Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System

Haiping Huang, *Member, IEEE*, Tianhe Gong, Ning Ye, Ruchuan Wang and Yi Dou

***Abstract*—The convergence of Internet of Things (IoT), cloud computing and wireless body-area networks (WBANs) has greatly promoted the industrialization of e-/m-healthcare (electronic-/mobile-healthcare). However, the further flourishing of e-/m-Healthcare still faces many challenges including information security and privacy preservation. To address these problems, a healthcare system (HES) framework is designed that collects medical data from WBANs, transmits them through an extensive wireless sensor network infrastructure and finally publishes them into wireless personal area networks (WPANs) via a gateway. Furthermore, HES involves the GSRM (Groups of Send-Receive Model) scheme to realize key distribution and secure data transmission, the HEBM (Homomorphic Encryption Based on Matrix) scheme to ensure privacy and an expert system able to analyze the scrambled medical data and feed back the results automatically. Theoretical and experimental evaluations are conducted to demonstrate the security, privacy and improved performance of HES compared with current systems or schemes. Finally, the prototype implementation of HES is explored to verify its feasibility.**

***Index Terms*—Internet of Things, healthcare system, wireless sensor network, security, privacy protection, key distribution**

I. Introduction

THE rapid technological convergence of Internet of Things (IoT), wireless body-area networks (WBANs) and cloud computing has caused e-healthcare (electronic-healthcare) to emerge as a promising information-intensive industrial application domain that has significant potential to improve the quality of medical care [1]. Therefore, how to achieve medical data collection, transmission, processing and presentation has become a critical issue in e-healthcare applications, in which a variety of wireless sensor nodes and terminal devices play important roles in network data aggregation and communications. Furthermore, the evolution of m-health (mobile-health) technology has made it possible for people to gather information concerning their health status easily, anytime and anywhere using smart mobile devices [2]. However, these medical data consist of personal private information that should not be susceptible to eavesdropping or malicious tampering during transmission. Therefore, the privacy protection and secure transmission of e-/m-healthcare (electronic-/mobile-healthcare) data has drawn more attention from many researchers. A secure and reliable e-/m-healthcare framework to defend against hostile attacks and threats is highlighted for available applications of the informationalized healthcare industry. Moreover, a challenge remains concerning how to effectively process the ever-growing volume of healthcare data and protect data privacy but maintain low sensor network overhead [3]. Due to the resource-strained characteristics (such as limited power) of mobile devices and sensors, the tradeoff between efficiency and privacy or security must be further balanced for the commercial promotion of e-/m-healthcare. Therefore, a meaningful concern of this paper is the design of a feasible, efficient and privacy-guaranteed e-/m-healthcare information system employing wireless sensor networks.

Most current e-/m-healthcare systems require doctors (or system administrators) to participate in medical information processing, which brings two problems: low effectiveness caused by manual operations and privacy breaches due to doctors' acquaintance with users' private data. A medical expert system that can automatically analyze users' scrambled private data but minimize doctors' participation can address these two problems, particularly for the application of general physical examinations. Even with perfect access control mechanisms, frequent human intervention will always cause a higher risk of privacy disclosure in e-/m-healthcare. As a major component of e-/m-healthcare systems, the development of a medical expert system is another focus of this paper.

Various implantable and network-oriented medical devices such as medical sensors and body-area network components are considered in e-/m-healthcare systems [4]. However, a practical market survey on medical instruments illustrates that most current wearable medical devices and nodes cannot be directly

This work was supported by the National Natural Science Foundation of P. R. China (No. 61672297, 61373017 and 61373138), the Key Research and Development Program of Jiangsu Province (Social Development Program, No.BE2015702), Postdoctoral Foundation (No. 2015M570468 and 2016T90485), The Sixth Talent Peaks Project of Jiangsu Province (No. DZXX-017), Jiangsu Natural Science Foundation for Excellent Young Scholar(No. BK20160089).

H. P. Huang, T. H. Gong, N. Ye and R. C. Wang are with the School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: hhp@njupt.edu.cn; g405252865@163.com; yening@njupt.edu.cn; wangrc@njupt.edu.cn; corresponding author: H. P. Huang, phone: 86-13813826704; fax: 86-25-83492152; e-mail: hhp@njupt.edu.cn).

Y. Dou is with the Department of Computing, The Hong Kong PolyTechnic University, Hung Hom, Kowloon, Hong Kong (e-mail: csydou@comp.polyu.edu.hk).

linked with smart mobile terminals through 4G or Wi-Fi. Additional network infrastructure or gateway devices are required to enable interconnection between such devices and nodes. Even when the mobile phone has been directly equipped with medical sensors or biometric information-sensing components, current technology limits it to collecting only one or two data items. Furthermore, many e-/m-healthcare architectures fail in terms of the feasibility of data transmission directly from WBANs to wireless personal area networks (WPANs) or the Internet because implementation difficulty and the need for network connectivity are not considered. Therefore, this paper focuses on designing a distinctive e-/m-healthcare architecture in which medical sensing data from a wireless body-area intranet is relayed via an extended wireless sensor network infrastructure and then scattered to personal area networks or the Internet. This architecture also emphasizes security and privacy preservation during data transmission while guaranteeing data availability.

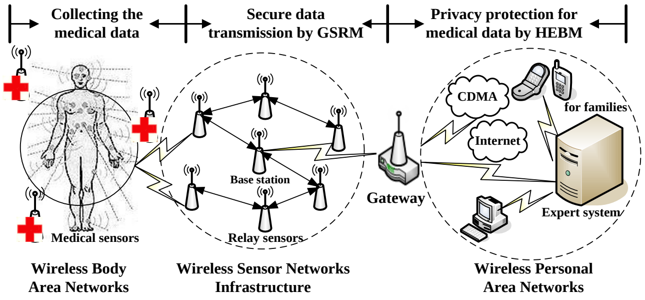

Collecting the medical data
Secure data transmission by GSRM
Privacy protection for medical data by HEBM
CDMA
Internet
for families
Base station
Gateway
Expert system
Medical sensors
Relay sensors
Wireless Body Area Networks
Wireless Sensor Networks Infrastructure
Wireless Personal Area Networks

Fig. 1. The architecture of HES

As shown in Fig. 1, the distinction between our e-/m-healthcare architecture and others lies in secure, efficient and privacy-ensured data transmission in a wireless sensor network infrastructure and data release via gateway to WPANs (including the expert system or servers) through protocol conversion among IEEE 802.15.4, 802.11 or CDMA. The architecture of Fig. 1 not only addresses the problem of communications between implantable medical nodes and WAPNs but also takes full advantage of the characteristics of a low-cost, easily deployed and scalable wireless sensor network infrastructure. Furthermore, this architecture permits authorized families and guardians to obtain users' health information anytime and anywhere via mobile handheld devices.

Our major contributions can be described as follows: (1) the e-/m-healthcare architecture "HES", based on wireless sensor networks, is proposed. HES incorporates an expert system designed to achieve an automatic analysis of scrambled medical data and "minimal participation" of authorized doctors in general physical examinations. (2) A key distribution scheme based on a group send-receive model "GSRM" is proposed for secure data transmission in wireless sensor networks, and a privacy-preserving strategy of homomorphic encryption based on matrix "HEBM" is advanced to disrupt the original medical data before release onto WPANs. (3) Theoretical analysis and simulation experiments are conducted to verify that the performance of the proposed designs can indeed achieve security, efficiency, feasibility, network delay-toleration and connectivity simultaneously. (4) The implementation of HES includes the development of medical sensors, correlative software and network system.

