J Med Syst
DOI 10.1007/s10916-011-9716-z

ORIGINAL PAPER

Deployment of Secure Mobile Agents for Medical Information Systems

Tzer-Long Chen · Yu-Fang Chung · Frank Y. S. Lin

Received: 18 January 2011 / Accepted: 12 April 2011

Abstract Changes in global population and demography, and advances in medicine have led to elderly population growth, creating aging societies from which elderly medical care has evolved. In addition, with the elderly susceptible to chronic diseases, this together with the changing lifestyles of young adults have not only pushed up patient numbers of chronic diseases, but also effected into younger patients. These problems have become the major focus for the health care industry. In response to patient demand and the huge shortage of medical resources, we propose remote healthcare medical information systems that combine patient physiological data acquisition equipment with real-time health care analyses. Since remote health care systems are structured around the Internet, in addition to considering the numerous public systems spread across insecure heterogeneous networks, compatibility among heterogeneous networks will also be another concern. To address the aforementioned issues, mobile agents are adopted. With a mobile agent's characteristics of easy adaptability to heterogeneity and autonomy, the problem of heterogeneous network environments can be tackled. To construct a hierarchical safe access control mechanism for monitoring and control of patient data in order to provide the most appropriate medical treatment, we also propose to use the Chinese Remainder Theorem and discrete logarithm to classify different levels of monitoring staff and hence, to grant permission and access according to their authorized levels. We expect the methods proposed can improve medical care quality and reduce medical resource wastage, while ensuring patient privacy. Finally, security analysis of the system is conducted by simulating a variety of typical attacks, from which it can be concluded that the constructed remote healthcare information system be secure.

Keywords Chinese remainder theorem · Mobile agent · Health information system

T.-L. Chen (✉) · F. Y. S. Lin
Department of Information Management,
National Taiwan University,
Taipei, Taiwan
e-mail: d97725005@ntu.edu.tw

F. Y. S. Lin
e-mail: yslin@im.ntu.edu.tw

Y.-F. Chung
Department of Electrical Engineering, Tunghai University,
Taichung, Taiwan
e-mail: yfchung@thu.edu.tw

Introduction

Improvement to nutrition and healthcare knowledge, together with advances in medicine, has prompted a rapid increase in world population. As such, the elderly population has also grown, leading to great changes in the global population structure. With the growing elderly population and the formation of aging societies, elderly-related issues of medical and healthcare concerns have also emerged. In addition, while the elderly has been susceptible to chronic diseases, the young population because of stress, inappropriate diet, lack of exercise, and other factors, has become vulnerable to chronic diseases, pushing up patient population suffering from chronic diseases by the year. Current chronic disease treatment requires long-term follow-ups, such that most chronic patients are required to make routine trips to hospitals for checkups and treatments. However, such treatments not only consume excessive time and money from the repeated trips for treatments, but also reduce patients' quality of life significantly. In addition, often because effective monitoring and

Published online: 28 April 2011

care cannot be provided in time, chronic diseases evolve into acute ones, resulting in greater social costs of medical resources. Therefore, developing a system that can enable the elderly and chronic patients to receive long-term care at home with minimal medical resource wastage is an urgent issue that needs to be resolved.

At present, many countries around the world are striving to provide chronic patients with home-based long-term care to achieve the goal of enhancing patients' quality of lives. With advanced technologies, non-invasive physiological data taken at home is sent to hospitals for long-term monitoring and diagnosis. Doctors upon receiving the data, interpret, diagnose, and recommend appropriate treatment to the patients, saving patients and their families from exhaustive trips to the hospitals, and putting medical resources to most effective use. In recent years, the Internet technology has come to be widely used in remote homecare system development resulting into the combined use of medical, healthcare, communication, and wireless medical devices [1, 4, 5], allowing patients to enjoy healthcare services [2, 3] in the comfort of their home and community. In order to provide a wide range of healthcare services, it is crucial to have a remote care information platform that uses the Service Oriented Architecture (SOA) concept to complete, link, and integrate the construction of remote homecare services. Messages can be exchanged by adopting Simple Object Access Protocol (SOAP) standards, while system message exchange formats follow the HL7/XML standards. This system should have the feature of real-time monitoring that monitors the physiological status of the user, and personal alarm incident reporting processes that record, communicate, and process emergency occurrences. For example, after a user uses a device for measuring blood pressure, the system sends the data to the database via the Internet. Thereafter, the system inspects the user for abnormalities according to the user's current status. As shown in Fig. 1, when an abnormality is detected, the system with activate the pre-configured alert incident reporting process to inform the related personnel with information concerning "who", "how" and "what".. Also, a healthcare professional can use the system to search, report, and record emergencies to achieve active care.

With the advance of social welfare in advanced countries, the healthcare for the citizens is promoted. In terms of the cared objects, smart cards are issued that the medical practice is immediately confirmed. However, there is still risk of personal data outflow. The proposed method applies double authentication or the authentication on healthcare hardware or software. Since it is located in the healthcare environment of the patient, it can be fixed in certain area, such as the room or the activity range in a house. Regarding the hardware devices, such as heart strap or the equipment for blood pressure measurement, encryption technologies could be applied to the medical equipments for identity double authentication. For instance, One-Time Password (OTP) can reinforce the security and solve the identity authentication problem. In addition to smart cards, the patient's family could be included in the identity authentication to prevent the patient's conditions from being accessed by non-authorized people.

For effective identity authentication for both the patient (and family members) and healthcare personnel, the following methods may be adopted:

Public-key cryptography-based (PKI-based) method, including (i) challenge-response mode (the system encrypts a message using the public key of the person to be authenticated and demand return of the message from the person), and (ii) self-authentication mode (person to be authenticated uses his private key to encrypt a message to the system)

(1). Traditional credential-based method (ID and password)
(2). Smart card as another token
(3). Biometrics technologies, including fingerprint and face verification

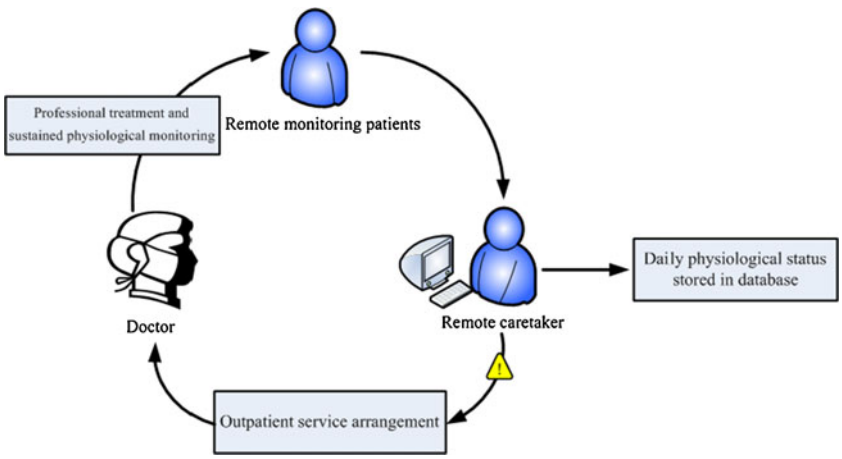

Fig. 1 Remote medical care concept

All the above can be adopted jointly to form a multi-modal (multi-factor) authentication system for higher security.

