This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings.

Preserving Privacy in Emergency Response Based on Wireless Body Sensor Networks

Jinyuan Sun*, Xiaoyan Zhu‡, and Yuguang Fang†‡
*Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996, USA
†Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611, USA
‡National Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China
Email: jysun@eecs.utk.edu, {xiaoyanzhu@, fang@ece.}ufl.edu

***Abstract*—E-healthcare is becoming a vital part of our living environment and exhibits advantages over paper-based legacy systems. Wireless body sensor networks are indispensable in one application of e-healthcare, the remote monitoring or remote care services. However, privacy is the foremost concern of the patients and the biggest impediment of the deployment of e-healthcare systems. In addressing privacy issues, conflicts from the functional requirements must be taken into account. One such requirement is the efficient and effective response to medical emergencies. In this paper, we propose to solve these conflicting goals based on suitable cryptographic schemes. In addition, security enhancements are proposed which satisfy other fundamental security goals besides the privacy requirements.**

I. Introduction

Advances in wireless communications and computing technologies fuel the migration of healthcare from paper-based systems to electronic health record (EHR) systems. E-healthcare systems offer great convenience to patients and healthcare providers, and improves the quality of life. One such example is the remote care application based on wireless body sensor networks, where the healthcare professionals remotely monitor the patients and provide consultation services. Remote care enables patients to retain their living style and causes minimal interruption to their daily activities. In addition, it significantly reduces the hospital occupancy rate, allowing more critical patients and patients who need in-hospital treatment to be admitted.

Despite the tremendous benefits, e-healthcare system easily incurs threats that are impossible or very rare in paper-based system. Privacy and security breaches have already penetrated e-healthcare systems, including EHR theft and insiders' selling EHRs for monetary gains [1]. Thus, there is an urgent need for the development of architectures/mechanisms assuring privacy and security that are imperative to safeguarding confidential or sensitive information wherever it digitally resides. The design of secure e-healthcare systems is envisioned to be complex, in that the highly confidential medical data are the basis for almost all operations. The creation, modification, deletion, storage, access, and sharing of such data need strict regulations. Due to the various and stringent requirements of e-healthcare systems, including security and functional requirements, cautions must be taken in the development of such systems to prevent the compromise of one requirement in the realization of another.

Privacy is the foremost issue concerning patients in e-healthcare. Without privacy guarantee, health information may be leaked to cause life-changing consequences to patients such as difficulties in obtaining insurance or employment, being discriminated for having certain diseases, etc. Most importantly, healthcare systems lacking privacy guarantees cannot be socially accepted and hence are not likely to be advocated and implemented. However, in certain special circumstances, such as emergencies, privacy requirement may obstruct the proper operation and thus need be overridden by the functional requirement, i.e., saving lives.

This work was partially supported by the U.S. National Science Foundation under grants CNS-0716450 and CNS-0916391.

Related Work. Security issues such as key management, authentication, and access control have been addressed for e-healthcare systems in [2], [3], [4], respectively. The proposed scheme differs from these works mainly in the employment of wireless body sensor network, which introduces unique security challenges such as more possible privacy breaches, and the difficulty incurred by using the wireless channel. A thorough survey on the challenges and opportunities of body sensor networks is provided in [5]. Key establishment and authentication within the body sensor network (BSN) have been the focus of [6], [7], and [8], exploring the unique functionalities of BSNs. These schemes rely on the physiological values (e.g., inter-pulse interval, heart rate variability) derived from sensor-collected biological signals (e.g., ECG or EKG, PPG), to generate symmetric keys for encryption among sensors, which may in turn be needed for authentication such as the challenge-response authentication proposed in [7]. This line of research explores the uniqueness of an individual's biological signals readily available in BSNs, and points out a promising research direction in applying cryptography to solving security problems. Our proposed scheme is not along this line in that we target at solving security issues between the BSN and the healthcare provider network. Similar to our senario which relies on BSNs, the work of Tan *et al.* [9] is a technical realization of the role-based approach proposed in [10]. In spite of specifying the algorithms for storing and retrieving healthcare records, the scheme in fact failed to achieve privacy protection in that the storage site will learn the ownership of the encrypted records (i.e., which records are from which patient) in order to return the desired records to the querying doctor. Such leakage will compromise patients' privacy by violating the unlinkability requirement. Experiments are conducted in [11] to deploy BSNs for monitoring the health condition of the patients in the waiting area of an emergency room. The results show the necessity of BSNs in the timely admission of patients with deteriorating or critical health conditions, and indicate the promising future of BSNs in assisting emergency healthcare.