The remainder of this paper is organized as follows. Section II describes GSRM and HEBM for security and privacy-guarantee, respectively. Security proof, performance analysis and comparisons are presented in section III. Section IV introduces the implementation of HES. In Section V, we provide an overview of related work. Finally, the conclusion and future directions are summarized in Section VI.

II. Security and Privacy Scheme Design of HES

A. GSRM for data secure transmission

To ensure the security of medical data transmitted in wireless sensor networks, key distribution schemes and block encryption methods are required. A reasonable key distribution scheme can improve efficiency by decreasing the resource consumption of memory, computation and communication of sensors. Because most sensor nodes have only a single connection path, a key distribution scheme based on a group send-receive model (GSRM) and AES is proposed.

Related definitions:

Definition 1: A set of nodes is a group of send-receive, if and only if:

(1) All the sensor nodes are included within a circle whose radius is *R* (half of the sensor communication range).

(2) The count of nodes in the group is an even number, denoted by 2ξ (ξ=1, 2 ...).

(3) Approximately one-half of the nodes (denoted by *Ss*) only send messages. The other one-half (denoted by *Sr*) only receive messages.

(4) A leader node exists that is elected by one given algorithm in a group.

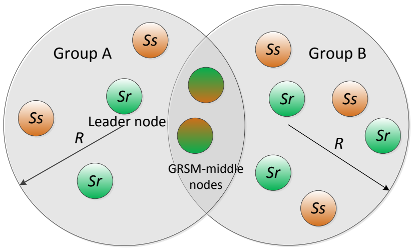


Fig. 2. Group send-receive and GSRM-middle nodes

In Fig. 2, there exist two groups named "Group A" and "Group B", respectively.

Definition 2: A node is a GSRM-middle node if and only if the node simultaneously belongs to at least two adjacent groups and can send (or receive) messages from one group to the other or receive (or send) messages in opposite directions.

As shown in Fig. 2, two nodes are GSRM-middle nodes, not only in Group A but also in Group B. Generally, there should be more than one GSRM-middle node to make the network unobstructed.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2017.2687618, IEEE Transactions on Industrial Informatics

Definition 3: GSRM-level is a function $L(d)$ and is relative only to the distance d between a sensor node and the base station. The function $L(d)$ has the following attributes:

(1) $\forall d \in \Re$, there must be $L(d) \in \aleph$, where $\Re$ denotes the set of real numbers and $\aleph$ denotes the set of natural numbers.

(2) $\forall d_1 < d_2$, there must be $L(d_1) \le L(d_2)$.

For example, there are two nodes denoted by "A" and "B" with GSRM-level values $L(d_A)$ and $L(d_B)$, respectively. If $L(d_A)=L(d_B)$, "A" and "B" are in the same level; else if $L(d_A)=L(d_B)+1$, "A" is the next level farther than "B" from the base station.

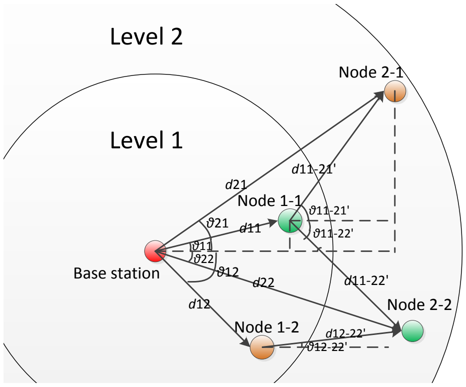


Fig. 3. The calculation of GSRM-level value

We assume that the base station is at the center of the wireless sensor network infrastructure and that its GSRM-level is 0. Quantities of sensor nodes are deployed uniformly around the base station. Different areas are divided according to GSRM-level values, and each subarea is an annulus in Fig. 3. $L(d)$ can be defined as $[d/R]$, $[d^{k_1}/R]$ or $[k_2(e^d-1)/R]$ when considering a practical environment, where k_1 and k_2 are both constants and k_1>1, k_2>0. For the convenience of experimental evaluations, we use the function $L(d)=[d/R]$.

<u>Group construction:</u>

When a wireless sensor network is initialized (the procedure can be completed off-line for security considerations), the base station can be considered the origin of a polar coordinate system. A node that can communicate with the base station within one hop, for example Node 1-1 in Fig. 3, calculates the distance d_{11} between itself and the base station and the departure angle to the base station θ_{11}, where $d_{11}>0$, $-\pi \le \theta_{11} \le \pi$. Then, it sends the two parameters d_{11} and θ_{11} to all its neighbor nodes in one hop. Node 2-1 in Fig. 3, for example, also calculates the relative distance d_{11-21}' and the departure angle θ_{11-21}' between itself and the corresponding sender. Then, Node 2-1 can calculate the following:

$$\begin{cases} d_{21} = \sqrt{(d_{11}\cos\theta_{11} + d_{11-21}'\cos\theta_{11-21}')^2 + (d_{11}\sin\theta_{11} + d_{11-21}'\sin\theta_{11-21}')^2} \\ \theta_{21} = \arctan(\dfrac{d_{11}\sin\theta_{11} + d_{11-21}'\sin\theta_{11-21}'}{d_{11}\cos\theta_{11} + d_{11-21}'\cos\theta_{11-21}'}) \end{cases} \quad (1)$$

However, every node whose GSRM-level is greater than 0 will most likely receive more than one message with distance and angle parameters. For example, in Fig. 3, Node 2-2 received two messages $\{d_{11}, \theta_{11}\}$ and $\{d_{12}, \theta_{12}\}$ from Node 1-1 and 1-2, respectively. Their relative distance and departure angle corresponding to Node 1-1 and Node 1-2 are $\{d_{11-22}', \theta_{11-22}'\}$ and $\{d_{12-22}', \theta_{12-22}'\}$, respectively. To avoid cumulative errors, the mean value will be calculated.

The values of d_{22} and θ_{22} can be obtained from (2).

Once the distance between the base station and every node is calculated, the node is able to learn its accurate GSRM-level value $L(d)$. The above-mentioned calculation will be repeated until arrival at the edge of a sensor network, when all GSRM-level values have been completed. The construction procedure is described as Algorithm 1.

$$\begin{cases} d_{22} = \dfrac{1}{2}[\sqrt{(d_{11}\cos\theta_{11} + d_{11-22}'\cos\theta_{11-22}')^2 + (d_{11}\sin\theta_{11} + d_{11-22}'\sin\theta_{11-22}')^2} + \\ \sqrt{(d_{12}\cos\theta_{12} + d_{12-22}'\cos\theta_{12-22}')^2 + (d_{12}\sin\theta_{12} + d_{12-22}'\sin\theta_{12-22}')^2}] \\ \theta_{22} = \dfrac{1}{2}[\arctan(\dfrac{d_{11}\sin\theta_{11} + d_{11-22}'\sin\theta_{11-22}'}{d_{11}\cos\theta_{11} + d_{11-22}'\cos\theta_{11-22}'}) + \arctan(\dfrac{d_{12}\sin\theta_{12} + d_{12-22}'\sin\theta_{12-22}'}{d_{12}\cos\theta_{12} + d_{12-22}'\cos\theta_{12-22}'})] \end{cases} \quad (2)$$