Remote care can monitor and improve the quality of life for many people; for example: patients suffering from arrhythmia, or pregnant women who require fetal heart rate monitoring. In general, to develop remote care information system, it will still be structured around the internet, but in combination with patient physiological data acquisition equipment that sends the data once it is produced through wireless communication system via the Internet to the Internet database for real-time analysis. In remote healthcare, there is a monitoring device on the cared patient, such as a heart strap or equipment for blood pressure measurement. Such equipment would regularly or irregularly transmit data to the host in the monitored area. The system could be programmed with responding thresholds to the medical patient's conditions. For example, if the patient has a history of hypertension, thresholds on the diastolic pressure and the systolic pressure could be programmed. When the patient's blood pressure exceeds these thresholds, a warning message will be transmitted to authorized members so that the healthcare professionals know the patient's conditions and the family realize what is happening.

When the user's status data exceeds the range of control, it automatically notifies the physician for the monitoring center, hospital, and other doctors to give consultations and notify the patient, all under the internet environment as shown in Fig. 2. More and more remote care research propose the use of mobile agent technology [8], because of its heterogeneity and mobility features, permitting mobile agents to communicate between different hosts and still be able to carry information, making it ideal for provide service, or transfer of patient personal and medical information.

While the use of mobile agent technology in remote healthcare has its advantages, it has its risk in information security. The mobile agent when carrying out its mandate, roams the Internet, and comes into contact with different hosts and agents for information exchange, exposing it to security threats. For example: the data it is carrying can be tapped or retrieved, or it can be attacked to prevent it from effectively completing its mission, or the mobile agent platform can be threatened with malicious attacks, etc. [7, 9] Therefore, mobile agent security is crucial in remote care information systems.

For these reasons, we propose a key management mechanism based on Chinese Remainder Theorem [17] with hierarchical management structure as basis. The mobile agent is regulated with key management and access control mechanism, making it a much more secure mechanism for electronic medical record retrievals when put to use in remote care systems to assure reliability. Meanwhile, security and efficacy is analyzed to verify its practicality and efficiency. In addition to ensuring the mobile agent's security when carrying out its mission, the system is also verified to satisfy the following four healthcare needs to increase key management performance and mobile agent system security: patient privacy [11–13], data security, real-time patient information, and non-repudiation of medical information.

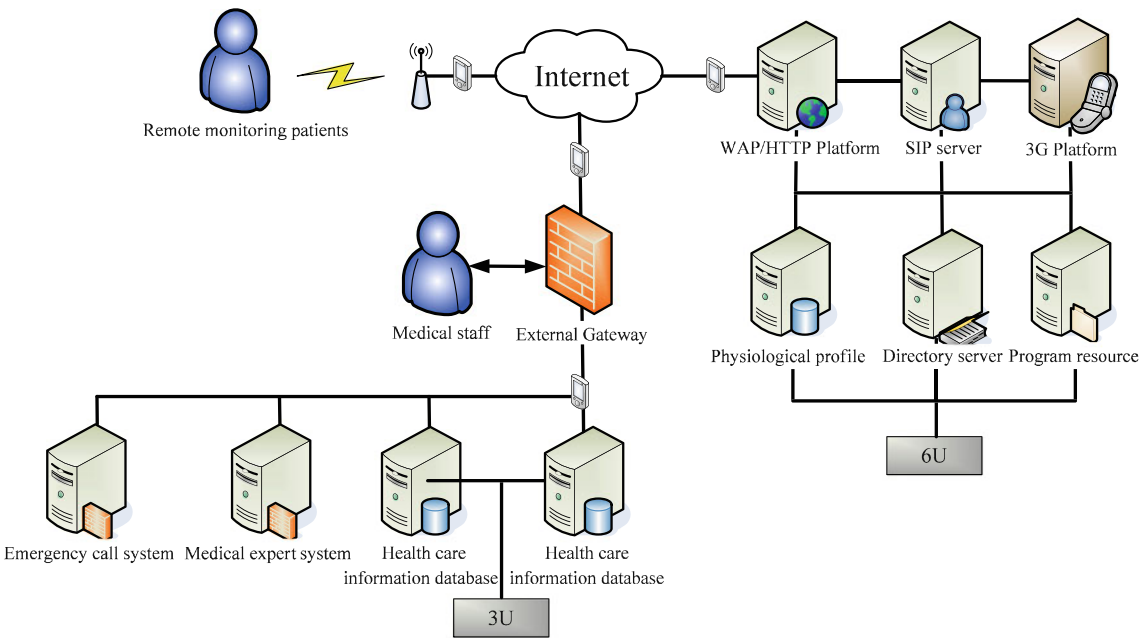

Fig. 2 Remote medical care system structure

Related work

Introduction to remote healthcare

In recent years, with rapid economic growth, improved living and education standard, there has been an increase in demand for healthcare services [19, 20], prompting higher average life expectancy. As a result, changes in population have led to aging societies, inducing concentration of medical resources among elderly and chronic patients. Thus, the need to put strained, limited medical resources to most effective use cannot be understated. This is echoed in advanced countries that have been actively promoting remote healthcare to replace prolonged hospitalization healthcare treatment, thereby reducing overall medical costs.

Remote healthcare is the integration of mobile communication [14, 15], hospital information system, and remote care applications. As shown in Fig. 3, the use of internet video system, and mobile health information monitoring device that can retrieve physiological data can transmit information via the Internet in real-time, provide contact for remote patients and doctors. Patients can receive immediate instructions, and doctors can take the initiative to understand the health status of patients to achieve early detection, and dispense treatment during the golden period, reducing unnecessary medical expenses, and improving healthcare quality. Remote care can be applied to diagnosis, prescribing medicine, health parameter monitoring, security monitoring, self-care instructing, patient education, and psychological and social support. Through remote care, patients can also practice self-management healthcare at home.

