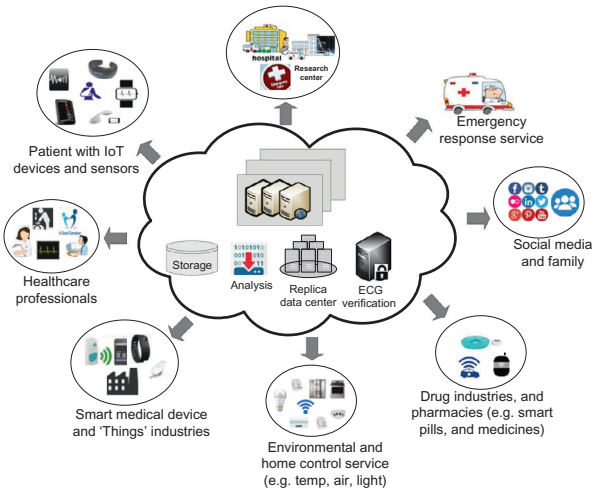


Fig. 1. Conceptual illustration and scenario for HealthIIoT ecosystem.

The Industrial IoT is the combination of big data, IoT, Machine to Machine (M2M) communication, cloud computing, and real-time analysis of data from interconnected sensor devices [22]. The success of HealthIIoT largely depends on the advancement of the cloud-computing technology and big data analytics. It creates a platform for interconnected smart medical devices to operate with large amounts of data (big data) from anywhere at any time. The data are actually generated by a myriad of interconnected smart devices, communication apps, and their usage in healthcare monitoring applications. Data are gathered and analyzed from e-health records, imaging equipment, medical sensors, devices, and smartphones over the cloud. This analysis augments the decision-making power of

Please cite this article as: M.S. Hossain, G. Muhammad, Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.01.009

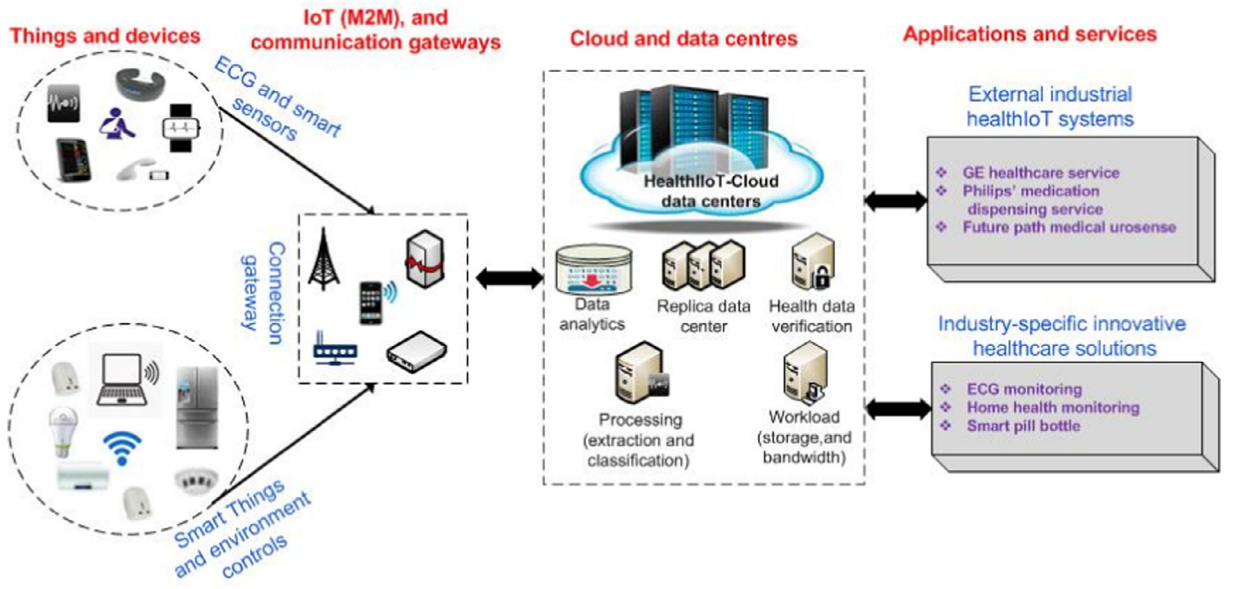


Fig. 2. Data flow architecture for HealthIIoT monitoring value chain.

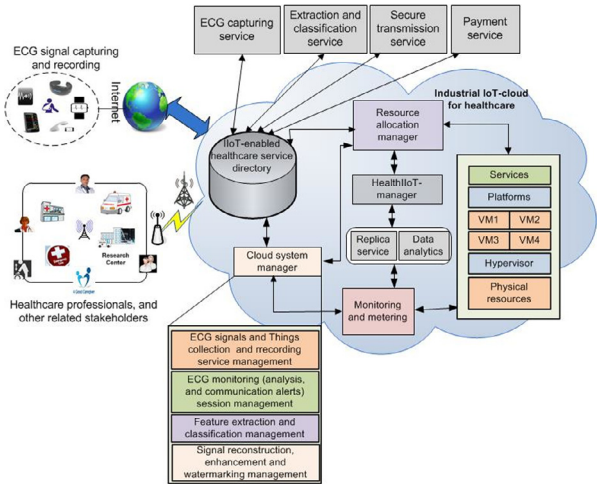


Fig. 3. The proposed HealthIIoT architecture for an ECG monitoring.

healthcare professionals, and helps patients have an active role in managing their personal health.