Algorithm 1: The generation of GSRM groups

```
1:  The base station starts the procedure of building a group from those nodes whose GSRM-level values are 0; it also acts as the leader of its own group;
2:  for each leader node in group
3:      The leader node will record the count of its neighbor nodes with the same GSRM-level values and the count of its neighbor nodes whose GSRM-level values are greater than its value by one; the former is denoted by $\xi_{q0}$ and the latter is denoted by $\xi_{q1}$;
4:      if $\xi_{q0}>\xi_{q1}$
            This leader node will discard ($\xi_{q0}-\xi_{q1}$) nodes with the same level that are the farthest nodes from itself;
            if ($\xi_{q0}-\xi_{q1}$)>$z_1$, where $z_1$ is a given constant;
                One of the dropped nodes will be chosen as the leader to build a new group according to the procedure mentioned above;
            Else
                The dropped nodes will become isolated nodes;
            end if
        Else
            This leader node will discard ($\xi_{q1}-\xi_{q0}$) nodes with the next level that are the farthest nodes from itself;
            $z_2$ of those dropped nodes will be chosen as leaders to build their respective new groups according to step 3, where $z_2$ is a constant;
        end if
    end for
```

<u>Key distribution:</u>

After the execution of Algorithm 1, the leader node of each group will distribute keys for member nodes. If the total number of one group's nodes is 2ξ, the total number of keys that will be distributed is ξ. For example, in a group, when ξ=2 (including two *Ss* nodes, Ss_1 and Ss_2, and two *Sr* nodes, Sr_1 and Sr_2), two keys will be generated and represented as key_1 and key_2. Furthermore, a hash function $h(x)$ is chosen to participate in the key distribution. The keys used for different sessions in this example are displayed in TABLE I.

TABLE I

KEYS USED IN DIFFERENT SESSIONS WHEN ξ=2

Send node	Receive node	Key to use
Ss_1	Sr_1	$h(key_1 \parallel key_2)$
Ss_1	Sr_2	$h(key_1)$
Ss_2	Sr_1	$h(key_2)$
Ss_2	Sr_2	$h(key_2 \parallel key_1)$

Based on TABLE I, we can derive other keys when $\xi=\xi'>2$ from the given recursion rules. If we have learned the key $h[key(i, j)]$ used by Ss_i and Sr_j when $\xi=\xi'-1$, then we can derive the current key "$key_{\xi'}$" dispatched for the session between Ss_i and Sr_j when $\xi=\xi'>2$. Two random integers r_1 and r_2 ($r_1, r_2 \in [1, \xi'-1]$) will be generated for the calculation of "$key_{\xi'}$". Furthermore, when $\xi=\xi'+1$, the recursion rules will be repeated. All cases of keys used for different sessions in one group are displayed in TABLE II when $\xi=\xi'>2$.

TABLE II
ALL CASES OF THE KEYS USED FOR DIFFERENT SESSIONS WHEN $\xi=\xi'>2$

Send node	Receive node	Key to use
Ss_i ($i<\xi'$)	Sr_j ($j<\xi'$)	$h[key(i, j)]$
Ss_i ($i<\xi'$ and $i \neq r_2$)	$Sr_{\xi'}$	$h[key(i, r_2) \parallel key_{\xi'}]$
Ss_{r_2}	$Sr_{\xi'}$	$h[key(r_2, r_1) \parallel key_{\xi'}]$
$Ss_{\xi'}$	Sr_j ($j<\xi'$ and $j \neq r_2$)	$h[key_{\xi'} \parallel key(i, r_2)]$
$Ss_{\xi'}$	Sr_{r_2}	$h[key_{\xi'} \parallel key(r_1, r_2)]$
$Ss_{\xi'}$	$Sr_{\xi'}$	$h[key_{\xi'}]$

When a node acquires its session key between itself and another node in the same group, it is allowed to send messages using the key. The GSRM-middle nodes are responsible for communications between two adjacent groups. The medical data collected from WBANs will be encrypted using the keys generated by GSRM. Then, the ciphertext will be decrypted via WSNs symmetrically in the gateway.

Keys will be updated periodically. When the updating occurs, each node in one group generates a random number rd_k for node i and sends it to the leader. The leader updates the session key between node i and node j according to (3) and informs them secretly, where i=1, 2, ..., j=1, 2, ..., and $i \neq j$:

$$Key'(i, j) = h[Key(i, j) \oplus rd_i \oplus rd_j] \tag{3}$$

Due to energy exhaustion or node breakdown, some nodes will be dead after a period of running of WSNs. If the dead node is not a leader, the leader will mark this node a "virtual node" and no keys in the group will be changed. However, other nodes in the group no longer send messages to the dead node. If the dead node is a leader, the election algorithm (Algorithm 1) in the group will be conducted and the new leader will mark the dead leader a "virtual node". If the number of virtual nodes exceeds one-half of the total members in the group, the leader node will delete them and re-distribute the keys in the group. However, if the alive nodes are too few (below a certain threshold) to maintain communications in the group, the group will be destroyed and all alive nodes will rejoin the network by seeking other groups. Specifically, if the dead node is a GSRM-Middle node, the node nearest to it within the communication range of the group will be searched and will replace it; otherwise, if an appropriate neighbor node cannot be found, the group will be destroyed and all living nodes will rejoin the network. If one node leaves the network unconventionally (for example, a capture attack occurs), the leader launches the key updating, generates a random number rd, then sends it confidentially to all other nodes and informs them to update keys for each other according to (4):

$$Key'(i, j) = h[Key(i, j) \oplus rd] \tag{4}$$

When a fresh node applies to join the network, it calculates the value of its GSRM-Level to decide in which group it will participate. Because the balance of the "send or receive" model (i.e., the count of nodes in one group is an even number) will be broken, if a virtual node exists, the fresh node can substitute for it and become the real node. The leader deletes the mark of the virtual node and launches the key updating. However, if no virtual node exists when the fresh node joins the group, the leader will create a virtual node to balance of the "send or receive" model and conduct the key updating.

B. *HEBM for data privacy protection*

Not all homomorphic encryption methods can be directly applied to the e-/m-healthcare system based on WSNs, particularly when considering resource constraints and the requirements of the expert system. To better adapt to the privacy-preserving characteristics of HES, HEBM (Homomorphic Encryption Based on Matrix) is proposed.

We suppose that a user of HES must submit n medical data items from WBANs via the wireless sensor network infrastructure to WPANs and then obtain the results through the automatic analysis of the expert system. Each type of medical data has a normal region, for example, the normal range of human body temperature (armpit) is between 36 degrees Celsius and 37 degrees Celsius, i.e., [36.00℃, 37.00℃]. If HES can examine a total of l types of medical data, the normal region of the ith medical data item (i=1, 2, ..., l) can be represented as [$\min_i$, $\max_i$]. Generally, $\max_i - \min_i < 100$. For the instance of $\max_i - \min_i \geq 100$, we can calculate $s = \left\lceil \frac{\max_i - \min_i + 1}{100} \right\rceil$, where $\lceil x \rceil$ denotes rounding up. Before the medical data of users such as x_i is transmitted from the gateway into WPANs, an operation $x_i = x_i/s$ has be done. For the normal region of the ith medical data item, the operations $\max_i = \max_i/s$ and $\min_i = \min_i/s$ have been done in the expert system.

The expert system proposed in this paper only feeds the results back based on three cases: normal, relatively low or high. For privacy protection, the query results of medical data must be kept secret, which means that attackers can never obtain the factual medical data within the period of validity.

We now define some functions about HEBM as follows:

$\lceil \mathbf{V} \rceil$: Round up each element in **V**.