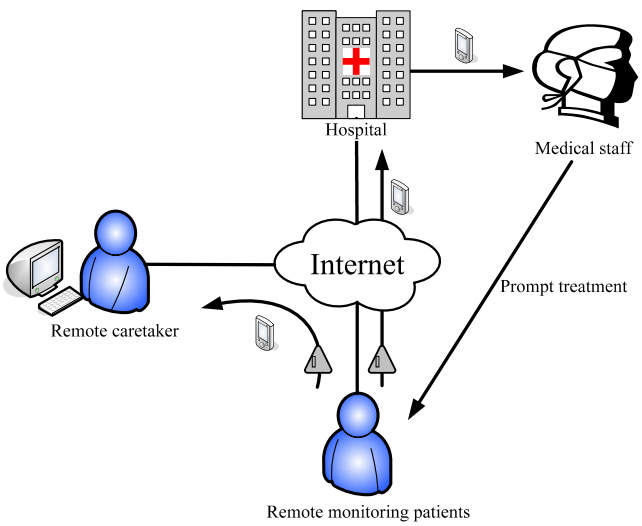

Fig. 3 Remote healthcare flowchart

Remote care service consists of three parts:

(1). Physiological information retrieval: The physiological information is effectively retrieved, transmitted correctly, stored and monitored in completeness. Physiological data includes temperature, heart rate, respiration rate, systolic pressure, diastolic pressure, mean blood pressure, electrocardiogram, oxygen ratio, basic lung function and other, more advanced monitoring, including for a variety of diseases, such as: liver function, diabetes, cholesterol, cancer, and other factors.

(2). Co-ordination of healthcare services: Through mobile communication, physiological parameter data measured with remote medical devices is transferred to the Internet database for real-time analysis to provide in time care, including assistance in providing emergency treatment on the home side, collection and transmission of warning signals, and notification for clinical visits.

(3). Assistance to health self-management: Patients are assisted to read the daily changes in physiological information, and in practicing good self-management, tracking, and early prevention. Thus, remote care system should include: reception inquiry of physiological information, transmission of exception alerts, analysis of biological information, doctor's suggestion, notification for clinical visits, medication tips, system support services, interactive interface for patients and doctors, and even integration of hospital's internal information system with electronic medical records, and provision of healthcare counseling services, emergency ambulance calls, etc. among other functions.

Following are the advantages of Remote care information systems:

(1). Universal Access: With information technology assistance, medical coverage can be expanded to remote areas to allow disadvantaged groups to have better medical care.

(2). Instant Support: Remote healthcare monitoring improves immediate healthcare service quality, assisting promptly those in need of medical assistance in case of emergencies.

(3). Personalization: According to individual situations, customized support can be provided for patients requiring special assistance.

(4). Improvement of Life Quality: Chronic patients and the elderly do not need to expend time for trips to the hospital. Through remote care, medical care can be provided right at home.

Characteristics of mobile agents

Remote care systems are constructed around the internet by integrating medical equipment to monitor for physiological information. The information is then sent through communication equipment to the database for real-time analysis. If the data exceeds the set scope of medical control, the system will alert and notify the relevant personnel. In the exchange or transfer of information, mobile agent technology [18] is necessary to secure transmission because of the mobile agent's heterogeneity and mobility features, allowing the mobile agent to communicate between different hosts. In addition, with its scalability and openness properties, it is ideal for providing services or transmitting patients' personal and health information, making the mobile agent most suitable for remote healthcare system.

The mobile agent is a piece of software placed in heterogeneous networks, and can move between hosts, and distributed resource systems to interact with other mobile agents. In addition, the mobile agent has the characteristic of retaining its autonomy in asynchronous environment. An autonomous mobile agent can self-control and operate when it is offline, and can decide on the next plan of action according to the environment status or implementation results. Therefore, the mobile agent is suitable for remote distributed care system and wireless network environments. Mobile agents can separately implement user-assigned tasks, or communicate with other mobile agents to achieve the purpose of division of labor, imparting to users greater benefits and convenience. In addition, the mobile agent also has a high degree of flexibility. It can be in accordance with the external environment, adjusting independently, and adapting to the current environment while completing its task. The mobile agent provides users high reliability, because only with the user's complete trust, can it represent the user.

The mobile agent can be placed on multiple computers simultaneously, or move between heterogeneous networks, and also be dispersed for autonomous computing. It has the following advantages:

(1). Reduce network load: Since the mobile agent carries its mission up till the point of execution, the mobile agent does not need to stay connected with the source. Only when the operation is completed will it need to use the network to return the data results and the program itself. Therefore, with less bandwidth consumption, network load is significantly reduced.

(2). Overcome network delay: With mobile agent technology, mobile agents are dispatched from the source to the destination terminal to implement the instructions only upon reaching its destination. Even message exchange during operation occurs only at the destination terminal. This way, network latency is effectively reduced. By using this feature in real-time systems like remote healthcare, immediate response time can be shortened.

(3). Encapsulation protocol: The mobile agent can encapsulate communication protocol. When the mobile agent reaches its destination, it can operate according to user protocol to establish connection for the appropriate communication protocol. Therefore, it does not need to consider host and client protocol issues in the remote healthcare system.

(4). Inherently heterogeneous: Both the network environment software and hardware are essentially heterogeneous. The mobile agent is independent from the computer, or network transport layer, and is related only to the execution environment. This helps in remote healthcare system operation.

However, because the Internet is an open environment, when the mobile agent is in the implementation process, it needs to roam in different host networks, and may be required to contact other mobile agents or hosts to exchange information. Hence, users should be worried about whether it will be subjected to malicious tampering or whether the host will come under attack, preventing the mobile agent from executing its task correctly. Illegal transmission of private data, or theft and eavesdropping by other mobile agents are other possible risks that make mobile agent security crucial in its application to remote care systems.

The chinese remainder theorem

The Chinese Remainder Theorem (CRT) is widely applied in computer science, especially in cryptography and data compression applications. Following is the derivation of CRT:

Theorem: Assume that n_1, n_2, n_3,..., n_t are pairwise-relatively prime positive integers, and x is an integer. After separate computation of n_k, (k= 1, 2,…, t), t number of integers a_1, a_2, …, a_t are derived, such that:

$$x \equiv a_1(n_1)$$
$$x \equiv a_2(n_2)$$
$$\cdots$$

$x \equiv a_t (\mathrm{mod}\ n_t)$,where $x(\mathrm{mod}\ n_1\ n_2\ \ldots\ n_t)$ has only one explanation.