Fig. 2 outlines how the flow of a patient's healthcare data (e.g., ECG signals) is captured securely; how it is transferred seamlessly through a connection gateway to the cloud data centers for further analysis and processing, such as feature extraction, classification, verification, workload measurement, and big data management. After being processed and securely stored in the cloud, the chain of collected data is either accessed by healthcare professionals, or delivered to external systems for further industry-specific healthcare IoT solutions.

Fig. 3 shows the cloud-assisted IIoT-enabled health monitoring framework. First, the patient's ECG signal is recorded through the connected devices and sensors, and then after possible signal reconstruction, enhancement, and watermarking, it is sent to the cloud-based system using network connections. The cloud system validates this information to check that the patient's information is correct, and then extracts some features, classifies the signal, and redirects it to the assigned healthcare professionals and providers for possible patient care.

The major components of the framework are described below.

Healthcare staff and other related stakeholders: Patients upload their ECG readings through an ECG interface, which is connected to the Internet. After some processing, the ECG reading is stored in the cloud database, where healthcare professionals can access it and review it for possible action based on the uploaded ECG readings.

ECG signal capturing and recording service: This service is used to record and store the ECG signal from different devices and smartphones.

Secure transmission service: The service enables a secure and authenticated transmission of the ECG signal through Internet. To accomplish this, watermarking is embedded into the signal, and later, is extracted to verify the authenticity.

Resource allocation manager: Manages virtual machine (VM) resources and web services.

Cloud system manager: Controls all VMs and allocates suitable resources through the resource allocation manager for each service, such as ECG signal and things collection and record service manager, ECG monitoring session manager, feature extraction and classification manager, and finally, signal reconstruction, enhancement and watermarking manager.

(1) *ECG signal and things collection and record service management*: This web service is responsible for managing the users' data and their related health information, and storing them in the database.

Please cite this article as: M.S. Hossain, G. Muhammad, Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.01.009

(2) *ECG monitoring (analysis and communication alerts) session management*: Responsible for managing and controlling the sessions, in addition to locating, tracking, and evaluating the activities.
(3) *Feature extraction and classification management*: This web service extracts collected data upon running the ECG apps on smartphones, and stores them in a MySQL database before sending them to the HealthI-IoT cloud.
(4) *Signal reconstruction, enhancement, and watermarking*: This web service generates, records, and tracks the performance of the monitoring function.

HealthIIoT manager: Manages all health-related IIoT data by assigning data to different replicated data centers, after verifying the authenticity of the data.

Monitoring and analytics: Analyzes the data by extracting features and applying classification techniques. Calculates and monitors the workload of the framework, such as storage and bandwidth.

Replica service: Because of the growing demand for interconnected medical devices with heterogeneous connectivity, HealthIIoT systems handle large numbers of data requests for accessing patient healthcare. Therefore, datasets need to be replicated in multiple sites and data centers to offer faster data access times. If one or more sites (data centers) are down, healthcare data can be accessed from other nearby sites. Generating replicas also enables the healthcare professionals' ECG file requests to distribute the workload through the replica servers, and avoid performance degradation due to network congestion. Moreover, this ensures faster access, scalability, and a reduction in response time.

IIoT-driven healthcare service directory: Records and stores data from the ECG capturing devices. It also registers and publishes different participating services. It facilitates continuous care for the patients by recording the ECG signal in portable ECG recording devices at home or outdoors, and sends them to smartphones or desktops. Some major elements in this directory are the ECG capturing service, feature extraction and ECG classification service, secure transmission service, and payment service. Healthcare professionals can get access to the ECG data from this directory without visiting the patient.

4. Proposed health monitoring approach

Our proposed health monitoring approach consists of some processing steps, which are signal enhancement, watermarking, feature extraction, ECG analysis, and signal reconstruction. Signal enhancement and watermarking are done on the client side. The work flow of the proposed framework is shown in Fig. 4.

4.1. Signal enhancement

An ECG monitoring system based on the cloud was proposed by Pandeya et al. [23]. In their system, ECG data were collected by mobile devices and were sent to the cloud for analysis. The system was just a prototype, and therefore, problems remained in its fully practical usage in

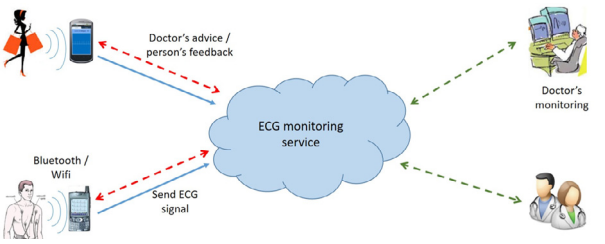


Fig. 4. Overall work flow of the ECG monitoring system in the cloud.

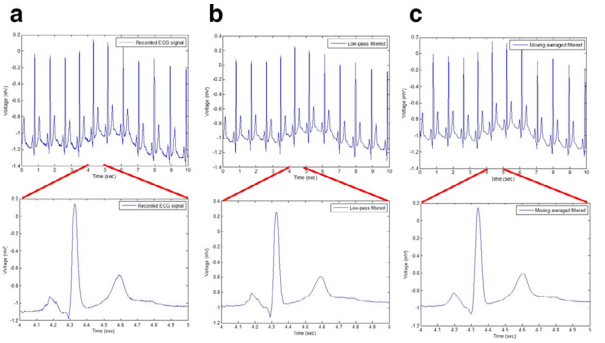


Fig. 5. Effect of low-pass filtering and moving average filtering: (a) the recorded ECG signal, (b) the low-pass filtered signal, and (c) the moving average filtered signal.

term of data collection and transmission. The first issue is to ensure the effectiveness of ECG data collection through mobile devices. Physiological artifacts can be caused by muscular activities that result in small spikes, and by human motion that results in large swings in the recorded data. Non-physiological artifacts can be produced by electrical interference and electrode malfunction. Electrode malfunction is initiated by loose connections, electrode misplacement, low amount of electrode gel, wrong filter setting, fractured wires, etc. Of them, electrode misplacement is a major source of malfunction of ECG data acquisition [24]. Cable misplacement can even result in ECG that resembles cardiac abnormalities like ectopic rhythm [25].