$\mathbf{M_1}$*$\mathbf{M_2}$: Perform the dot product for two matrices $\mathbf{M_1}$ and $\mathbf{M_2}$; each element of the multiplied result takes the operation of modulo g, where g is a given constant.

addCol(**M**, c_1, c_2, v): After adding the value amplified v times of each corresponding element in column "c_1" of **M**, each element in column "c_2" of **M** takes the operation of modulo g, where g is a given constant.

minusCol(**M**, c_1, c_2, v): After subtracting the value amplified v times of each corresponding element in column "c_1" of **M**, each element in column "c_2" of **M** takes the operation of modulo g, where g is a given constant and the modular arithmetic for a negative number can be denoted by $-a$ mod b=b-a mod b.

Therefore, the privacy transformation process of HEBM for a user's medical data can be described as follows:

Step1: After secure transmission based on GSRM, the medical data of a user can be denoted by an n-dimensional column vector $\mathbf{X}=(x_1, x_2, ..., x_n)^T$. $\mathbf{X}'=\lceil r_a\mathbf{X}\rceil$ is then calculated, where r_a is a random number and $r_a > 100$.

Step2: First, two matrices denoted by **M** and **M'** separately are identity matrices. Second, the random number r_b ($r_b > 1$) and the random prime number g ($g > 10000\cdot\max\{x_i\}\cdot r_a\cdot r_b$) will be generated. Third, three arrays a, b and f will be defined, and the following algorithm will be executed:

```
Algorithm 2: Initialization of Matrix M and M'
for $i$ = 1 to 1000
        Generate two different random integers $a_i$ and $b_i$, in region [1, $n$]; simultaneously generate $f_i$ stochastically in region [0, $g$);
end for
for $i$ = 1 to 1000
        addCol(M, $a_i$, $b_i$, $f_i$);
        minusCol(M', $a_{1001-i}$, $b_{1001-i}$, $f_{1001-i}$);
end for
```

Step3: $\mathbf{M}*\mathbf{X}'$ will be calculated, and then the scrambled data $\{\mathbf{M}*\mathbf{X}', r_b, g\}$ will be transmitted into WPANs.

Step4: Synchronously with Step1 and Step2 in the expert system, an n-dimensional row vector $\mathbf{Y}=(y_1, y_2, ..., y_n)$ is calculated in advance, where $y_i = \dfrac{1}{\max_i - \min_i}$. Then, a matrix **T** is constructed. Each element of **T**'s leading diagonal is equal to $-y_i\cdot\min_i$. The values of the remaining elements of **T** are generated stochastically.

Step5: After receiving the message $\{\mathbf{M}*\mathbf{X}', r_b, g\}$, the expert system calculates $\mathbf{Y}'=\lceil 10000 r_b\mathbf{Y}\rceil$ and $\mathbf{M}*\mathbf{X}'*\mathbf{Y}'$ (an n-dimensional matrix). Then, the message $\{\mathbf{M}*\mathbf{X}'*\mathbf{Y}', \mathbf{T}\}$ will be sent back.

Step6: The received $\mathbf{M}*\mathbf{X}'*\mathbf{Y}'$ will be left multiplied by **M'**, which establishes $\mathbf{M}'*\mathbf{M}*\mathbf{X}'*\mathbf{Y}'=\mathbf{X}'*\mathbf{Y}'=\mathbf{X}'\mathbf{Y}'$ due to $g > 10000\cdot\max\{x_i\}\cdot r_a\cdot r_b$. Then, the result matrix $\mathbf{O} = \dfrac{\mathbf{X}'\mathbf{Y}'}{100000 r_a r_b}$ is derived.

Step7: Users can obtain the values of elements on **O**'s leading diagonal, which can be expressed as re_i. Query results are determined by the value of re_i, which is normal if $0 < re_i < 1$, relatively low if $re_i < 0$ and relatively high if $re_i > 1$.

Further strengthening security and privacy

(1) In most cases, the user need not inquire all types of medical data (denoted by **Y**). For example, a user with Sinus rhythm cares about only his or her heart rate. If a user needs to inquire several types of medical data and the dataset can be denoted by $\mathbf{Y}^+$ and $\mathbf{Y}^+\subset\mathbf{Y}$, **Y** can be disorganized but keep every element in $\mathbf{Y}^+$ in the correct places of the matrix. For instance, if n=5, $\mathbf{Y}=(y_1, y_2, y_3, y_4, y_5)$, and the user focuses on only $\mathbf{Y}^+=\{y_2, y_4\}$, we can scramble the order of **Y**, for example as $(y_3, y_2, y_5, y_4, y_1)$. After the execution of HEBM, the matrix **O** is returned. Only y_2 and y_4 can provide correct results and the values of y_1, y_3 and y_5 confuse potential attackers.

(2) In Step 3 of HEBM, $\{\mathbf{M}*\mathbf{X}', r_b, g\}$ is completed, which can be further encrypted through the keys shared by the sender and receiver, and the transmission security will be enhanced.

III. Performance Analysis

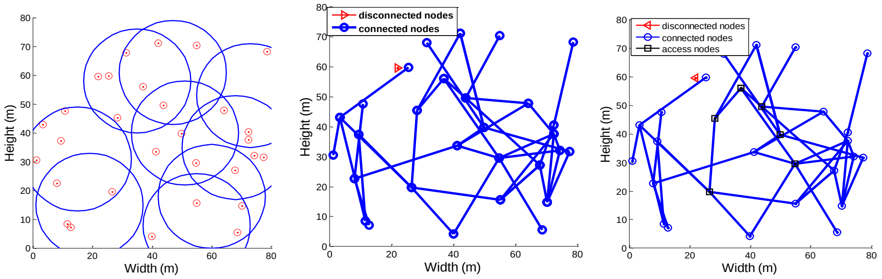
A. Average storage cost

The storage cost of HES proposed in this paper primarily comes from the keys stored in sensors. Generally, a more convincing analysis of the average key storage cost is based on comparisons among GSRM, the classic algorithm q-composite (short for qc) [5] and its improved algorithm proposed in [6] (short for Imp.qc). We suppose that N sensor nodes are randomly distributed in a range of $w\times h$, in which these nodes can be divided into groups by GSRM and the average number of nodes in each group is 2ξ. The average storage cost of each node in GSRM can be described as $2\pi\rho R^2$ and is positively related to the density ρ. In qc or Imp.qc, network connectivity must be guaranteed; otherwise, nodes cannot communicate with each other by exchanging shared keys. To prevent network connectivity from varying sharply, the density ρ is consistently kept as a constant with the coinstantaneous increase of both node number and region size. Relative simulation parameters are listed in TABLE III.