To prove: the existence of a solution, and then the uniqueness of the solution.

(1). The existence of a solution: with the following mathematical induction, the existence of the solution can be proven.

When $t = 1$, $x \equiv a_1 \pmod{n_1}$, thus solution $x = a_1 + t_1 n_1$ must exist, where t_1 is an integer. When $t = 2$, $x \equiv a_1 \pmod{n_1}$ and $x \equiv a_2 \pmod{n_2}$, such that $x = a_1 + t_1 n_1 \equiv a_2 \pmod{n_2}$, that is $t_1 n_1 \equiv a_2 - a_1 \pmod{n_2}$.

Because gcd(N/n_k, n_k) =1, thus $t_1 = \lambda + t_2 n_2$ must exist, where λ is an integer, and $\lambda n_1 = a_2 - a_1 \pmod{n_2}$. By replacing $t_1 = \lambda + t_2 n_2$ in $x = a_1 + t_1 n_1 = a_2 \pmod{n_2}$, $x = a_1 + (\lambda + t_2 n_2)\, n_1 \equiv a_2 \pmod{n_2}$ is obtained. When $x = a_1 + (\lambda + t_2 n_2)\, n_1$ undergoes $n_1 n_2$ computation, $x = a_1 + \lambda n_1 \pmod{n_1 n_2}$ is obtained, satisfying $x = a_1 \pmod{n_1}$ and $x = a_2 \pmod{n_2}$ at the same time.

Assume when $t=\mu$-1, the Chinese Remainder Theorem holds, thus an integer solution σ exists, requiring $x \equiv \sigma \pmod{n_1 n_2 \ldots n_{\mu-1}}$ to hold.

Next, the following needs to be proven: When $t=\mu$, the Chinese Remainder Theorem will also hold. Now $x \equiv \sigma \pmod{n_1 n_2 \ldots n_{\mu-1}}$, and $x \equiv a_\mu \pmod{n_\mu}$, such that $x = \sigma + t_{\mu-1} n_1 n_2 \ldots n_{\mu-1} \equiv a_\mu \pmod{n_\mu}$, that is $t_{\mu-1} n_1 n_2 \ldots n_{\mu-1} \equiv a_\mu - \sigma \pmod{n_\mu}$. Because gcd($n_1 n_2 \ldots n_{\mu-1}$, n_μ) =1, thus $t_{\mu-1} = v + t_\mu n_\mu$ must exist, in which $v n_1 n_2 \ldots n_{\mu-1} \equiv a_\mu - \sigma \pmod{n_\mu}$ and v is an integer. By replacing $t_{\mu-1} = v + t_\mu n_\mu$ in $x = \sigma + t_{\mu-1} n_1 n_2 \ldots n_{\mu-1} \equiv a_\mu \pmod{n_\mu}$, $x = \sigma + (v + t_\mu n_\mu) n_1 n_2 \ldots n_{\mu-1} \equiv a_\mu \pmod{n_\mu}$ is obtained. By putting $x = \sigma + (v + t_\mu n_\mu) n_1 n_2 \ldots n_{\mu-1}$ to undergo $n_1 n_2 \ldots n_\mu$ computation, $x = \sigma + v n_1 n_2 \ldots n_{\mu-1} \pmod{n_1 n_2 \ldots n_\mu}$ can be obtained, at the same time satisfying $x \equiv \sigma \pmod{n_1 n_2 \ldots n_{\mu-1}}$ and $x = a_\mu \pmod{n_\mu}$.

(2). The uniqueness of solution

Since $n_1, n_2, n_3, \ldots, n_t$ are pairwise relatively prime, making all $k = 1, 2, \ldots, t$, $(\frac{N}{n_k}, n_k) = 1$. Since $\frac{N}{n_k}$ and n_k are coprimes, therefore, there must be a congruence of the multiplicative inverse system y_k making $\frac{N}{n_k} y_k = 1 \bmod n_k$. In addition, when $k \neq j$, $\frac{N}{n_k}$ is the multiple of n_j, thus, $\frac{N}{n_k} y_k = 0 \pmod{n_j}$. If we set $x = a_1 \frac{N}{n_1} y_1 + a_2 \frac{N}{n_2} y_2 + \ldots + a_t \frac{N}{n_t} y_t \pmod{N}$, then x will satisfy the solution to the above remainder system, because to every $k, 1 \leqq k \leqq t$, $x \bmod n_k = (\frac{N}{n_k})\, y_k\, a_k \pmod{n_k} = a_k$.

Assume in the above mentioned remainder system, there exists two solutions, x_0 and x_1, $x_0 \neq x_1$; thus to every k, $1 \leqq k \leqq t$, $x_0 = x_1 = a_k \pmod{n_k}$, hence $n_j \mid (x_0 - x_1)$. Therefore $N \mid (x_0 - x_1)$, such that $x_0 = x_1 \pmod{N}$. In conclusion, this system can only have one solution.

(3). To illustrate: Use the Chinese Remainder Theorem to solve $x = 3 \pmod 5$, $x = 5 \pmod 7$, $x = 7 \pmod{11}$.

Solution: Since $x \equiv 3 \pmod 5$, thus assume $x = 3 + 5k_1$, where k_1 is an integer. Then, $3 + 5k_1 \equiv 5 \pmod 7$, obtains $k_1 \equiv 6 \pmod 7$. By replacing $k_1 = 6 + 7k_2$ in $x = 3 + 5k_1$, $x = 3 + 5k_1 = 3 + 5(6 + 7k_2) = 33 + 35k_2$ is obtained, where k_2 is an integer. Since $x = 33 + 35k_2$ and $x = 7 \pmod{11}$, so $x = 33 + 35k_2 = 7 \pmod{11}$, that $35k_2 = -26 \pmod{11} \equiv 7 \pmod{11}$, obtaining $k_2 \equiv 9 \pmod{11}$. By replacing $k_2 = 9 + 11k_3$ in $x = 33 + 35k_2$, $x = 33 + 35(9 + 11k_3) = 348 + 385k_3$ can be obtained, where k_3 is an integer. By putting $x = 348 + 385k_3$ to undergo 385 (that $5 \times 7 \times 11$) computation, $x = 348 \pmod{385}$ is obtained.

The proposed scheme

The following describes the proposed method. First, we will discuss the application of mobile agent technology coupled with secure access method for collecting information spread across medical institutions and patients' homes [21, 22]. Originally, the set-up of the host and the configuration of the healthcare environment has considered the patient's environment and the planning/allocation of healthcare. The healthcare hardware for the patient's environment or the training of the associated family members as well as the distribution of the mechanism is well planned that the entire system operation will be stable and scalable.