Therefore, in the proposed framework, the recorded ECG signals are enhanced before processing to get rid of some of the common artifacts. In the enhancement stage, the recorded ECG signal is passed through a low-pass filter to suppress the high frequency components that are referred to noise. A 25-point moving average filter is then applied to the output of the low-pass filter to smooth the signal. Fig. 5 shows the effect of low-pass filtering and moving average filtering of a recorded ECG signal. From the figure, we see that the signal looks 'clear' after applying these two filters. This preprocessing step is necessary to correctly detect electrical waves in the ECG signal, which is critical for subsequent online analysis and monitoring.

4.2. Peak R detection

To process the ECG signal, determining peak R is required. These two attributes in ECG signal are very important for ECG signal analysis. To detect R, we use analytical wavelet transform (AWT) [28]. A complex AWT

Please cite this article as: M.S. Hossain, G. Muhammad, Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.01.009

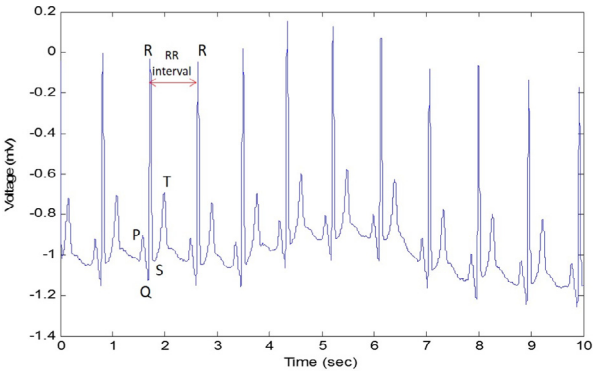


Fig. 6. Detected peak R.

can be expressed by Eq. (1).

$$\phi(\omega) = \omega^n e^{-\omega}, \quad \omega \geq 0 \\ = 0, \quad \omega < 0 \tag{1}$$

The above equation is obtained by combining a Hilbert transform and a wavelet transform. In Eq. (1), n is the derivative order. The advantage of using the above equation is that it combines the time-frequency location of a wavelet transform with the local slope information of the Hilbert transform.

After applying complex AWT, we apply thresholding and look for persistent lines. The local maximums are identified in the wavelet transform signal to find R (see Fig. 6).

4.3. ECG watermarking

The next stage is to watermark the signal to protect it from forgery. Watermarking is a procedure to embed some information in a signal without distorting the visibility or credibility of the signal for ownership claim. It has mainly two parts: watermark embedding and watermark extraction for verification. Embedding watermark in the ECG signal will ensure the authenticity of the ECG signal transmitted over the cloud. We adopt a simple yet efficient strategy of watermarking that has rarely been used for ECG signals. The watermarking is based on discrete wavelet transform (DWT)-singular value decomposition (SVD) [25,27]. The study in [25,27] did not use DWT-SVD watermarking scheme in ECG signals, e-healthcare or cloud-based systems. DWT is a multi-resolution technique that decomposes a signal into different levels of time and frequency. In the proposed step, we use a two-level DWT that decomposes the signal into three subbands: approximation subband L2, second-level detail subband H2, and first-level detail subband H1. SVD is a matrix factorization technique that decomposes a matrix into three matrices. If a rectangular matrix A of size $I \times J$ is the input, the output will be two orthogonal matrices and one diagonal matrix as follows (Eq. (2)):

$$A_{I\times J} = U_{I\times I} S_{I\times J} V^T_{J\times J} \tag{2}$$

where $U^T U = I_{I\times I}$and $V^T V = I_{J\times J}$, which means that U and V are orthogonal. S is a diagonal matrix, whose diagonal entries are singular values and arranged in descending order. These singular values are always real numbers. The computation of SVD is stable against round-off errors. The fact that a slight variation in the values of S matrix does not affect the perception of an ECG signal, watermark bits can be added to the singular values of S to get a robust watermarking.

The watermark is an image consisting of the client's registered ID in image format of size $I \times J$, where $I > J$. The detailed procedure is described as follows.

Step 1. Normalize the watermark image matrix by 255.

$$Im_{i,j} = \left\{watermark_{i,j}/255;\ 0 \leq i \leq I, 0 \leq j \leq J\right\}$$

Step 2. Apply SVD on the normalized matrix. The resultant S_w is a square matrix of size $I \times I$.

$$Im = U_w \cdot S_w \cdot V_w^T$$

Step 3. Multiply S_w by a watermark intensity factor, α.

$$S_{w\alpha} = \alpha \cdot S_w$$

Step 4. Store U_w, $V_w{}^T$, and α for watermark extraction. Use $S_{w\alpha}$for watermark embedding.

Step 5. Divide the ECG signal into N number of beats. The beat duration is 0.6 s and peak R is located at 40% of the duration.