Our Contributions. In this paper, we focus on the privacy issues introduced by incorporating wireless BSN as a vital component of the remote monitoring applications in healthcare. In our scenario, It is the role and access rights of the emergency medical technician (EMT) that complicates our design, in that the EMT can access the *relevant* medical data *if and only if* emergencies occur. As a result, we must first ensure that the EMT is able to obtain necessary data for emergency treatment. Furthermore, we need to guarantee that such access cannot take place under other circumstances (i.e.,

non-emergencies) or with respect to other medical data (i.e., data that are irrelevant or of little relevance). Identifying the above challenge in practice and proposing a sound and feasible solution are the main contributions of our paper. In addition, we propose security enhancements to fulfill other security objectives besides privacy.

The remaining sections are organized as follows. We introduce preliminary knowledge on the cryptographic techniques used for our scheme in Section II. Section III presents the system model including the network architecture, the threat model, and the security objectives we strive to achieve. Detailed descriptions and discussions of the proposed scheme are provided in Section IV, followed by the security analysis and enhancements in Section V. Finally, Section VI concludes the paper.

II. Preliminaries

This section introduces some preliminary knowledge on the cryptographic techniques used as building blocks of our proposed scheme.

A. Bilinear Pairings

Bilinear pairing operations are performed on elliptic curves. Let G_1 and G_2 be an additive group and a multiplicative group, respectively, of the same prime order q. Discrete logarithm problem (DLP) is assumed to be hard in both G_1 and G_2. Let P denote a random generator of G_1 and $e : G_1 \times G_1 \rightarrow G_2$ denote a bilinear map constructed by modified Weil or Tate pairing with the following properties:

1) Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$, $\forall P, Q \in G_1$ and $\forall a, b \in Z_q^*$, where Z_q^* denotes the multiplicative group of Z_q, the integers modulo q. In particular, $Z_q^* = \{x \mid 1 \leq x \leq q-1\}$ since q is prime.
2) Non-degenerate: $\exists P, Q \in G_1$ such that $e(P, Q) \neq 1$.
3) Computable: there exists an efficient algorithm to compute $e(P, Q), \forall P, Q \in G_1$.

Pairings are the basic operations used in the instantiation of the knowledge proofs involved in the registration, anonymous authentication, and data storage procedures of our scheme.

B. Commitment Scheme

In a commitment scheme, the committer commits to some value v by generating a commitment C on v using a committer-chosen number s. The committer can later show that the commitment C has indeed been computed from v and s, by revealing these two values to the verifier. The commitment scheme should be designed such that C reveals no information about v (i.e., the scheme is information-theoretically hiding), and the committer cannot open the commitment C by providing a value different from v (i.e., the committed value v is undeniable). The commitment scheme is useful when the committer does not want to disclose the committed value until after the final result is announced, e.g., in bidding. It is also useful to prevent the committer from modifying the committed value to gain benefits once the result is known, e.g., in bidding, horse betting.

Pedersen [12] proposed one of the earliest commitment schemes which is given as follows. Let g and h be the generators of a group G that is of prime order q. The committer commits to a value $v \in Z_q$ by choosing a random number $s \in Z_q$, and computes the commitment $C = g^v h^s$. The commitment C reveals no Shannon information about v under the discrete logarithm assumption. The commitment scheme is leveraged to construct the anonymous credential in the proposed scheme.

C. Proof of Knowledge

A proof of knowledge is an interactive proof where the prover convinces the verifier of the validity of a statement. In the case of a zero knowledge proof of knowledge, the above interactive proof is carried out without the prover revealing any information used to prove the statement. Let G be a cyclic group with generator g where solving the discrete logarithm is intractable. G is of prime order q. One can prove the knowledge of the discrete logarithm $x \in Z_q$ with respect to y in base g as $PK\{(x) : y = g^x\}$, which is the so-called Σ-protocol of three move structure: commitment, challenge, and response. Schnorr [13] first provided a construction for the Σ-protocol. The proof of knowledge technique is used for constructing the anonymous credential in the proposed scheme.

III. System Model

An overview of our application scenario leveraging wireless body sensor networks is provided in this section, along with the threat model and security objectives.