TABLE III
PARAMETERS OF SIMULATION

Parameters	Value
Width	w=80m in Fig. 4-(a) (b)(c)
Height	h=80m in Fig. 4-(a)(b)(c)
Number of nodes	N=30 in Fig. 4-(a) (b) (c), from 0 to 600 in Fig. 5
Network connectivity	>=95%
Network density	ρ=0.468%
Communication Distance	R=17.5m
Number of groups (GSRM)	*group*=9
Number of keys in pool (qc and Imp.qc)	*pool*=1000
Parameter q (qc and Imp.qc)	q=1
Parameter m (qc and Imp.qc)	m=20

In Fig. 4, the topologies of GSRM, qc and Imp.qc are shown in (a), (b) and (c), respectively. Nine groups are formed in GSRM, and each group is shown as the circle in Fig. 4-(a). The



(a) GSRM (b) qc (c) Imp.qc

Fig. 4. Different topologies of three schemes

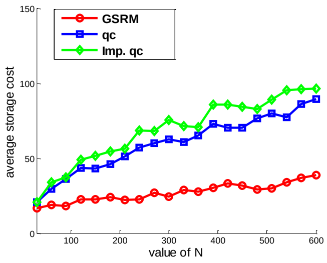


Fig. 5. Comparisons of average key-storage cost of three schemes

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2017.2687618, IEEE Transactions on Industrial Informatics

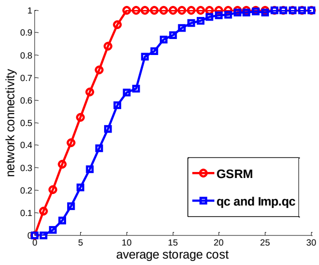


Fig. 6. Comparisons of network connectivity among GSRM, qc and Imp.qc

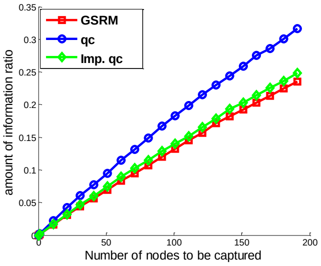


Fig. 7. Ratio with the varying number of captured nodes

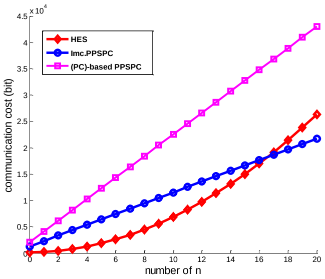


Fig. 8. Comparisons of communication cost among HES, Imp. PPSPC and (PC)-Based PPSPC

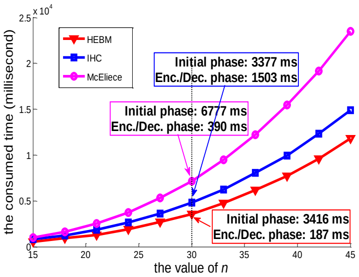


Fig. 9 Average consumed time of three homomorphic encryption methods

qc and Imp.qc algorithms retain high connectivity when only one isolated node exists. As shown in Fig. 5, when the scale of the network (both region size and node number) increases, GSRM guarantees a relatively stable level of the average storage cost, which means keys stored in each node are approximately ξ but not exactly ξ due to the key updating caused by entering and leaving of sensors. In contrast, the average storage cost of qc and Imp.qc gradually increases because when the network expands, an additional increase of keys in the key pool is needed to ensure the secure running of WSNs. This increase results in an increase of keys possessed by each node. The average storage cost of Imp.qc is slightly greater than that of qc because its access nodes need two key pools to distribute secret keys.

B. Network connectivity

The connectivity of GSRM, qc and Imp.qc is related to the keys stored in sensor nodes. To compare the network connectivity fairly, we assume that each sensor node shares the same average key storage, ranging from 0 to 30. There are 100 nodes in the network. Other relative simulation parameters except for N and ρ are shown in TABLE III.

As shown in Fig. 6, the GSRM algorithm is superior to qc (Imp.qc and qc have the same connectivity) when the numbers of keys stored in each sensor are relatively small. However, when keys reach 20 or more, the network connectivity of these two schemes, in which the isolated nodes have been neglected, is approximately 100%.

C. Security analysis

The security analysis of HES can be divided into two parts: the security of GSRM and that of HEBM.

a. security of GSRM

In a key management system, an attacker can obtain a large number of keys by capturing a small fraction of sensor nodes, which enables him (or her) possibly to take control of the entire network by deploying a replicated mobile sink to preload some compromised keys for authentication and then initiate data communication with any sensor node. Here, we make the following assumptions:

(1) The attacker can randomly capture nodes from any network area.

(2) The attacker has the ability to read the memory information of a captured node and obtain all its secret keys.

(3) The attacker is unable to capture or attack the base station.

(4) We use the ratio of the number of keys originating from those nodes captured by the attacker to the total keys as the metric of anti-capturing attacks.

We assume that the keys stored in each node range from 2 to 5, with 2000 nodes in the network and 1000 keys in the key pool. Shown in Fig. 7, the ratio increases approximately linearly with the rise of captured nodes. GSRM has a stronger anti-capturing ability than Imp.qc and qc because the keys carried by each node are dispersed in groups, resulting in less information being obtained by the attacker even when he (or she) has controlled the whole group.

In addition, GSRM has the following properties:

(1) Forward Confidentiality: Once the network detects a node that has suffered from the capture attack, keys updates are performed automatically, thus making it impossible for the captured node to obtain the new keys instantly or to participate in subsequent sessions.

(2) Backward Confidentiality: When key updates occur, due to the lack of previous keys, the fresh nodes are unable to decrypt the data packages generated before they entered the network.

b. security and privacy of HEBM

The HEBM scheme focuses more on the privacy protection of medical data. The matrix permutation and data confusion make it impossible for anyone except the source to obtain the plaintext of private data. Therefore, HEBM can effectively resist the following attacks.

(1) A leakage of privacy by the administrator or anyone who owns the highest authority. Even when the information stored in the WPANs server is decrypted, it remains confused and thus cannot be discriminated even by the administrator.

(2) Eavesdrop attack. The attacker is unable to access substantive information even when a data packet is captured due to the lack of decrypted keys.

(3) Chosen plaintext attack.

We make the following assumptions for the chosen plaintext attack on HEBM: the attacker has already obtained the entire records of a specific user who utilized medical services from HES t times. Each service record can be described as a triple $\{\mathbf{X}, \mathbf{M}, \mathbf{C}\}=\{\mathbf{X}_i, \mathbf{M}_i, \mathbf{M}_i*\mathbf{X}_i\}$, where $\mathbf{X}$, $\mathbf{M}$ and $\mathbf{C}$ indicate the real medical data, scrambling matrix and confused medical data, respectively; i=1, 2, ..., t. We shall prove that when the attacker accesses a new medical record $\mathbf{M}_{t+1}*\mathbf{X}_{t+1}$ from the same user, the posterior probability $P(\mathbf{X}=\mathbf{X}_{t+1} \mid \mathbf{C}=\mathbf{M}_{t+1}*\mathbf{X}_{t+1})$ that $\mathbf{X}_{t+1}$ is broken by the attacker equals the prior probability $P(\mathrm{X}=\mathbf{X}_{t+1})$, where $\mathbf{X}_i$ and $\mathbf{M}_i$ are mutually independent.

To prove:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2017.2687618, IEEE Transactions on Industrial Informatics

$$P(\mathbf{X}=\mathbf{X}_{t+1} \mid \mathbf{C}=\mathbf{M}_{t+1}*\mathbf{X}_{t+1})=$$

$$\frac{P(\mathbf{X}=\mathbf{X}_{t+1},\mathbf{C}=\mathbf{M}_{t+1}*\mathbf{X}_{t+1})}{P(\mathbf{C}=\mathbf{M}_{t+1}*\mathbf{X}_{t+1})} =$$

$$\frac{P(\mathbf{X}=\mathbf{X}_{t+1},\mathbf{C}=\mathbf{M}_{t+1})}{P(\mathbf{C}=\mathbf{M}_{t+1}*\mathbf{X}_{t+1})}=\frac{P(\mathbf{X}=\mathbf{X}_{t+1})P(\mathbf{C}=\mathbf{M}_{t+1})}{P(\mathbf{C}=\mathbf{M}_{t+1}*\mathbf{X}_{t+1})} \tag{5}$$