Step 6. Step 6: Apply two-level DWT on each beat. Take H2 (detail coefficients at level 2) for watermark embedding. Store L2 (approximation coefficient) and H1 (detail coefficients at level 1) for reconstruction of watermarked ECG signal.

Step 7. Form a matrix G using H2 of all the frames. The number of rows corresponds to the number of beats of the signal.

Step 8. Apply SVD on matrix G. The resultant S_s is a square matrix of size $N \times N$.

$$G = U_s \cdot S_s \cdot V_s^T$$

Step 9. A new matrix, S_{new}, of size $N \times N$ is formed by using matrices $S_w\alpha$ and S_s.

$$S_{new} = \begin{cases} S_{w\alpha}(n,n) + S_s(n,n), & \leq n \leq I \\ S_s(n,n), & (I+1) \leq n \leq N \end{cases}$$

Step 10. Using U_s, $V_s{}^T$, and S_{new}, perform inverse SVD to get matrix G'.

$$G' = U_s \cdot S_{new} \cdot V_s^T$$

Step 11. Using $L2$, G', and H1, perform inverse DWT to get watermarked ECG signal.

The watermark image can be reconstructed by using the following steps.

Step 1. Subtract S_s from S_{new} to get S_{im}. S_{im} should be equal to S_w if the watermarked speech signal is not under attack.

$$S_{im} = S_{new}(n,n) - S_s(n,n), 1 \leq n \leq I$$

Step 2. Apply inverse SVD to get the normalized watermark.

$$Im' = U_w \cdot S_{im} \cdot V_w^T$$

Step 3. Get the watermark image by multiplying the values by 255 and dividing by α.

$$Im'_{i,j} = \left\{ Im'_{i,j} \times 255/\alpha; \quad 0 \le i \le I, 0 \le j \le J \right\}$$

If there is no attack, $Im'_{i,j}$ will be the same as the watermark image.

The enhancement stage and the watermark stage are performed on the client side. Once the ECG signal is watermarked signal is transmitted to the cloud, where it is processed to extract features and to analyze.

4.4. Feature extraction

Several features are extracted from the ECG signal in the cloud server. The features include heartbeat rate (HBR), durations of *P* wave, PR interval, QRS complex, and QT interval, and the shape (inverted or not, and peaked or not) of *T* wave. These are total of seven features.

The HBR is determined by the inverse of the time difference between RR intervals and expressed as beats per minutes (bpm) as expressed by Eq. (3).

$$HBR(bpm) = \frac{60}{RR \text{ intervals (s)}} \tag{3}$$

An unusual p-wave may represent ectopic atrial pacemaker. p-wave longer than 80 ms can indicate atrial enlargement. A PR interval smaller than 120 ms may be a cause of Wolf–Parkinson–White syndrome, while larger than 200 ms may indicate a first degree of atrioventricular block. QRS complex wider than 120 ms suggests a disruption of the heart's conduction system, or sever hyperkalemia. A prolonged corrected QT interval ($>$ 440 ms) risks for ventricular tachyarrhythmia, while an unusual short interval may indicate severe hypercalcemia. For a corrected QT interval, QT interval should be normalized by the square root of the RR interval. Inverted T waves may be syndromes of myocardial ischemia, or high intracranial pressure, while a peaked (determined by the variance of the wave) T wave may indicate hyperkalemia or early myocardial infarction.

Spectral features are also calculated by applying the Fast Fourier Transform (FFT) to each beat. A 512-point FFT is used and first half of the magnitude output is retained. The 256 bins are linearly resampled to F number of bins, where F is varied to 10, 20, 30, and 40. These F number of features are appended to previously mention seven features for classification.

4.5. One-class support vector machine (OCSVM) classification

OCSVM is a one-class classification technique, where the feature space is mapped to a higher dimensional space so that a hyperplane maximizes the distance between the hyperplane and the origin. In a typical SVM, there are two classes, while in OCSVM, there is only one class in the training. OCSVM is used in this framework, because it can detect the personal ECG as abnormal or not. For the experiments, MIT-BIH database was used [29]. The first group of 48 records are divided into two sets: first set comprises of first 3 min of data in each record for training, while second set consists of remaining 27 min of data in each record for testing.

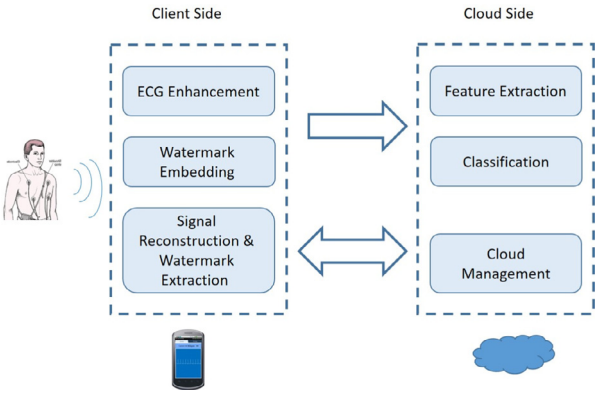


Fig. 7. ECG signal modules on the client side and the cloud side.

Fig. 7 shows the separation of the modules in the client side and the cloud side.

5. Experimental results and evaluation

Several experiments were performed to validate the proposed IoT-enabled ECG signal monitoring. They are described in details in the followings sections.