A. Remote Monitoring Based on Wireless Body Sensor Networks

As wireless technology and e-healthcare evolve, patients increasingly opt for home care and remote monitoring services offered by healthcare providers. Wireless body sensor network (WBSN) is indispensable for remote monitoring applications which reduce the hospital occupancy rate. It is also of paramount importance to monitoring patients in the waiting area of the emergency room [11], to detect deterioration of health conditions and correspondingly admit life-endangering patients. The most attractive feature of remote care is that patients can enjoy ease and comfort of living with minimal change while being treated. Furthermore, the wireless nature of the WBSN enables the patient to engage in daily activities without much constraint. The network architecture of the remote monitoring application is illustrated in Fig. 1.

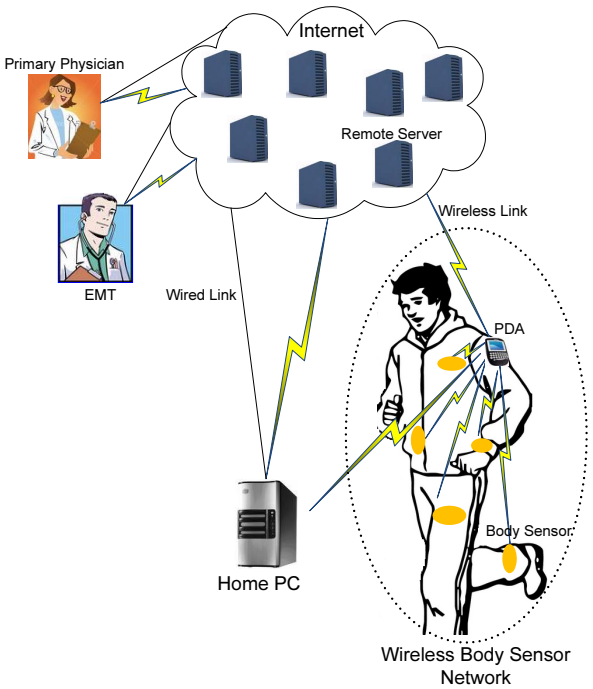

Fig. 1. Remote Monitoring Based on Wireless Body Sensor Network.

Body sensors serving different monitoring purposes, e.g., pulse oximetry sensor, ECG sensor, blood pressure sensor, motion sensor, are attached to or embedded into the human body. The WBSN

features short-ranged communications between the sensor and PDA, as well as between sensors (not shown in the figure), using Bluetooth and Zigbee radio technologies. Outside the WBSN, the PDA can communicate with home PC through Bluetooth connection when the patient is home. The wireless links between the PDA or home PC and the remote servers are in general based on Wi-Fi or WiMAX radio. The home PC can also access the Internet using legacy wired connections. The monitor centers, either independent or within a hospital, offer services and storage (i.e., remote servers) to patients under home or critical care. The monitored medical data outsourced to the remote servers can be retrieved by the primary physician for long-term evaluation, or by the emergency medical technician (EMT) for urgent care.

B. Threat Model

The entities engaged in the application scenario of our interest include the patient (i.e., the PDA), primary physician, EMT, and the remote server. The primary physician is fully trusted who can normally act on the patient's behalf for various operations involving the private medical data. The EMT and remote server, on the other hand, are assume honest-but-curious, in that they will not launch attacks to the medical data such as modification, deletion, injection of bogus data, to cause life-threatening consequences. However, they will attempt to compromise the patient's privacy which is defined in Section III.C, by illegally learning the content of the private medical data. Compared to the primary physician, the EMT has limited access rights to the patient's private information and thus is restricted to viewing only the allowed medical data (cf. Section IV). Furthermore, the remote server, EMT, and the credential authority (cf. Section IV.B) may collude in order to compromise the patient's privacy.

In addition, we assume that passive eavesdroppers will try to learn the content of the medical data. Active outside attackers will intercept and modify the medical data being transferred on the wireless link, or inject bogus data into the remote server to interrupt regular services.

C. Security Objectives

The primary security objective of the proposed scheme is privacy. Privacy concerned in our application scenario comprises anonymity, unlinkability, and location privacy requirements. Anonymity is two-fold: medical data anonymity and authentication anonymity. Medical data anonymity is demanded when the identifying information (e.g., name, social security number, mailing address) in the medical data need be hidden from certain parties. These parties include insurance companies, researchers, some management staff, and any related personnel that has no appropriate access privileges. Since these parties are not involved in the particular scenario we consider, medical data anonymity will not be the focus in this paper. However, as will be explained shortly, medical data anonymity must be guaranteed in order to achieve unlinkability. Authentication anonymity ensures that the patient is not identified when authenticating to the remote server for medical data storage in our scenario. It should be noted that the identity of a patient can be deduced from the IP address of the PDA that transmits the medical data over wireless networks, if the IP address of the PDA is identifiable. This vulnerability is associated with the employment of the wireless body sensor network.