For any random $\mathbf{X}_{t+1}$, there necessarily exists the corresponding $\mathbf{M}_{t+1}$ to satisfy $\mathbf{C}=\mathbf{M}_{t+1}*\mathbf{X}_{t+1}$; then (5) can be transformed into (6), where $\mathbf{X}_j$ and $\mathbf{M}_j$ separately represent all possible values and matrices that satisfy $\mathbf{X}_j*\mathbf{M}_j=\mathbf{C}=\mathbf{M}_{t+1}*\mathbf{X}_{t+1}$. Meanwhile the equation $\sum P(\mathbf{X}=\mathbf{X}_j)$ =1 is established.

$$\frac{P(\mathbf{X}=\mathbf{X}_{t+1})P(\mathbf{C}=\mathbf{M}_{t+1})}{\sum P(\mathbf{X}=\mathbf{X}_j)P(\mathbf{C}=\mathbf{M}_j)} \tag{6}$$

Furthermore, $\mathbf{M}_j$ is generated randomly. Therefore, for any $\mathbf{M}_k$ and $\mathbf{M}_j$ ($k \neq j$), there is $P(\mathbf{C}=\mathbf{M}_k)=P(\mathbf{C}=\mathbf{M}_j)$. Therefore, we can derive $\frac{P(\mathbf{X}=\mathbf{X}_{t+1})P(\mathbf{C}=\mathbf{M}_{t+1})}{P(\mathbf{C}=\mathbf{M}_{t+1})\sum P(\mathbf{X}=\mathbf{X}_j)}$ = $P(X=\mathbf{X}_{t+1})$.

Prove up.

Therefore, under the condition that the attacker obtains the new confused medical record, the probability of acquiring the plaintext will not increase. Next, we estimate the cost that the attacker will pay using an exhaustive attack to further prove the security of HEBM against chosen-plaintext attacks.

Assume one specific user holds ten medical data items; then, each item in the column vector $\mathbf{M}*\mathbf{X}$ occupies 4 bytes (32 bits). Thus, the total data consist of 320 bits. The attacker randomly searches collision items in the data space. According to the birthday paradox, the computation complexity of finding a collision is approximately $\sqrt{2^{320}}$ $=2^{160}$. The probability that the attacker has acquired this collision item in advance is $t/2^{320}$; thus, the attacker needs a total of $2^{480}/t$ calculation times. Suppose that the attacker attained t medical records of the user, for instance $t=10^6$ (impossible in reality); if the computer processes 1200 trillion times per second, it will require $8.2*10^{115}$ years.

(4) Replay attacks.

During each handshaking session, the scrambled medical data conveyed in channels at one specific moment differs from that at another moment because the matrix $\mathbf{M}$ is randomly generated, and such an inconformity is unpredictable. Therefore, the attacker is unable to conduct a fake inquiry by replay attacks.

(5) Camouflage trust attack.

If a fake server claims to be an expert system, it is impossible for it to obtain the plaintext because the data packet is encrypted. Moreover, it remains impractical for the fake server to acquire the results even when the data packet is decrypted because the data remain confused.

D. System delay

The system delay of HES for transmission and processing of the medical data remains low due to the following aspects:

(1) During the initialization of WSNs, the group division and key distribution can be performed offline; once the initialization is completed, the network can be employed without any delay.

(2) The characteristics of GSRM facilitate decreased information exchange between nodes; during the send-receive process of medical data, only three handshakes are required to finish a circle. Thus, a reduced communication frequency means less network delay.

(3) The rapid and efficient operation hastens the transmission of data.

Generally, 0.5 second is an acceptable system delay. We compare HES with SecourHealth [7]; SecourHealth focuses on highly sensitive medical data collection applications and considers delay tolerance. The configuration of mobile phone (Model No. Android MI 2SC) includes a Quad-Core 1.7 GHz CPU and 2 GB RAM; the delay comparisons of initialization, calculation and message transmission are shown in TABLE IV.

TABLE IV
COMPARISONS OF SYSTEM DELAY BETWEEN HES AND SECOURHEALTH

Phase	SecourHealth		HES	
Initialization	PBKDF2	1038ms	Generate M Generate T	1.095ms 0.190ms
Calculation	$E_{MK}^{-1}(x)$	1.761ms	$\mathbf{M*X}$ $\mathbf{M*X*Y}$ $\mathbf{M'*M*X*Y}$	4.476ms
	$h(x)$	0.428ms	$\mathbf{X*Y+T}$	
Message Transport	Send a seed or resp. (100 bits)	121ms	Send a matrix (800 bits)	123ms

According to the statistics in TABLE IV, during the initialization of SecourHealth, the PBKDF2 algorithm is adopted, which causes the main system delay. However, the initialization of HEBM only uses two matrices, ensuring its system delay advantage compared with SecourHealth. During other processes, the time intervals of these two systems are as short as several milliseconds; thus, users can barely sense them.

E. Network communication cost and energy cost

For a better comparison, we assume that each user has n medical data items, two times data transmissions are needed during three handshakes in WPANs, and the communication cost of each session is estimated in TABLE V.

TABLE V
COMMUNICATION COST OF HES

Series	Communicati on cost	Variable types	Communicatio n cost (bit)
1	$\mathbf{M}*\mathbf{X}'$	n*1 vector	$32n$
	r_b	64bits integer	64
	g	64bits integer	64
2	$\mathbf{M}*\mathbf{X}'*\mathbf{Y}'$	n* n integer matrix	$32n^2$
	$\mathbf{T}$	n* n float matrix	$32n^2$

Thus, the total communication cost of one HES service is $64n^2+32n+128$ (bits). The communication cost of the improved PPSPC protocol (short for Imp. PPSPC) proposed in [8] is $(n+1)\cdot 1024+256$ (bits), and that of the (PC)-based PPSPC protocol introduced in [9] is $(n+1)\cdot 2048$ (bits). Comparisons of communication costs of three schemes are depicted in Fig. 8.

In Fig. 8, when $n<17$, the communication cost of HES is better than Imp. PPSPC and (PC)-Based PPSPC. When $n>17$, the communication cost of HES is inferior to Imp. PPSPC, and when $n \geq 32$, the communication cost of HES is not as good as (PC)-Based PPSPC. Given the scenario of routine physical examination, the count of a user's medical data items "n" usually ranges from 5 to 15; in this range, HES has a smaller communication cost. Although the homomorphic privacy-protection mechanism of HES increases the transmission amount of the matrix every time, an advantage is the reduction of communication frequency during handshakes when *n* is relatively small. When the value of *n* increases, the communication efficiency of the solution based on the matrix will inevitably be inferior to that based on the vector. Such a sacrifice of the communication cost is deserved, considering that homomorphic encryption can enhance privacy protection.

F. Computation efficiency

To test and verify the computation efficiency of HEBM, similar approaches based on homomorphic encryption are found and analyzed. Consequently, simulation experiments are conducted for comparisons among HEBM, IHC (proposed in [10]) and McEliece (proposed in [11]); all of them achieve data privacy-preservation based on matrix operation. All three methods can be divided into two phases: the initial phase and the encryption/decryption phase (Enc./Dec. phase for short). In the initial phase, reciprocal matrices and random numbers are generated for the encryption, and both encryption and decryption operations are carried out during the second phase. One thousand runs are performed with a gradual increase of the number of medical data items *n*. Fig. 9 shows the average time consumed per computation. In particular, when *n*=30, the time-consumed details of three methods in two distinct phases are highlighted.

HEBM obtains more-satisfactory computation efficiency among the three homomorphic encryption methods. Although they are all based on similar mechanisms, multi-round matrix operations lead to the increasing computation cost of IHC, and the utilization of a public key system in McEliece brings high computation complexity, whereas a lightweight algorithm is wisely adopted by HEBM.