5.1. Watermarking performance

The performance of the ECG watermarking was measured in terms of imperceptibility, and robustness against attacks [30]. Imperceptibility is a measure of how much the signal is distorted perceivably. To measure imperceptibility, we used signal-to-noise ratio (SNR), which is an objective measurement. SNR is defined by Eq. (4).

$$SNR_{dB} = 10 \log_{10} \frac{P_s}{P_s - P'_s} \tag{4}$$

where, P_s and P_s are the power of original ECG signal and the watermarked ECG signal, respectively. Another closely related metric is peak SNR or PSNR. In PSNR, the numerator of logarithm in Eq. (4) is replaced by the square of the maximum value of the pixel in the original watermark image.

With regard to robustness against attack, we considered two common attacks, which are additive white Gaussian noise (AWGN), and filtering of type low-pass, high-pass, and band-pass. The measurement were obtained by using a correlation factor, η, which is computed by using Eq. (5).

$$\eta(w, w') = \frac{\sum_{i=1}^{N} w_i w'_i}{\sqrt{\sum_{i=1}^{N} w_i{}^2} \sqrt{\sum_{i=1}^{N} w'_i{}^2}} \tag{5}$$

where, w and w' are the original and extracted watermark, respectively, N is the number of pixels in the watermark image. η takes the value between 0 (no relation) and 1 (perfect relationship).

Fig. 8 shows the obtained SNR and PSNR in dB using the proposed DWT-SVD based watermarking. The proposed scheme was compared with another popular method,

Please cite this article as: M.S. Hossain, G. Muhammad, Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.01.009

Fig. 8. PSNR (dB) and SNR (dB) using the proposed DWT-SVD based watermarking, which is compared with DWT-DCT based watermarking.

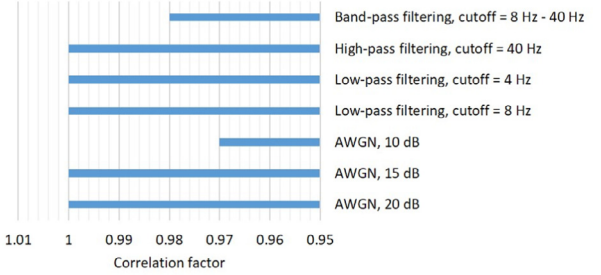


Fig. 9. Correlation factor after different types of attack.

which is DWT-DCT (discrete cosine transform)-based [31]. From the figure, we see that the proposed watermarking has a very good SNR and PSNR, and it outperforms the DWT-DCT based method.

Fig. 9 shows correlation factor, η, after different types of attacks. The attacks were applied in the cloud server. The attacks included band-pass filtering with passband between 8 Hz and 40 Hz, high-pass filtering with cutoff frequencies of 40 Hz, low-pass filtering with cutoff frequencies of 8 Hz, and 4 Hz, and AGWN of 20 dB, 15 dB, and 10 dB. From the figure, we see that almost in all the cases the correlation factor was 1, which indicates the robustness of the proposed watermarking algorithm. For a comparison with DWT-DCT based method, the correlation factor of DWT-DCT based watermarking is 0.98 for AWGN 20 dB attack.

5.2. Classification performance

Two types of classification experiments were performed: one with the MIT-BIH database as mentioned in the classification section, and the other with actual data recorded through the proposed framework. Fig. 10 shows the average classification accuracy using the two databases. Seven features correspond to features without spectral features. With 37 features, the accuracy reached up to 87.7% with MIT-BIH database and 90.4% with private database. Fig. 11 shows the time spent from transmitting the data to the cloud, extracting features, to classifying the data. One instance, three instances, and fives instances of servers

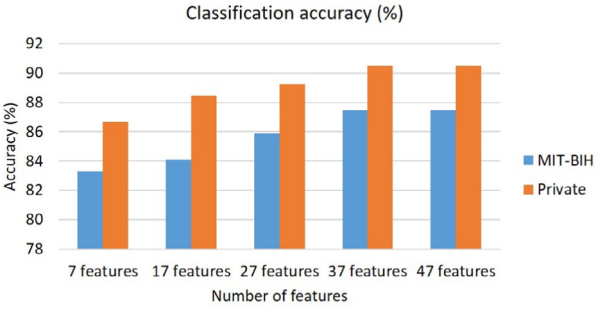


Fig. 10. Classification accuracy of the proposed framework.

Fig. 11. Time requirement of the proposed framework.

Table 1
Storage configurations.

Config.	Node capacity (GB)	Total storage (TB)	Relative storage (%)
1	[50–1000]	20.75	80
2	[50–500]	15	60
3	[50–200]	12	46.75
4	[20–50]	4.5	18
5	[10–20]	3.5	15

were used in the cloud. With five instance server, only around two seconds were needed while using 37 features.

5.3. Workload of the IIoT-enabled health monitoring service

To evaluate the proposed IIoT-based for health monitoring, we used a Java-based simulator program. The simulation environment includes cloud topology and an ECG data access pattern by a healthcare professional. To reduce overhead and latency, ECG files are replicated so that healthcare professionals can get access to the desired data for a specific patient from neighboring data centers. We have used a similar multi-tier cloud topology structure [32] with multiple data centers using the following storage configurations of replica servers as shown in Table 1, where the capacity of relative storage ranges from 15% to 80%. While submitting a task, a number of ECG files are requested for access to patient data. The sequence of file request is handled by three access patterns, such as Zipf distribution, random distribution, and Gaussian distribution. The framework is evaluated in terms of ECG data access by healthcare professionals. The access time refers to the time of completion of all tasks for the ECG file

Please cite this article as: M.S. Hossain, G. Muhammad, Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.01.009