In this paper, polynomials are established in the mobile agent so that, when there are too many cared objects, the tasks for the mobile agent could be dispersed to various hosts to reduce the load of each host. Besides, the tasks could be exchanged among mobile agents to save the time for communication with the hosts. Moreover, in the polynomials, only the host which is going to access is true (i.e. 1 and would consume system resources), others are false (i.e. zero and virtually consume no resource), so that they can be rapidly computed to enhance the efficacy of the entire system and can possibly disperse the load of the system. Next, for providing patients with the most appropriate remote medical care, the construction of a hierarchical structure [6, 10] together with the application of the Chinese Remainder Theorem to ensure medical information security and instant information will be explained.

Despite the different communication protocols that may exist between hosts, with the mobile agent's ability to roam in heterogeneous networks, the mobile agent can maintain the original host's status and overcome the problem of incompatibility. This feature is exploited in our method to collecting information both internal and external. Next, according to the medical personnel's access levels a hierarchical access control mechanism is constructed, keeping in mind the actual needs of the framework. This is accompanied by the Chinese Remainder Theorem for constructing a password security system. The access authority is established a hierarchical structure in static mobile agent for the distinction of authority levels. Since the mobile agent is individually dispatched by various sectors, the data are read separately, but the information is same and consistent. When an authorized user tends to write in data, the data state would be changed to write-state and is locked from being accessed. Another user who tries to write in or access to the data has to wait until the write-state being changed to access-state. When the data are accessed, they are read separately so as to maintain the consistence of the data. Besides, the data are based on the

level of access authority that the uniformity of the data could be remained. By imparting mathematical difficulty and complexity to the constructed system, the access system's security is enhanced, preventing illegal users from access and tempering of the system.

The following will focus on the concepts and methods of this paper. First, DK_j is a symmetric encryption secret key used to encrypt or decrypt confidential information; the Chinese Remainder Theorem is used to construct the superkey, SK_i, of the hierarchical structure, in which the superkey, SK_i, by substituting the remainder theorem in the public and private parameters of each leaf node can be calculated. Subsequently, with the use of one-way has function, the private keys under S_i can be calculated. The security of the system in this paper is mainly based on S_i, without which, or the lack of access of it, information on private parameters cannot be obtained. This together with the Chinese Remainder Theorem's characteristics, makes Superkey SK_i as the ultimate superkey which unauthorized users will never be able to calculate through public parameters, in the event where crucial parameter information is difficult to obtain. Thus, the proposed mechanism can guarantee that only authorized servers to confidential data can obtain the encryption key, rendering our method safe.

Before the proposed method is discussed in detail, the parameters used are defined as follows (Table 1):

Defining key property of "≤":

Assume $S_i \neq S_j$; there exists two situations where we cannot have both $S_j \leq S_i$ and $S_i \leq S_j$. Assume that $S_i \neq S_j$. If both $S_j \leq S_i$ and $S_i \leq S_j$, then $\exists$ path $S_0 \rightarrow S_i \rightarrow S_j$ and $\exists$ path $S_0 \rightarrow S_j \rightarrow S_i$. Then we can find a path $S_o \rightarrow S_i \rightarrow S_j \rightarrow S_i \rightarrow S_o$. This contradicts the definition of a tree (=a connected graph with no loop). From the above description, relationship of the structure's access extent is thus defined as "≤," a partial order on the set$\{S_0, S_1, \ldots, S_k\}$。

(1). Reflexive: $S_i \leq S_i, \forall$ i This follows the definition of "≤".

Table 1 Parameters for constructing the system

DK_u	decryption key that protects the medical information
S_i	server S_i indicates authorized medical personnel to data access
J_i	explains the relationship between server S_i and decryption key $J_i = \{u : S_i$ has permission to access decryption key $DK_u\}$
n_u	a large prime for each DK_u, $\forall u = 1, 2, \ldots, m$
N_i	N_i is obtained by performing continuous multiplication on the n_u that corresponds to DK_u gcd $(N_i/n_u, n_u) = 1$
r_u	distinct r_u for DK_u
W_u	W_u is the unique primitive multiplicative inverse of N_i/n_u (mod n_u)
SK_i	secret Superkey of server S_i
E	Encryption function
D	Decryption function

(2). Transitive: $S_q \leq S_j$ and $S_j \leq S_i \Rightarrow S_q \leq S_i$
$S_q \leq S_j \Rightarrow \exists$ path $S_o \rightarrow S_j \rightarrow S_q$
$S_j \leq S_i \Rightarrow \exists$ path $S_o \rightarrow S_i \rightarrow S_j$
Hence $\Rightarrow \exists$ path $S_o \rightarrow S_i \rightarrow S_j \rightarrow S_q$
That is $\Rightarrow \exists$ path $S_o \rightarrow S_i \rightarrow S_q \ \therefore S_q \leq S_i$

(3). Anti-symmetric: $S_j \leq S_i$ and $S_i \leq S_j \Rightarrow S_i = S_j$. (This follows the key property.)

In the hierarchical structure, the decryption key, DK_u, (where $u = 1, 2, \ldots, m$) of the bottom most layer's leaf node is the key used for encrypting and decrypting the medical data that needs to be protected; the intermediate nodes are nodes indicating authorized medical personnel or corresponding units and servers to data access, demoted by S_i, $i = 1, 2, \ldots, n$; next, by defining $J_i = \{u: S_i$ has permission to access decryption key $DK_u\}$ is to indicate the relationship between server S_i and decryption key. As demonstrated by Fig. 4, $J_4 = \{1, 2\}$ indicates S_4 has authorized access to DK_1, DK_2; in $J_1 = \{1, 2, 3, 4\}$, it indicates that S_1 has authorized access to DK_1, DK_2, DK_3 and DK_4.