Unlinkability requires that multiple medical data sent in different times cannot be linked to a same owner. This requirement is necessary because it prevents the profiling of a patient by the remote servers (i.e., the administrators) that store patient data, under the honest-but-curious model of the remote server. It is apparent that medical data anonymity is a prerequisite for unlinkability, since identifying information renders the medical data linkable.

Location privacy need be guaranteed in the remote care scenario, where the WBSN deployed to monitor a patient can be exploited to track the patient's whereabouts, through the IP address of the PDA when the medical data are wirelessly transferred to the server. When the patient is in normal health condition (i.e., emergency response is not needed), he/she should be considered as a regular network user enjoying wireless network services. In this case, location privacy of the patient should be preserved as is required for regular network users.

Fundamental security requirements such as authentication, data confidentiality and integrity need also be assured, to protect the network against illegitimate user/data, eavesdropping, and data alteration, respectively.

IV. The Proposed Privacy Preservation Scheme

As specified in the HIPAA (Health Insurance Portability and Accountability Act) regulation [14], privacy of the patient and his/her medical data should be overridden in emergencies, where the patient's consent on the use and disclosure of the medical data is not required. However, the emergency situation should not create an avenue for attacks and misbehavior. Therefore, the privacy requirements need still be guaranteed whenever the emergency care operations are not impeded.

The complication and challenges in system design arise from taking several, and possibly conflicting requirements into consideration. Such challenge is identified in our scenario (i.e., remote healthcare applications leveraging WBSNs) as the requirements for patient privacy and efficient response to emergency situations. The potential privacy breach in the emergency scenario is the linkability of stored medical data by the EMT. In particular, the role and access rights of the EMT differ from those of the primary physician, in that the EMT is interested in the most relevant data for efficient and effective first medical response. These data are typically recorded within the past few days (e.g., 3-5 days) which indicate the cause of the emergency. The primary physician, nevertheless, will demand outdated data to evaluate the general health condition and perform long-term treatment. The EMT will be abusing his/her access rights when attempting to review the medical data other than those necessary. As explained in Section III.C, linkability of the medical data can be coped with by ensuring the authentication anonymity and unlinkability requirements. It is, however, very challenging to achieve authentication anonymity and unlinkability in emergency care. On the one hand, the EMT should be able to obtain the relevant data for successful medical aid. On the other hand, irrelevant data stored in the same server but the access to which is not granted, should not be linked by the EMT to have originated from the same patient. We subsequently propose a solution to address these conflicting goals. Note that the medical data anonymity and location privacy requirements are overridden due to the need for accurately performing the emergency rescue.

A. Overview of The Proposed Scheme

We explicitly consider the scenario that the PDA of the patient transmits medical data to the remote server at the monitor center, facilitating emergency treatment carried out by the emergency medical technician (EMT). Since one of the benefits and purposes of deploying WBSNs is to render freeness and flexibility in the patient's daily life, the PDA will need to wirelessly deliver

medical data to the monitor center, when the patient is away and hence the home PC cannot be relied on. Depending on the configuration of WBSNs, the PDA collecting the medical data from body sensors, may send aggregated data periodically and critical data in real-time for relevant healthcare operations (either upon detecting abnormal conditions or upon the primary physician's query).

Our scheme is based on anonymous credentials, pseudorandom number generator (PRNG), and the assumptions made by the cryptographic techniques that serve as building blocks of our scheme. First of all, the patient registers at the credential authority, located at the medical monitor center where the patient is a subscribed user. The registration is essentially the procedure in which the patient obtains an anonymous credential from the credential authority, for future authentication with the remote server. This procedure is constituted by a commitment phase, a signature phase, and a credential derivation phase.

Next, (the PDA of) the patient performs mutual authentication with the remote server when the medical data are to be outsourced to the server. The patient can authenticate the server using the ID-based public/private key pair [15] of the server whose anonymity is not a concern. We will not further elaborate on this authentication which can be realized straightforwardly through digital signature. The server authenticates the patient using the anonymous credential which will be described in the following subsection.

The PDA then stores the monitored medical data collected in each time period under some random unlinkable sequence number, such that the EMT cannot arbitrarily link the medical data sent in different periods unless he/she is authorized by the patient.