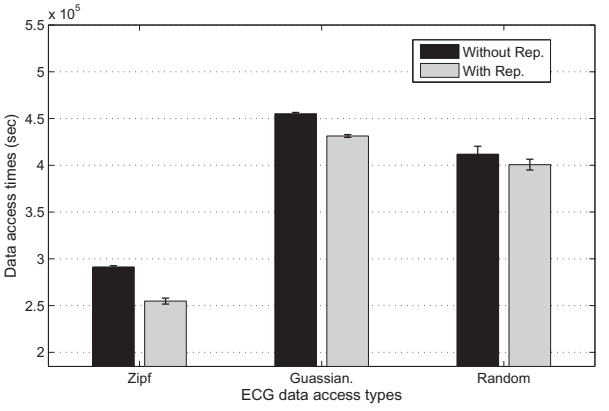


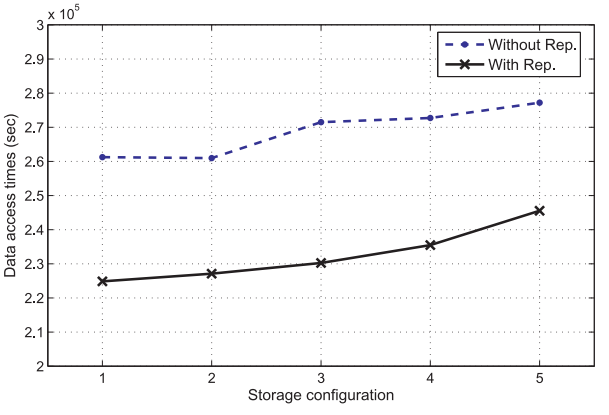
Fig. 12. ECG data access time using relative storage capacity 80%.

requests. The objective is to reduce ECG data access time. In the simulation, constant data access rate is considered. The total data access time is a summation of time needed by the disk to find a replica of an ECG file from the replica data center disk and network communication latency for replica transmission. The data access time, $Access(R)$, is calculated using the following model, Eq. (6):

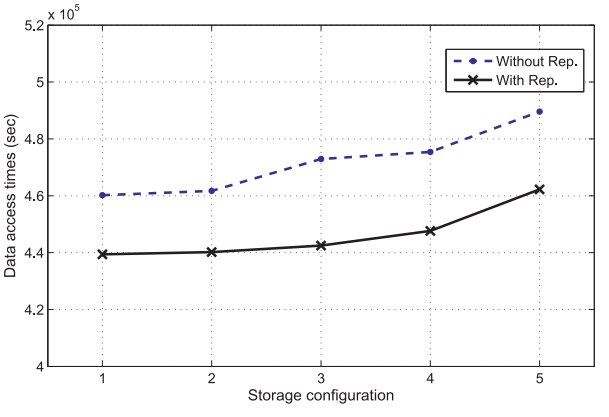
$$Access(R) = \sum_{v \in G} f(v,n) \cdot D_{latency}(v,r) + G_{network}(v,r) \quad (6)$$

where, $G = (V, L)$ is undirected tree structure of the cloud, R is a set of replica data centers, n is an ECG file or sample, $f(v,n)$ is data access frequency by a healthcare professional (v) for an ECG file (n), r is lowest ancestor of v in R, $D_{latency}$ is disk access latency, and $G_{network}$ is network communication latency.

We compared ECG data access time by integrating replication and without considering replication approaches to the proposed framework. Fig. 12 compares the ECG data access times by considering replication and non-replication strategies for the first storage configuration, as shown in Table 1. In the majority of cases, a storage configuration with replication resulted in a shorter ECG data access time than a configuration without replication. Replicated datasets in several data center locations decrease the data access time because healthcare professionals have access to the required ECG data for a particular patient from a nearby site. Moreover, the storage capacity of the

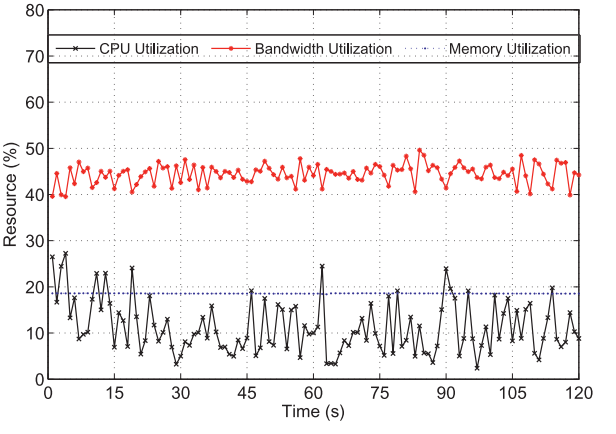


(a) Zipf.

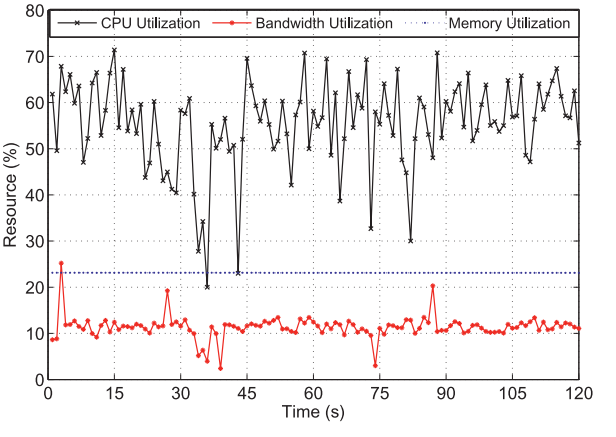


(b) Gaussian

Fig. 13. ECG data access time comparison for all storage configuration.