IV. IMPLEMENTATION OF HES

To verify the feasibility of HES, we have designed a prototype system and realized the fundamental functions. As shown in Fig. 10, wearable medical nodes include the HK-2000H digital pulse sensor, the DS-100A oxygen finger clip and the DS-18B20 temperature sensor. Many temperature sensor nodes based on the CC2420 communication module are self-organized as relay networks. The gateway node realizes the protocol transformation between ZigBee and CDMA2000 or publishes the medical data to the expert system and other mobile devices within WPANs through Wi-Fi. We developed healthcare applications for handy mobile devices based on Android 4.1 and an expert system based on Ubuntu OS. We deployed our medical nodes and relay nodes in one specific hospital, finished the integration of HES software and hardware with the network system, and installed the APP on the mobile phones of some patients, doctors and nurses.

Due to the limitations of the test conditions, we collected only seven medical data items (of which the first three are real and the rest are simulated) of one specific examination for patient A, whose values are shown in TABLE VI. The real medical data of patient A can be denoted by **X**, and **X**' is calculated followed by the generation of random numbers r_a, r_b and g. Then, matrix **M** and **M'** are selected stochastically, and the message {**M*****X'**, r_b, g} is transmitted from the APP client to the expert system.

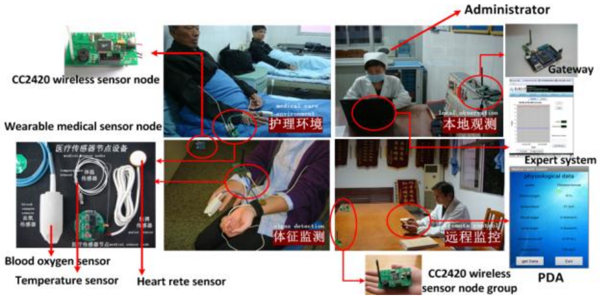


Fig. 10. Integration of HES software and hardware with network system

After completing the group division and key distribution based on GSRM, we collect the medical data sent by the relay sensor nodes using Wireshark packet sniffing tools, simulate the eavesdrop attack and obtain the **M*****X'** vector encrypted by AES. However, the attacker is unable to further ascertain the real value of **M*****X'** because of the lack of keys. If a capture attack is conducted by the attacker against one specific node and secret decryption keys are grasped through the access to memory information, the attacker can attain the plaintext of **M*****X'**. However, because matrix **M**, **M'** and integer r_a are randomly generated, the attacker cannot predict or access the real value of original medical data. Not only the attacker but also doctors and even the administrator of the HES server in the hospital are limited to calculating **M*****X'*****Y'** and **T** and remain unable to seize the actual data.

TABLE VI
MEDICAL DATA OF PATIENT A

Medical data name	Normal region	Examined value	Results
Heart rate	70~80 times/min	95 times/min	Higher
Blood oxygen	95~98 %	96 %	Normal
Temperature	36.2~37.2 ℃	36 ℃	Lower
Blood sugar	3.61~6.11 mmol/L	6.6 mmol/L	Higher
Urine sugar	0~100 mmol/L	4.5 mmol/L	Normal
White blood cell	(4.0~10.0) *10^9 /L	4.5 *10^9 /L	Normal
Hemoglobin	120~160 g/L	130.0 g/L	Normal

For the example in TABLE VI, when the result of {**M*****X'*****Y'**, **T**} is received, by left multiplying **M*****X'*****Y'** with **M'** and adding **T**, the elements on the leading diagonal of the matrix **O**: [2.5000 0.3333 -0.2000 1.1932 0.0447 0.0833 0.2500] can be calculated. The values of the 1st (heart rate) and 4th (blood sugar) items of **O** are greater than 1, the value of the 3rd (body temperature) item is less than 0, and the other values are

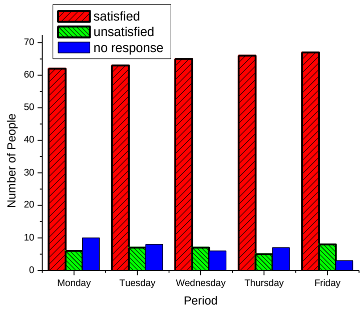


Fig. 11. User's feedback toward HES

between region (0,1). The heart rate and blood sugar are relatively high, body temperature is relatively low, and the other data items stay in a normal range, which is consistent with TABLE VI.

To verify preliminarily the reliability and feasibility of the expert system, we tested 78 patients using HES (only body temperature, heart rate and blood oxygen) for a duration of one week. Note that one important feature of HES is that it is available for the families and guardians to access health status information of these 78 patients via their mobile phones' APP, which also caters to the scenario of remote healthcare for old people. The analysis of questionnaires of their families and guardians is shown in Fig. 11. Three situations are possible: satisfied with the results provided by the expert system, unsatisfied and no response. We see a relatively high approval of results provided by the expert system.

V. RELATED WORK

The emergence of wireless body-area networks (WBANs) has become a key enabler of remote and in-home health monitoring. The technology is expected to revolutionize the health and real-time body-monitoring industry [1]. However, e-/m-healthcare still faces many challenges to its widespread adoption such as privacy breach violations [7].

J. Reid et al [12] design a role-based access control scheme that assigns the access authorities in terms of different doctor levels. J. Mirkovic et al [13] also propose a similar access control method. Moreover, an encryption method is frequently selected for the design of secure and privacy-preserving e-/m-healthcare. J. A. Akinyele et al [14] consider attribute-based encryption as an effective approach of protecting the privacy of electronic medical records. L. K. Guo et al [15] find a close relationship between patients' medical records and a sequence of attributes such as existing symptoms and undergoing treatments, and put forward a decentralized m-health system that leverages patients' verifiable attributes to authenticate each other in order to preserve attribute and identity privacy. Furthermore, some approaches based on homomorphic encryption have drawn more focus, although not all of them can be directly utilized in e-/m-healthcare. A. C. F. Chan [10] designs two schemes, which ensure that highly similar plaintexts can be transformed into distinctly different ciphertexts to resist ciphertext-only attacks. C. C. Zhao et al [11] study the homomorphic properties of the McEliece Public-key Cryptosystem and claims that this method can ensure security when data are transmitted in an unsafe environment. These schemes focus mostly on medical data privacy or security; however, some important performance metrics such as computation overhead, network connectivity, delay and power consumption are ignored.

Considering network efficiency and aiming at the different demands on various parts of the medical data, J. J. Yang et al [16] suggest a solution that achieves balance between medical data utilization and privacy protection by combining statistical analysis and cryptography. O. Kocabas et al [17] explore an efficient and accurate medical monitor system based on Fully Homomorphic Encryption (FHE) and AES. A. Page et al [18] also present a privacy-preserving medical remote monitoring scheme based on FHE, achieving a desirable efficiency. C. Wang et al [3] adopt the compressive sensing method for the first time to achieve functions such as simplified data acquisition, secure data reconstruction, and local resource savings. The above schemes obtain better tradeoffs between security or privacy and desirable efficiency.

Different from our proposal, particularly aiming at medical emergencies, R. X. Lu et al [8] present a secure and privacy-preserving opportunistic computing framework, SPOC, which comprises user-centric, attribute-based privacy access-control strategies based on scalar product computation. The (PC)-based PPSPC protocol proposed in [9] can also be used with the SPOC framework. Both of them consider computation cost and energy consumption while minimizing privacy disclosure. Similar work involves the BMEDiSN system [19], which provides electronic medical services for sudden disaster events. However, these solutions are designed only for healthcare emergency or disaster scenarios but not for more universal medical industry applications.