Key generation

step 1. Mobile agent owner chooses unrepeated random integers $\{DK_1, DK_2, \ldots, DK_m\}$ (suppose there are m confidential files), as the decryption key of encrypted confidential files and selects pairwise relative primes n_u for each DK_u, $\forall u = 1, 2, \ldots, m$. DK_u is kept secret and n_u is a public parameter.

step 2. Mobile agent constructs the N_i for the internal node S_i. N_i is obtained by taking the product of the n_u that corresponds to DK_u which S_i is authorized to access. That is:

$$N_i = \prod_{u \in J_i} n_u \tag{1}$$

By the construction of N_i, we have gcd$(N_i/n_u, n_u) = 1$, $\forall i = 1, 2, \ldots, k$; $\forall u \in J_i$.

step 3. Mobile agent owner randomly chooses distinct r_u for DK_u. r_u is kept secret.

step 4. Mobile agent owner calculates separately a unique primitive multiplicative inverse number W_u that satisfies the following equation (2), where n_u denotes S_i is authorized to access DK_u. Since N_i/n_u and n_u are coprimes, a multiplicative inverse number W_u of a congruent remainder system must exist. The equation is as follows:

$$W_u \cdot \frac{N_i}{n_u} \equiv 1 (\mathrm{mod}\, n_u), \forall u \in J_i \tag{2}$$

step 5. Mobile agent owner multiplies and adds the corresponding r_u and $W_u \cdot \frac{N_i}{n_u}$ of DK_u, (the autho-

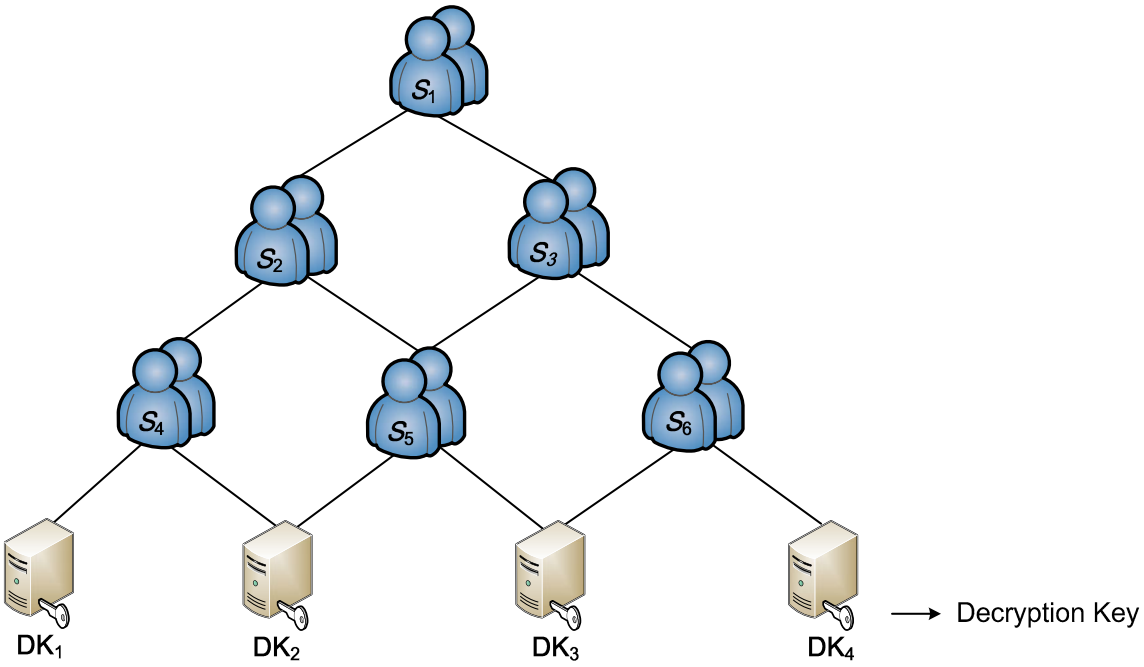

Fig. 4 The hierarchical structure of mobile agents

rized decryption key of server S_i), obtains the remainder of modulo N_i and calculates the superkey of S_i, SK_i.

$$SK_i = \sum_{u \in J_i} r_u \times W_u \times (\frac{N_i}{n_u}) (\text{mod } N_i), \quad (3)$$

$$\forall i = 1, 2, \ldots, k$$

Based on the Chinese Remainder Theorem, SK_i is the unique primitive solution to the following system of congruences.

$$y \equiv r_u (\text{mod } n_u), \forall u \in J_i$$

Hence we have $SK_i \equiv r_u (\text{mod } n_u)$, $\forall u \in J_i$

step 6. Defines and publishes an one way hash function h (.) Defines the generating function $f_u(x)$ for DK_u by $x = h(r_u||SK_i)$as public, $\forall u \in J_i$, substitutes hash function h(.) in the corresponding r_u of DK_u and SK_i and publishes the calculation, f(x):

$$f_u(x) = \prod_{i:u \in J_i} [x - h(r_u||SK_i)] + DK_u, \forall 1 \le u \le m. \quad (4)$$

The expanded form of (4), other than (4) itself, is published. We note that DK_u is embedded in the constant term of the expanded form of (4); this prevents the extraction of DK_u.

Key derivation

When a server S_i corresponding to an internal node wishes to access its leaf nodes DK_u, the following steps are performed:

step 1. Server S_i uses Superkey SK_i and public parameter n_u to find the value of the secret parameter r_u. The formula is as follows:

$$r_u \equiv SK_i (\text{mod } n_u), \forall u \in J_i \quad (5)$$

step 2. S_i uses r_u and Superkey SK_i to compute $h(r_u||SK_i)$ and then obtains DK_u by the public formula is as follows:

$$DK_u = f_u(h(r_u||SK_i)), \text{for } u \in J_i \quad (6)$$

Example

According to the above described steps and processes, we demonstrate with Fig. 4, first by setting the parameter for each secret file:

According to Fig. 4, between each server nodes, there exists a hierarchical relationship. The server nodes are S_1, S_2,…, S_6. To protect the data, the encryption keys of DK_1, DK_2,…, DK_4 are set with parameters as shown in Table 2.

Table 2 An example for parameter setting

(Secret)		(Public)
Decryption key	Participate parameter (r_u)	Participate parameter (n_u)
DK_1	r_1=3	n_1=7
DK_2	r_2=4	n_2=5
DK_3	r_3=9	n_3=11
DK_4	r_4=12	n_4=13

First, we must calculate N_i for Server S_i. With $N_i = \prod n_u$ (u=1~4,i=1~6), the following is arrived at:

N_1	N_2	N_3
7*5*11*13=5005	7*5*11=385	5*11*13=715
N_4	N_5	N_6
7*5=35	5*11=55	11*13=143

Next, according to the access right of S_i, DK_u is accessed and its corresponding W_u is calculated. With the following formula, W_1~W_4 can be calculated. Using Server S_1 as an example: Assume that S_1 has access to DK_1~DK_4. The calculated results are the corresponding W_1~W_4.