When the body sensors detect abnormal biological signals indicating a possible emergency, the PDA immediately contacts the primary physician who will evaluate the situation and request emergency services if necessary. If the primary physician is irresponsive in a predefined short time, the PDA will automatically place an emergency call and seek for rescue. The EMT at the emergency scene will demand necessary medical data by sending the date range he/she is interested in to the PDA, which may only accept a reasonable range of recent dates. At this point, it is clear that our scheme can be considered as a stringent access control mechanism the patient exercises on the EMT, enabling him/her to properly carry out emergency medical care while restricting the access to only necessary information.

The above descriptions are summarized in Fig. 2 where the system entities, their interrelations and interactions are illustrated.

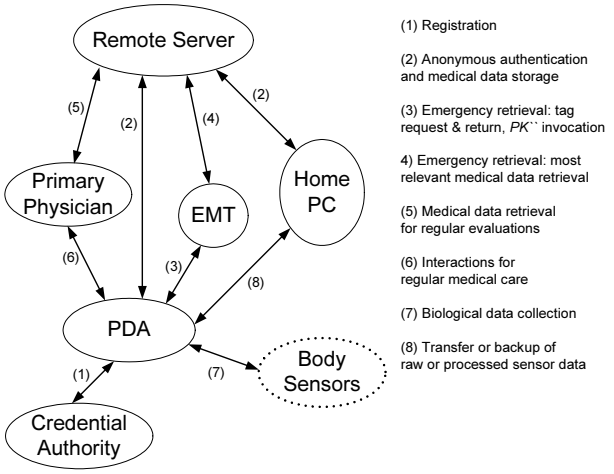

Fig. 2. Interrelations and Interactions of System Entities.

B. Technical Description of The Proposed Scheme

The technical details of the proposed scheme described above will be presented in what follows.

1. Registration:
    1) Commitment: The PDA sends (C, PK) to the credential authority, where C is a commitment on patient-chosen secrets $(\alpha, \beta) \in_R Z_q^*$ and PK is a proof of knowledge for the correct formation of C. The Pedersen commitment $C = g^\alpha h^\beta$ and the proof $PK\{(\alpha, \beta) : C = g^\alpha h^\beta\}$ are necessary in the correct issuance of anonymous credential, where g and h are generators of a multiplicative group G. This commitment and proof of knowledge are standard techniques used in anonymous credential systems [16]–[19].
    2) Signature: The authority inputs randomly selected parameters $r, r' \in_R Z_q^*$ to sign the commitment C using CL signature [20] or BBS signature [21], and returns the resulting signature σ and (r, r') to the patient for forming the credential.
    3) Derivation: The patient derives his/her anonymous credential $Cred$ using the information returned by the authority in 2) and his/her own secrets (α, β) as follows: $Cred = (\sigma, r, \alpha, \beta')$, where $\beta' = f(\beta, r')$. The function f denotes modular operations to compute β' taking β and r' as input, and is different in various anonymous credential systems such as [17]–[19]. We do not attempt to spell out the detailed instantiations since any credential system fulfilling the desired anonymous authentication functionality for our system can be adopted.

    Note that this credential will never be revealed after the derivation. The patient only needs to prove the knowledge of the possession of such a credential when authenticating with the remote server.
2. Anonymous authentication: The PDA sends PK' to the remote server, where PK' denotes the proof of the authenticity of the credential (i.e., the patient is a legitimate user of the monitor center services), and is constructed by the PDA taking $Cred$ as input and proving the knowledge of its components $(\sigma, r, \alpha, \beta')$. A possible formation of PK' can be found in [18] as $PK'\{(\sigma, r, \alpha, \beta') : \sigma^{r+S} = \tilde{g} g^\alpha h^{\beta'}\}$, where S is the authority's secret key and $\tilde{g}$ is a generator of G. The instantiation of this proof is based on bilinear pairings, the details of which are omitted here to avoid lengthy reproduction. Other possible formations and instantiations of proofs serving this purpose (i.e., proving the authenticity of an anonymous credential) can be found in [17], [19].
3. Data storage: After successful authentication, the PDA proceeds to store medical data on the remote server. Steps 1) and 2) show the preparation phase needed for emergency medical data retrieval. The actual data storage occurs in Step 3) which follows the authentication in Step 2.
    1) Serial number generation: The PDA randomly selects a secret seed η to feed into the PRNG, which generates pseudorandom serial numbers $(s_1 \cdots s_n)$ at the output, each for an update period (e.g., every 3-5 days) of the medical data. The number of s_i's generated in period

j, denoted by l_j, is also recorded by the PDA.