VI. CONCLUSION

Aiming at the existing issues of e-/m-healthcare systems, a distinct framework "HES" is proposed in this paper. The features of HES can be summarized in three areas: (1) using low-cost and easily-deployed wireless sensor networks as the relay infrastructure for GSRM-based secure transmission of medical data from WBANs to WPANs; (2) addressing the problem of achieving direct communications between a user's mobile terminals and embedded (wearable) medical devices (nodes); and (3) enforcing privacy-preserving strategies HEBM and achieving satisfactory performance. The implementation of an expert system that primarily addresses routine physical examinations can greatly reduce a doctor's or administrator's involvement and enable families and guardians to access users' health information anytime and anywhere. Therefore, HES can serve as a significant component of the informationization of medical industries. However, some problems remain unsolved; for example, the diagnosis reliability of the expert system is not perfect, and HES cannot currently monitor or analyze sudden diseases.

REFERENCES

[1] A. Sawand, S. Djahel, Z. Zhang, and F. Na ï-Abdesselam, "Toward Energy-Efficient and Trustworthy eHealth Monitoring System, " China Commun., vol.12, no. 1, pp. 46-65, Jan. 2015.

[2] M. S. Shin, H. S. Jeon, Y. W. Ju, B. J. Lee, and S. P. Jeong, "Constructing RBAC Based Security Model in u-Healthcare Service Platform," The Scientific World J., vol. 2015, Article ID 937914, 13 pages, http://dx.doi.org/10.1155/2015/937914, 2015.

[3] C. Wang, B. Zhang, K. Ren, J. M. Roveda, C. W. Chen, and Z. Xu. "A Privacy-aware Cloud-assisted Healthcare Monitoring System via Compressive Sensing," in Proc. of 33rd IEEE INFOCOM, 2014, pp. 2130-2138.

[4] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area

Networks," in Proc. of 35th IEEE Symp. on Security and Privacy, 2014, pp. 524-539.

[5] C. Bekara and M. Laurent-Maknavicius, "A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks," in Proc. of 3rd IEEE Int. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMOB 2007), 2007, pp. 59-59.

[6] P. T. Sivasankar and M. Ramakrishnan, "Active key management scheme to avoid clone attack in wireless sensor network," in Proc. of 4th Int. Conf. on Computing, Communications and Networking Technologies (ICCCNT'13), 2013, pp. 1-4.

[7] A. Marcos, J. Simplicio, H. I. Leonardo, M. B. Bruno, C. M. B. C. Tereza, and M. N¨aslund, "SecourHealth: A Delay-Tolerant Security Framework for Mobile Health Data Collection," IEEE J. Biomedical and Health Informatics (IEEE Trans. INF TECHNOL B), vol. 19, no. 2, pp. 761-772, Mar. 2015.

[8] R. X. Lu, X. D. Lin, and X. M. (Sherman) Shen, "SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency," IEEE Trans. Parall. distr., vol. 24, no. 3, pp. 614-624, Mar. 2013.

[9] A. Amirbekyan and V. Estivill-Castro, "A New Efficient Privacy-Preserving Scalar Product Protocol," in Proc. of Sixth Australasian Conf. Data Mining and Analytics (AusDM '07), 2007, pp. 209-214.

[10] A. C. F. Chan, "Symmetric-Key Homomorphic Encryption for Encrypted Data Processing," in Proc. of 2009 IEEE International Conference on Communications (ICC '09), 2009, pp.1-5.

[11] C. C. Zhao, Y. T. Yang, and Z. C. Li, "The Homomorphic Properties of McEliece Public-Key Cryptosystem," in Proc. of 2012 Fourth International Conference on Multimedia Information Networking and Security (MINES'12), 2012, pp.39-42.

[12] J. Reid, I. Cheong, M. Henrickson, and J. Smith, "A novel use of RBAC to protect privacy in distributed health care information systems," in Proc. of 8th Australasian Conf. on Information Security and Privacy, 2014, pp. 403-415.

[13] J. Mirkovic, H. Bryhni, and C. Ruland, "Secure solution for mobile access to patient's health care record," in Proc. 13th IEEE Int. Conf. e-Health Netw. Appl. Serv., 2011, pp. 296-303.

[14] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson, and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in Proc. of 1st ACM Workshop Security Privacy Smart phones Mobile Devices, 2011, pp. 75-86.

[15] L. K. Guo, C. Zhang, J. Y. Sun, and Y. G. Fang, "A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks," IEEE Trans. Mobile Compu., vol. 13, no. 9, pp. 1927-1941, Sep. 2014.

[16] J. J. Yang, J. Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," Future Generation Computer Systems, vol. 2015, no. 43-44, pp. 74-86, Nov. 2015.

[17] O. Kocabas, T. Soyata, J. P. Couderc, M. Aktas, J. Xia, and M. Huang, "Assessment of cloud-based health monitoring using Homomorphic Encryption," in Proc. of 2013 IEEE 31st International Conference on Computer Design (ICCD'13), 2013, pp.443-446.

[18] A. Page, O. Kocabas, S. Ames, M. Venkitasubramaniam, and T. Soyata. "Cloud-based secure health monitoring: Optimizing fully-homomorphic encryption for streaming algorithms," in Proc. of 2014 Globecom Workshops, 2014, pp.48-52.

[19] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices," In Proc. of ACM Sigcomm'11, Aug. 2011, pp. 2-13.

Haiping Huang (M'12) received the B.Eng. degree and M.Eng. degree in Computer Science and Technology from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2002 and 2005, respectively; and the Ph.D. degree in Computer Application Technology from Soochow University, Suzhou, China, in 2009.

From May 2013 to November 2013, he was a Visiting Scholar with the School of Electronics and Computer Science, University of Southampton, Southampton, U.K. He is currently a professor with the School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include information security and privacy protection of wireless sensor networks.

Dr. Huang is currently an associate editor of International Journal of Communication Systems and an editor of International Journal of Distributed Sensor Networks.

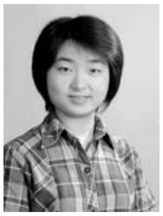
Tianhe Gong received the B.Eng. degree in Information Security from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2014. He is currently with successive postgraduate and doctoral programs of study with the School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include information security and privacy protection of wireless sensor networks.

Ning Ye received the B.S. degree in Computer Science from Nanjing University in 1994, the M.Eng. degree in Computer & Engineering from Southeast University in 2004, and the Ph.D. degree in Computer Science from Nanjing University of Posts and Telecommunications in 2009, Nanjing, China.

In 2010, Ning Ye worked as a Visiting Scholar and Research Assistant in the Department of Computer Science, University of Victoria, Canada. She is currently a professor with the School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. Her research interests include information processing in wireless networks and Internet of Things. She is a senior member of Chinese Computer Federation (CCF).

Ruchuan Wang received his B.S. degree in Computational Mathematics from The PLA Information Engineering University, Zhengzhou, China, in 1968.

He was a Visiting Scholar with Bremen University, Germany, Munich University, Germany, and Max-Planck Institute, Germany, during 1984-1992. He is currently a professor and a Ph.D supervisor with the School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include intelligent agent, information security, wireless networking and distributed computing.



Yi Dou received the B.Eng. degree in Information Security and M.Eng. degree in Computer Science and Technology from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2011 and 2014, respectively. She is currently a Ph.D candidate with the Department of Computing, The Hong Kong PolyTechnic University, in Hong Kong. Her research interests include wireless sensor networks, Internet of Things, privacy preserving and information security.