$$W_u \times (\frac{N_i}{n_u}) \bmod n_u = 1 \text{ for } u \in J_i$$

W_1=1	W_2=1
W_1×(5005/7)mod 7=1	W_2×(5005/5)mod 5=1
W_3=3	W_4=5
W_3×(5005/11)mod 11=1	W_5×(5005/13)mod 13=1

$$\Rightarrow W_1 = 1, W_2 = 1, W_3 = 3, W_4 = 5.$$

Next, the corresponding Superkey SK_1 of $S_1$is calculated:

$$SK_1 = \sum r_u \times W_u \times (\frac{N_1}{n_u}) \bmod N_1$$

$$SK_1 = \left\{ \begin{array}{l} r_1 \times W_1 \times (\frac{N_1}{n_1}) + r_2 \times W_2 \times (\frac{N_1}{n_2}) \\ + r_3 \times W_3 \times (\frac{N_1}{n_3}) + r_4 \times W_4 \times (\frac{N_1}{n_4}) \end{array} \right\} \bmod N_1$$

$$\begin{aligned} SK_1 &= \{3 \times 1 \times (5005/7) + 4 \times 1 \times (5005/5) + 9 \times 3 \times (5005/11) + 12 \times 5 \times (5005/13)\} \bmod 5005 \\ &= (2145 + 4004 + 12285 + 23100) \bmod 5005 = 1494 \end{aligned}$$

Since $3 \in J_1 = \{1, 2, 3, 4\}$, S_1 has permission to access DK_1. S_1 uses its Superkey SK_1 to compute the secret parameter r_3 for DK_3 and the hash value $h(r_3||SK_1)$. Recall that the generating function for DK_3 is the expanded form of

$$\begin{aligned} f_3(x) &= \prod_{i:3 \in J_i} (x - h(r_3||SK_i)) + DK_3 \\ &= \prod_{i \in \{1,2,3,5,6\}} [x - h(r_3||SK_i)] + DK_3 \\ &= [x - h(r_3||SK_1)] \times [x - h(r_3||SK_2)] \times [x - h(r_3||SK_3)] \times \\ &\quad [x - h(r_3||SK_5)] \times [x - h(r_3||SK_6)] + DK_3 \end{aligned}$$

S_1 obtains DK_1 by $DK_1 = f_3(h(r_3||SK_1))$. We notice that $3 \notin J_4 = \{1, 2\}$, S_4 has no permission to access DK_3. S_4 can't derive the secret parameter r_3 for DK_3. Even if S_4 somehow manages to obtain r_3, he still can't derive SK_3 by computing $f_3(h(r_3||SK_4))$.

Analysis of security

This section analyses the attacks the Telecare Service may face, and how the method proposed in this paper can effectively fend off the attacks. Also to be discussed is how the mobile agent employed in our proposed system can raise the quality of medical care and protect patients' privacy through key management and access control mechanism, in order to illustrate that our proposed Remote healthcare service is safe and secure.

Reverse attack

Reverse Attack is a possible type of attack to hit the system. For users of the remote healthcare system, medical personnel have access rights to medical data that can be imparted to authorized, legal mobile agents to effectively collect data spread across institutions and homes. When a medical personnel that corresponds to mobile agent internal node S_j falls into a $S_j \leq S_i$ relationship with another node S_i, can node S_j use its own Superkey SK_j with other public parameters to calculate Superkey SK_i of S_i, and subsequently access, steal, and modify data which S_i is authorized to?

If the personnel corresponding to mobile agent internal node S_j wants to launch a reverse attack, $SK_i = \sum_{u \in J_i} r_u \times W_u \times (\frac{N_i}{n_u}) (\mathrm{mod}\ N_i)$ must be calculated. Before calculating SK_i, S_j will already have the secret parameter r_u of $SK_j = \sum_{u' \in J_j} r_{u'} \times W_{u'} \times (\frac{N_j}{n_{u'}}) (\mathrm{mod}\ N_j)$, where $u' \in J_j$, and can freely obtain public parameter n_u to calculate the following parameters of SK_i:$N_i = \prod_{u \in J_i} n_u$ and multiplicative inverse W_u, where $W_u \cdot \frac{N_i}{n_u} \equiv 1 \ (\mathrm{mod}\ n_u)$. Since there exist a $S_j \leq S_i$ relationship, S_j can obtain parts of r_u of S_i with its own r_u. But according to the predefined $u' \in J_j$, where $J_j = \{u' \mid S_j$ has permission to access decryption key $DK_{u'}\}$, S_j without access rights will not be able to derive the complete r_u of S_i. Although W_u and N_i can be derived through complex calculations, there is no way to derive the information of all leaf nodes r_u. Hence, without the information of r_u, Server S_j cannot determine the Superkey SK_i of S_i.

Collusion attacks

Another threat of the system is from collusion attacks. A collusion attack implies a collaboration effort, where numerous personnel from the medical organization combine their information to derive illegally the decryption key and subsequently, obtain unauthorized data. Suppose there is an internal medical personal that corresponds to mobile agent internal node S_j, which has a $S_j \leq S_i$ relationship with another Server S_i. Can S_j collaborate with other medical personnel $S_{j+1}, \ldots, S_{j+t}$, ($t+1$ represents the number of servers after S_i, where $S_{j+t} < S_i$), and together with their access rights collect the relating system's public parameter to derive SK_i belonging to a higher access level S_i?

The r_u mentioned in our method is so important, that to derive any superkey, a private r_u must be substituted in, in order to derive the key. For those personnel who wish to obtain higher access levels, they exchange their private parameter r_u and tries to derive the superkey using the following formula:

$$SK_{j+t} = \sum_{u' \in J_{j+t}} r_{u'} \times W_{u'} \times (\frac{N_j}{n_{u'}}) (\mathrm{mod}\ N_{j+t}),$$

$$\text{where } t \geq 0, j + t < i$$

Through collusion attack, the r_i wishes to derive S_i, and subsequently, SK_i. But from the above formula, it is still not possible to obtain sufficient information to derive Superkey SK_i. From the above analysis, it can be seen that basing our mechanism on the Chinese Remainder Theorem is to ensure security through discrete algorithm mathematics [16]. For any subsequent S_k, $S_{k+1}, \ldots, S_{k+t}$, obtaining any r_u above their access right is relatively difficult. It is also impossible to obtain Superkey SK_i of S_i, thus ensuring that the system be safe from such attacks.