2) Tag computation: The PDA then computes tags based on the serial numbers as $t_i = (H(s_i))^\alpha$ for $i = 1 \cdots n$, such that t_i's appear random and unlinkable, where $H : \{0,1\}^* \rightarrow G$ denotes a cryptographic hash function.
3) Storage data formation: The PDA attaches (t_i, PK'') to the medical data sent in the jth period and stores them in the server, where $PK''\{\alpha : t_i = (H(s_i))^\alpha\}$ is the proof for the correct formation of the tag and can be easily instantiated using standard techniques. The reason for requiring this proof will be explained in Section IV.C below. After delivery to the monitor center, the medical data are erased from the PDA, along with t_i's, and s_i's. All the s_i's and t_i's can be efficiently re-generated by η, l_j's, and α.

4. Emergency retrieval: The PDA inputs η into the PRNG and reproduces the serial numbers s_i's for the desired data, based on the date range received from the EMT and l_j's. The serial numbers are in turn leveraged to reconstruct the corresponding t_i's, which will be returned to the EMT for retrieving the relevant data from the remote server.

C. Discussion

We present some alternatives to the proposed approach and discuss their unsuitability for the scenario considered. Basically, there are several other popular anonymous authentication techniques, namely, pseudonym, group signature, blind signature, k-time anonymous authentication, besides the anonymous credential used in this paper. In the pseudonym technique, the credential authority is generally required to issue a bunch of pseudonyms to a user and thus will link these pseudonyms to the real identity. The linkability can be removed by using the self-generated pseudonyms [22], which will cause problem in revocation. When the user needs to be revoked, e.g., the patient is not subscribed to the services any more, the self-generated pseudonyms which are only known to the user him/herself, can continue to be used for authentication rendering the revocation unattainable. The group signature, blind signature, and k-time anonymous authentication all enable the real identity of the user to be traced somehow (i.e., the group manager in group signature, double-spender tracing in blind signature, and public tracing in k-time anonymous authentication). In the proposed scheme, the anonymous credential used for authentication ensures that no entity is able to learn the identity of the patient under all circumstances. When the patient need be revoked, the credential authority can simply stop issuing anonymous credentials to the patient. This is possible since the patient must show his real identity to authenticate with the credential authority before the issuance of the credential (not shown in Section IV.B). However, the identity cannot be linked to the issued anonymous credential, which is known only to the patient as described in the derivation phase.

Another key design in the proposed scheme is the tag attached to each transferred medical data. The main purpose of the tag is to facilitate the patient and EMT to accurately locate desired medical data in emergencies, while not causing linkability to other medical data that are from the same patient but are not allowed for the EMT to access. Although some other techniques can be used for tagging the data, they would fail in one way or another in achieving the above purpose. Specifically, if the random numbers produced by a hash chain are used as tags, unlinkability will be broken if any number in the chain is returned to the EMT for data retrieval, in that other numbers down the chain can be calculated based on the given number. If we use a randomly-chosen number r, i.e., $r \in_R \{0,1\}^m$ where m denotes the bit length of r, as the tag, the PDA will need to store all these numbers or at least those likely to be queried, since these numbers cannot be reproduced. Note that in the data storage procedure above, the serial numbers s_i's generated by the PRNG would suffice to tag the medical data, ensuing both unlinkability and efficient retrieval. The reason for further computing the tag t_i's is to prevent the potential man-in-the-middle attack by assuring data authenticity. The attack can be launched during the EMT's retrieval of medical data from the remote server in emergencies. The attacker can pose as the server and return fake data to the EMT to undermine the emergency rescue work. In our scheme, the EMT is ascertained of the authenticity of the medical data by verifying the proof of knowledge PK'' on the formation of the tag, which cannot be correctly produced by the attacker without knowing the patient's anonymous credential.

V. Security Analysis and Enhancements

The previous section elaborates on the assurance of the unlinkability and authentication anonymity requirements in emergencies. In this section, we present the techniques that have achieved unlinkability and authentication anonymity. In addition, we propose security enhancements to the main scheme described in Section IV, for satisfying the remaining requirements defined in Section III.C, i.e., medical data anonymity, location privacy, authentication, confidentiality, and integrity, which should be guaranteed when no emergency takes place.

Authentication. We are concerned with the authentication performed by the remote server towards the patient, which must be anonymous. It can be achieved by the patient proving the knowledge (i.e., PK') of the anonymous credential issued by the credential authority, as described in Section IV.B. In the authentication performed by the patient, standard (non-anonymous) technique such as digital signature can be used since no other entities in the considered scenario require anonymity. Furthermore, we do not require the EMT to authenticate the patient in emergencies because all emergency calls should be responded. However, the patient's PDA and remote server may need to authenticate the EMT upon emergency to ensure the legitimacy of the EMT, which can simply be realized through standard digital signature.