(a) ECG Transmission



(b) ECG Capturing

Fig. 14. Workload for ECG monitoring.

Please cite this article as: M.S. Hossain, G. Muhammad, Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.01.009

data centers favors using the replication approach. With a reduced storage capacity, the ECG data access times for both approaches (i.e., with and without replication) are increased, but by different magnitudes. Fig. 13 shows the execution times for Zipf and Gaussian distributions for all the storage configurations listed in Table 1. Shorter access times for all storage configurations are correlated with using the replication approach.

Fig. 14 shows the workload of the main services used for health monitoring of the proposed HealthIIoT framework. We have concentrated on three key services: ECG capturing service, transmission service, and extraction or classification service. To understand the features of those workloads as they relate to ECG monitoring, the run-time characteristics of those workloads are collected by running the proposed health monitoring prototype on the Amazon Elastic Computing Cloud (EC2). For this purpose, we rented a VM with an Intel®*Core*^{TM} 2 Duo, DDR3 ECC RAM at 2.53 GHZ, 1 Gbps bandwidth, and 4.0GB memory, running Windows Server 2010. The performance monitor of Windows has been used to record the resource consumptions of those workloads for memory, CPU, and network bandwidth utilizations.

6. Conclusion

IIoT-driven healthcare monitoring is an emerging healthcare service that may potentially revolutionize the healthcare industry in terms of improving access to patient information, and offer quality patient care through continuous monitoring from anywhere at any time, through a multitude of devices. With HealthIIoT, healthcare professionals may be able to access patient information, store it, and analyze it in a real-time manner to monitor and track the patient. However, interconnected wearable patient devices and healthcare data (such as ECG signals) are subject to security breaches. To this end, this paper describes a cloud-integrated HealthIIoT monitoring framework, where healthcare data are watermarked before being sent to the cloud for secure, safe, and high-quality health monitoring. Future work will involve testing the proposed HealthIIoT monitoring framework for data security and notification functions, as well as implementing a test trial with real-world patients and health professionals.

Acknowledgment

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia for funding this work through the research group project no. RGP 228.

References

[1] T. J. McCue, $117 billion market for internet of things in healthcare by 2020, forbes, April 2015, Retrieved from http://www.forbes.com/sites/tjmccue/2015/04/22/117-billion-market-for-internet-of-things-in-healthcare-by-2020.
[2] S. Schneider, How the industrial internet of things can save 50,000 lives a year, January 2015, Industrial Internet Consortium, Retrieved from http://blog.iiconsortium.org/2015/01/how-to-industrial-internet-of-things-can-save-50000-lives-a-year.html.
[3] J. Bresnick, Healthcare internet of things driving global market growth, June 2015, Retrieved from http://healthitanalytics.com/news/healthcare-internet-of-things-driving-global-market-growth.
[4] J. Mohammed, A. Thakral, A.F. Ocneanu, C. Jones, C.H. Lung, A. Adler, Internet of Things: Remote patient monitoring using web services and cloud computing, in: Proceedings of the 2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom), and IEEE Cyber, Physical and Social Computing (CPSCom), Taipei, 1–3 September 2014, pp. 256–263.
[5] M. Hassanalieragh, A. Page, T. Soyata, G. Sharma, M. Aktas, G. Mateos, B. Kantarci, S. Andreescu, Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges„ in: Proceedings of the IEEE International Conference on Services Computing, 2015, pp. 285–292.
[6] L. Hu, M. Qiu, J. Song, M.S. Hossain, Software defined healthcare networks, IEEE Wirel. Commun. Mag. 22 (6) (2015) 67–75.
[7] S.M.R. Islam, D. Kwak, M.H. Kabir, M. Hossain, K.S. Kwak, The Internet of Things for health care: A comprehensive survey, IEEE Access 3 (2015) 678–708.
[8] J. Jara, M.A. Zamora-Izquierdo, A.F. Skarmeta, Interconnection framework for mHealth and remote monitoring based on the Internet of Things, IEEE J. Sel. Areas Commun. 31 (9) (2013) 47–65.
[9] B. Xu, L.D. Xu, H. Cai, C. Xie, J. Hu, F. Bu, Ubiquitous data accessing method in IoT-based information system for emergency medical services„ IEEE Trans. Ind. Inf. 10 (2) (2014) 1578–1586.
[10] P.Y. Li, L. Guo, Y. Guo, Enabling health monitoring as a service in the cloud, in: Proceedings of the IEEE International Conference on Utility and Cloud Computing, October 2014, pp. 81–84.
[11] M.S. Hossain, Cloud-supported cyber-physical framework for patients monitoring, IEEE Syst. J. (2015), doi:10.1109/JSYST.2015.2470644.
[12] K. Zhang, K. Yang, X. Liang, Z. Su, X.S. Shen, H.H. Luo, Security and privacy for mobile healthcare networks: From a quality of protection perspective, IEEE Wirel. Commun. Mag. 22 (4) (2015) 104–112.
[13] M.S. Hossain, G. Muhammad, Cloud-based collaborative media service framework for health-care, Int. J. Distrib. Sensor Netw. 2014 (2014) 11. Article 858712.
[14] J. Granados, A.M. Rahmani, P. Nikander, P. Liljeberg, H. Tenhunen, et al., Web-enabled intelligent gateways for eHealth internet-of-things, in: R. Giaffreda, et al. (Eds.), Internet of Things. User-Centric IoT, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), 2015, pp. 248–254.
[15] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, G. Marrocco, RFID technology for IoT-based personal healthcare in smart spaces, IEEE Internet Things J. 1 (2) (2014) 144–152.
[16] L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, M.L. Stefanizzi, L. Tarricone, An IoT-aware architecture for smart healthcare systems, IEEE Internet Things J. 2 (6) (2015) 515–526, doi:10.1109/JIOT.2015.2417684.
[17] D. bib17, Securing the industrial Internet of Things, Inf. Syst. Secur. Assoc. (ISSA) J. (2015) 24–30.
[18] A. Sawand, S. Djahel, Z. Zhang, F. Naït-Abdesselam, Toward energy-efficient and trustworthy eHealth monitoring system, China Commun. 2 (1) (2015) 46–65.
[19] M. Chen, Y. Zhang, Y. Li, S. Mao, V. Leung, EMC: Emotion-aware mobile cloud computing in 5G, IEEE Netw. 29 (2) (2015) 32–38.
[20] M. Chen, Y. Zhang, Y. Li, M. Hassan, A. Alamri, AIWAC: Affective interaction through wearable computing and cloud technology, IEEE Wirel. Commun. Mag. 22 (1) (2015) 20–27.
[21] M. Chen, NDNC-BAN: Supporting rich media healthcare services via named data networking in cloud-assisted wireless body area networks, Inf. Sci. 284 (10) (2014) 142–156.
[22] M. Chen, J. Wan, S. Gonzalez, L. Xiaofei, V.C.M. Leung, A survey of recent developments in home M2M networks, IEEE Commun. Surv. Tutor. 16 (1) (2014) 98–114.
[23] S. Pandeya, W. Voorsluys, S. Niua, A. Khandoker, R. Buyyaa, An autonomic cloud environment for hosting ECG Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the Internet-of-Things data analysis services, Future Gen. Comput. Syst. 28 (2012) 147–154.
[24] H. Tam, J. Webster, Minimizing electrode motion artifact by skin abrasion, IEEE Trans. Biomed. Eng. 24 (1977) 134–139.
[25] V. Batchvarov, M. Malik, A. Camm, Incorrect electrode cable connection during electrocardiographic recording, Europace 9 (2007) 1081–1090.
[26] M.S. Hossain, G. Muhammad, Cloud-assisted speech and face recognition framework for health monitoring, Mob. Netw. Appl. 20 (3) (2015) 391–399.