External attacks

The following refers to external attacks by non-medical or unrelated bodies that do not have related access rights, but desires to derive the decryption key through public parameters, and subsequently, obtain unauthorised data. In this paper, using the Chinese Remainder Theorem we impart to each medical personnel, the one and only Superkey $SK_i = \sum_{u \in J_i} r_u \times W_u \times (\frac{N_i}{n_u}) (\mathrm{mod}\ N_i)$ that can decrypt its corresponding confidential files. If an external attacker wishes to obtain protected medical data, he must first obtain the SuperKey. From public n_u, the attackers may be able to calculate N_i and W_u, but without knowing r_u, the attackers cannot use N_i and W_u to derive SK_i. This is to say, the attacker will not be able to obtain the superkey through the above mentioned method. Thus, it is not possible for external attackers to obtain unauthorised medical data through public information.

Conclusion

Global elderly population is on the rise, changing population structure, and creating bigger aging societies. Arising from decreased mobility, or ability of the elderly, many problems relating to elderly medical care have evolved. In addition, with chronic patient numbers increasing by the year and its patient age decreasing so, to satisfy such medical needs under limited resources, medical institutions have begun providing remote healthcare services that allow remote regular monitoring of patients' health status and consequently increased the quality of life for many patients. The information system of most remote healthcare services

integrates patient physiological data measuring devices with the Internet to facilitate data transfer to network databases for usage by staff belonging to the monitoring centre and medical institution. This paper proposes a more integrated remote healthcare information system that is different from that limited by environment and distance. Based on the concept of remote healthcare, we structure our system around the Internet and employ the mobile agent's heterogeneity and mobility features to adapt to heterogeneous networks and systems different from the mobile agent. By allowing the mobile agent to communicate between different servers, together with its scalability and openness properties, this enables data collection from a diverse range of monitoring devices in order to put together the most complete patient profile and medical information. At the same time, by constructing a system with hierarchical access control mechanisms based on the Chinese Remainder Theorem, we allow the mobile agent to provide secure and credible service when performing remote healthcare services. In addition, we have also analyzed the proposed system's security by verifying the system's feasibility and efficiency to prove the security of the mobile agent when carrying out tasks, and have also satisfied the four needs of medical care institutions: patient privacy, data security, real-time patient information, and non-repudiation of medical information. Furthermore, successful key management has also effectively increased the mobile agent system security.

Acknowledgment This work was supported partially by National Science Council of Republic of China under Grants NSC99-2622-E-029-011-CC3.

References

1. Calcote, S., Developing a secure healthcare information network on the internet. *Healthcare Financial Management* 51(1):68–70, 1997.
2. Buckley, J., The importance of telecare for people with dementia. *Nursing & Residential Care* 8(5):212–214, 2006.
3. Debray, M., Couturier, P., Greuillet, F., Hohn, C., Banerjee, S., Gavazzi, G., and Franco, A., A preliminary study of the feasibility of wound telecare for the elderly. *Journal of Telemedicine and Telecare* 7(6):353–358, 2001.
4. Gund, A., Ekman, I., Lindecrantz, K., Sjoqvist, B. A., Staaf, E. L., Thorneskold, N., "Design Evaluation of a Home-Based Telecare System for Chronic Heart Failure Patients", *the 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5851–5854, 2008.
5. Hou, C., Jia, S. M., and Takase, K., Real-time multimedia applications in a web-based robotic telecare system. *Journal of Intelligent & Robotic Systems* 38(2):135–153, 2003.
6. Chen, T. S., Chung, Y. F., and Tian, C. S., A novel key management scheme for dynamic access control in a user hierarchy. *Proceedings of the IEEE Annual International Computer Software and Applications Conference* 1:396–401, 2004.
7. Bierman, E., Pretoria, T., Cloete, E., "Classification of Malicious Host Threats in Mobile Agent Computing," *Proceedings of the 2002 Annual Research Conference of The South African Institute of Computer Scientists and Information Technologists on Enablement Through Technology*, pp. 141–148, 2002.
8. Corradi, A., Montanari, R., Stefanelli, C., "Security Issues in Mobile Agent Technology," *Proceedings of the 7th IEEE Workshop on Future Trends of Distributed Computing System*, pp. 3–8, Cape Town, South Africa, 1999.
9. Karnik, N. M., Tripathi, A. R., "A Security Architecture for Mobile Agents in Ajanta," *Proceedings of the International Conference on Distributed Computing Systems*, pp. 402–409, Taipei, Taiwan, 2000.
10. Volker, R., and Mehrdad, J. S., Access control and key management for mobile agents. *Computer and Graphics* 22 (4):457–461, 1998.
11. "The State of HIPAA Privacy and Security Compliance", *AHIMA*, April 2006.
12. Safran, C., Rind, D., Citroen, M., Bakker, A. R., Slack, W. V., and Bleich, H. L., Protection of confidentiality in the computer-based patient record. *MD Computing* 12(3):187–192, 1995.
13. Barrows, R. C., Jr., and Clayton, P. D., Privacy, confidentiality, and electronic medical records. *Journal of the American Medical Informatics Association* 3(2):139–148, 1996.
14. Borselius, N., Mobile agent security, electronics and communication. *Engineering Journal* 14(5):211–218, October 2002.
15. Maes, P., Guttman, R. H., and Moukas, A. G., Agents that buy and sell. *Communications of the ACM* 42(3):81–91, 1999.
16. Nechaev, V. I., Complexity of a determinate algorithm for the discrete logarithm. *Mathematical Notes* 55:165–172, 1994.
17. Stallings, W., Cryptography and Network Security-Principles and Practices, 3rd Edition, *Prentice Hall*, 2003.
18. Sulaiman, R., Huang, X., Sharma, D., "E-health Services with Secure Mobile Agent," *Proceedings of the 2009 Seventh Annual Communication Networks and Services Research Conference*, pp. 270–277, 2009.
19. Jiang, S., Xue, Y., Giani, A., Bajcsy, R., "Providing QoS Support for Wireless Remote Healthcare System," *International Conference on Multimedia and Expo,* pp. 1692–1695, 2009.
20. Kang, E., Youn, H. Y., Kim, U., "Mining Based Decision Support Multi-Agent System for Personalized E-Healthcare Service", *ProcEedings of the 2nd KES International Symposium on Agent and Multi-Agent Systems*, pp. 733–742, 2008.
21. Jen, W., Chao, C., Hung, M., Li, Y., and Chi, Y., Mobile information and communication in the hospital outpatient service. *International Journal of Medical Informatics* 76:565–574, 2007.
22. Markovic, M., Savic, Z., Kovacevic, B., "Secure Mobile Health Systems: Principles and Solutions, M-Health: Emerging Mobile Health Systems," *Kluwer Academic Publishers*, pp. 81–106, 2007.