Privacy. Recall that privacy consists of authentication anonymity, medical data anonymity, unlinkability, and location privacy. The authentication anonymity is basically guaranteed during the anonymous authentication just mentioned. This anonymity is unconditional in the sense that even if the collusion among the EMT, remote server, and credential authority is allow, the authentication anonymity cannot be compromised, since no useful information will be deduced by such collusion to link the real identity of a patient to the ongoing or past anonymous authentication. Moreover, the IP address of PDA from which the authentication messages and subsequent medical data are transmitted, can be exploited to identify the patient. We therefore need an additional mechanism, an anonymous communication network such as [23] to obfuscate the source IP address, preventing the attackers from observing the traffic origin. Medical data anonymity can be fulfilled using the anonymization technique [24] which removes the identifying information from the medical data and creates ambiguity. The monitored medical data thus contain two parts: the outcome of the anonymization (i.e., de-identifying information), and the identifying information encrypted under the EMT's role-based public key (see below). Unlinkability is assured by both the medical data anonymity which eliminates linkable information from the

medical data, and the random unlinkable tags indispensable for the efficient retrieval of the stored medical data. Since t_i's are unlinkable, the EMT cannot arbitrarily review the patient's data for which the t_i's are not returned by the PDA to the EMT. To satisfy the requirement of location privacy, the aforementioned anonymous communication substrate [23] will suffice.

Confidentiality. Note that the PDA does not encrypt the entire medical data during storage, in that if the data are to be accessed by other roles (e.g., primary physician, nurse), it will result in multiple encryptions on the same data, once for each role, dramatically increasing the computation, communication, and storage overhead. Instead, only identifying data which should be kept confidential are encrypted, under the role-based public key. Role-based encryption leveraging ID-based cryptosystem (IBC) [15], is the *de facto* technique in the fine-grained control of the access to confidential data, indicating the need for IBC as the public key infrastructure (PKI) in our application scenario. The role-based technique enables the patient to encrypt medical data under the EMT's role-based public key (specifying a general role instead of a particular identity) in advance of the actual emergencies, when the patient is uncertain about which specific EMT will be providing the emergency service. Since the medical data are partially encrypted, the anonymization technique should also remove sensitive information (e.g., certain types of disease) in addition to the identifying information, to prevent the eavesdroppers or active attackers who intercept the data to learn any information that may be of interest.

Integrity. Message authentication code (MAC) and digital signature can be leveraged to protect medical data integrity from illegal modification. In particular, MAC requires a shared key between the two communicating parties. Since there is normally a pre-shared key between the patient and primary physician, MAC can be employed for the integrity assurance on the medical data intended for the primary physician. MAC is not suitable for communications with the EMT, in that the patient cannot establish the key without knowing which EMT will treat him/her in the emergency. One solution is to allow the primary physician to delegate the EMT upon emergency, by revealing the shared key for verifying MAC. The downside of this approach is that the patient and primary physician have to re-establish the shared key after the emergency, since this key is normally also useful for other security operations such as encryption. In addition, if the primary physician is unavailable at the time of emergency, the patient could be delayed for treatment. For the more general case where no shared key is possible, digital signature can be adopted instead. However, pseudonym should be used as the ID-based public key in lieu of the real identity which will undermine the privacy guarantee. Although pseudonym renders revocation intractable as explained in Section IV.C, it is only used for integrity (not authentication) and will not affect the proper revocation. If the patient no longer subscribes to the monitor service and thus need be revoked, he/she cannot successfully authenticate with the server and will not be able to outsource the medical data to the server.

Due to space limitations, we cannot cover the efficiency analysis which will be presented in the full version of this paper.

VI. Conclusion

In this paper, we propose to solve the conflicts between the privacy requirements and the functional requirement by identifying the unique security challenges in our application scenario. Through the analysis, we demonstrate that the privacy requirements are satisfied while no impediment is caused for the emergency care, and that the proposed scheme is efficient in terms of storage and computation. We also propose security enhancements, leveraging both cryptographic and non-cryptographic (e.g., anonymization) techniques, to fulfill other security objectives besides the privacy requirements addressed in the main scheme.

References

[1] P. Ray and J. Wimalasiri, "The need for technical solutions for maintaining the privacy of EHR," *in Proc. 28th IEEE EMBS Annual International Conference*, pp. 4686–4689, Sept. 2006.