Please cite this article as: M.S. Hossain, G. Muhammad, Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.01.009

[27] M. Ali, C.W. Ahn, An optimized watermarking technique based on self-adaptive DE in DWT-SVD transform domain, Signal Process. 94 (2014) 545–556.
[28] H. Zhao, F. Wang, Z. Chen, J. Liu, A robust audio watermarking algorithm based on SVD-DWT, Elektron. Ir Elektrotech. 20 (1) (2014) 75–80.
[29] J.M. Lilly, S.C. Olhede, On the analytic wavelet transform, IEEE Trans. Inf. Theory 56 (8) (2010) 4135–4156.
[30] G.B. Moody, R.G. Mark, The impact of the MIT-BIH arrhythmia database, IEEE Eng. Med. Biol. Mag. 20 (3) (2001) 45–50.
[31] J. Grody, L. Brutun, Performance evaluation of digital audio watermarking algorithms, Proceedings of the Forty-third IEEE Midwest Symposium on Circuits and Systems, 2000, pp. 456–459.
[32] M. Shorfuzzaman, A. Alelaiwi, M. Masud, M.M. Hassan, M.S. Hossain, Usability of a cloud based collaborative learning framework to improve learner's experience, Comput. Hum. Behav. 51 (2015) 967–976.

M. Shamim Hossain is an Associate Professor of SWE, CCIS, at King Saud University, Riyadh, KSA. He received his Ph.D. degree in Electrical and Computer Engineering from the University of Ottawa, Canada. His research interests include serious games, cloud and multimedia for healthcare, big data for multimedia, social media, and biologically inspired approach for multimedia and software system. He has authored and co-authored around 100 publications including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters. He has served as a member of the organizing and technical committees of several international conferences and workshops. Recently, he received outstanding paper award from an IEEE Conference. He has served as co-chair, general chair, workshop chair, publication chair, publicity chair, and TPC for over 12 IEEE and ACM conferences and workshops. He is on the editorial board of Springer Multimedia tools and Applications (MTAP). Currently, he serves as a lead guest editor of IEEE Transactions on Cloud Computing, IEEE Communication Magazine, Elsevier Future Generation Computer Systems, Elsevier Computers and Electrical Engineering, Springer Multimedia tools and Applications (MTAP), Springer Cluster Computing. Previously, he served as a lead guest editor of IEEE Transactions on Information Technology in Biomedicine (currently JBHI), Springer Multimedia tools and Applications, and Hindawi International Journal of Distributed Sensor Networks. He is a Senior Member of IEEE and a member of ACM.

Ghulam Muhammad is an Associate Professor in the department of Computer Engineering, College of Computer and Information Sciences at the King Saud University, Riyadh, KSA. He received his Ph.D. in Electrical and Computer Engineering from Toyohashi University and Technology, Japan in 2006. His research interests include serious games, cloud and multimedia for healthcare, resource provisioning for big data processing on media clouds and biologically inspired approach for multimedia and software system, image and speech processing. He has authored and co- authored more than 120 publications including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters.

Please cite this article as: M.S. Hossain, G. Muhammad, Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.01.009