[2] W.-B. Lee and C.-D. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," *IEEE Trans. Information Technology in Biomedicine*, Jan. 2008.

[3] G. Ateniese, R. Curtmola, B. de Medeiros, and D. Davis, "Medical information privacy assurance: cryptographic and system aspects," *in 3rd Conference on Security in Communication Networks (SCN'02)*, Sept. 2002.

[4] L. Zhang, G. J. Ahn, and B. T. Chu, "A rule-based framework for role-based delegation and revocation," *ACM Transactions on Information and System Security*, vol. 6, no. 3, pp. 404–441, 2003.

[5] M. A. Hanson, H. C. Powell Jr., A. T. Barth, K. Ringgenberg, B. H. Calhoun, J. H. Aylor, and J. Lach, "Body area sensor networks: Challenges and opportunities," *Computer*, pp. 2455–2458, Jan. 2009.

[6] S. Gupta, K. K. Venkatasubramanian, and A. Banerjee, "Ekg-based key agreement in body sensor networks," *Mission Critical Networks Workshop (MCN'08)*, Apr. 2008.

[7] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems," *in Proc. 28th IEEE EMBS Annual International Conference*, pp. 58–65, Sept. 2005.

[8] S.-D. Bao, C. C. Y. Poon, Y.-T. Zhang, and L.-F. Shen, "Using the timing information of heartbeats as an entity identifier to secure body sensor network," *IEEE Trans. Information Technology in Biomedicine*, vol. 12, no. 6, pp. 772–779, Nov. 2008.

[9] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "Body sensor network security: an identity-based cryptography approach," *The ACM Conference on Wireless Network Security (WiSec'08)*, Apr. 2008.

[10] M. C. Mont, P. Bramhall, and K. Harrison, "A flexible role-based secure messaging service: Exploiting IBE technology for privacy in health care," *in Proc. 14th International Workshop on Database and Expert Systems Applications (DEXA'03)*, 2003.

[11] D. W. Curtis et al., "SMART: Integrated wireless system for monitoring unattended patients," *Journal of the American Medical Informatics Association*, vol. 15, no. 1, pp. 44–53, Jan. 2008.

[12] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," *in Proc. CRYPTO'91, LNCS, Springer Verlag*, vol. 576, pp. 129–140, 1992.

[13] C.-P. Schnorr, "Efficient signature generation by smart cards," vol. 4, no. 3, pp. 161–174, Jan. 1991.

[14] G. M. Stevens, "A brief summary of the medical privacy rule," *CRS Report for Congress*, 2003.

[15] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing. extended abstract in CRYPTO 2001," *SIAM J. of Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[16] J. Camenisch and A. Lysyanskaya, *Signature Schemes and Anonymous Credentials from Bilinear Maps*, in Advances in Cryptology: CRYPTO'04, LNCS 3152, 2004.

[17] J. Camenisch *et al.*, "How to win the clonewars: efficient periodic n-times anonymous authentication," *in ACM Conference on Computer and Communications Security (CCS)*, pp. 201–210, 2006.

[18] P. Tsang, M. H. Au, A. Kapadia, and S. W. Smith, "Blacklistable anonymous credentials: Blocking misbehaving users without TTPs," *in ACM Conference on Computer and Communications Security (CCS)*, pp. 72–81, 2007.

[19] L. Nguyen and R. Safavi-Naini., "Dynamic k-times anonymous authentication," *in Applied Cryptography and Network Security Conference*, vol. 3531, pp. 318–333, 2005.

[20] J. Camenisch and A. Lysyanskaya, *A Signature Scheme with Efficient Protocols*, in SCN 2002, LNCS 2576, 2002.

[21] D. Boneh, X. Boyen, and H. Shacham, *Short group signatures using strong diffie hellman*, in CRYPTO'04, Springer Verlag, 2004.

[22] S. M. M. Rahman, A. Inomata, T. Okamoto, M. Mambo, and E. Okamoto, "Anonymous secure communication in wireless mobile ad-hoc networks," *in Proc. 1st Intl. Conf. on Ubiquitous Convergence Technology*, pp. 131–140, Dec. 2006.

[23] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," *in Proc. USENIX Security Symposium*, pp. 303–320, Aug. 2004.

[24] K. E. Emam and F. K. Dankar, "Protecting privacy using k-anonymity," *Journal of the American Medical Informatics Association*, vol. 15, no. 5, pp. 627–637, Sept. 2008.