Towards Auditable Cloud-Assisted Access of Encrypted Health Data

Yue Tong*, Jinyuan Sun*, Sherman S. M. Chow†, and Pan Li‡
* Department of Electrical Engineering and Computer Science
University of Tennessee, Knoxville, TN 37996, USA
Email: {ytong3, jysun}@utk.edu
† Department of Information Engineering
Chinese University of Hong Kong, Sha Tin, N.T., Hong Kong
Email: sherman@ie.cuhk.edu.hk
‡ Department of Electrical and Computer Engineering
Mississippi State University, MS 39762, USA
Email: li@ece.msstate.edu

***Abstract*—Motivated by the privacy issues curbing the adoption of electronic healthcare systems and the wild success of cloud service models, we propose to build privacy into electronic healthcare systems with the help of private cloud. Our system offers salient features including privacy-preserving data access, especially during emergencies, and auditability for misusing health data. Specifically, we propose to integrate the concept of attribute-based encryption with threshold signing for providing role-based access control with auditability to prevent potential misbehavior, in both normal and emergency cases.**

I. Introduction

Fast access to health data enables better healthcare service provisioning, improves quality of life and helps saving life by assisting timely treatment in medical emergencies. Anywhere-anytime-accessible electronic healthcare systems play a vital role in our daily life. Services supported by mobile devices, such as home care and remote monitoring, enable patients to retain their living style and cause minimal interruption to their daily activities. In addition, it significantly reduces the hospital occupancy, allowing patients with higher need of in-hospital treatment to be admitted.

While these e-healthcare systems are increasingly popular, a large amount of personal data for medical purpose are involved, and people start to realize they would completely lose control over their personal information once it enters the cyberspace. According to U.S. Department of Health and Human Services [1], around 8 million patients' health information was leaked in the past two years. There are good reasons for keeping medical data private and limiting the access. For example, an employer may decide not to hire someone with certain diseases. Despite the paramount importance, privacy issues are not addressed adequately at the technical level and efforts to keep health data secure have often fallen short. This is because protecting privacy in the cyberspace is significantly more challenging. Thus, there is an urgent need for the development of viable protocols, architectures and systems assuring privacy and security to safeguard sensitive and personal digital information.

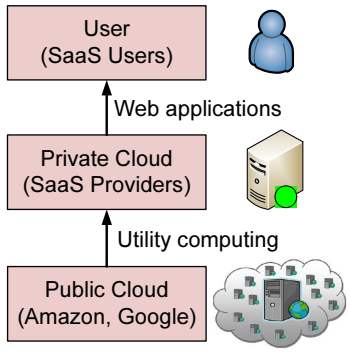

Fig. 1. The SaaS Service Model

Outsourcing data storage and computational tasks becomes a popular trend as we enter the cloud computing era. A wildly successful example is Amazon's EC2 (Elastic Compute Cloud) service used by TC3 (Total Claims Capture & Control), which provides claim management solutions for healthcare payers such as Medicare payers, insurance companies, municipalities, and self-insured employer health plans. Their clients send in tens of millions of claims daily which contain sensitive health information. Outsourcing the computation to the cloud saves TC3 from buying and maintaining servers, and allows TC3 to take advantage of Amazon's expertise to process and analyze data faster and more efficiently. The proposed cloud-assisted electronic health networking is inspired by the power, flexibility, convenience, and cost

978-1-4799-0895-0/13/$31.00 ©2013 IEEE

efficiency of the cloud-based data/computation outsourcing paradigm.

We introduce the private cloud which can be considered as a service offered to mobile users. The proposed solutions are built on the service model shown in Fig. 1. A SaaS (Software as a Service) provider provides private cloud services by using the infrastructure of the public cloud providers (*e.g.*, Amazon, Google). Mobile users outsource data processing tasks to the private cloud which stores the processed results on the public cloud. The cloud-assisted service model supports the implementation of practical privacy mechanisms since intensive computation and storage can be shifted to the cloud, leaving mobile users with lightweight tasks.

II. Related Work

Some early works on privacy protection for e-health data concentrate on the framework design [2], [3], [4], [5], [6], including the demonstration of the significance of privacy for e-health systems, the authentication based on existing wireless infrastructure, the role-based approach for access restrictions, *etc*. In particular, identity-based encryption [7] has been used [3] for enforcing simple role-based cryptographic access control. Among the earliest efforts on e-health privacy, MIPA [4] pointed out the importance and unique challenges of medical information privacy. MIPA was one of the first few projects that sought to develop privacy technology and privacy-protecting infrastructures to facilitate the development of a health information system, in which individuals can actively protect their personal information. We followed our line of research [8], [9], [10], [11], [12], [13] with other collaborators and summarized the security requirements for e-health systems in [10], [13].

There is also a large body of research works on privacy-preserving authentication, data access and delegation of access rights in e-health systems [14], [15], [16], [11], [17], [18], [19], [5], [6], [20], [21], among which [16], [20], [21] are most related to our proposed research. Benaloh *et al.* [20] proposed the concept of patient-controlled encryption (PCE) such that health-related data is decomposed into a hierarchy of smaller piece of information which will be encrypted using the key which is under the patients' control. They provided a symmetric-key PCE for fixed hierarchy a public-key PCE for fixed hierarchy, and a symmetric-key PCE for flexible hierarchy from RSA. The first public-key PCE for flexible hierarchy from pairings is proposed by Chu *et al.* [21]. The system of Li *et al.* [16] utilizes multi-authority attribute-based encryption [22], [23] proposed by Chase and Chow for fine-grained access control. Their system allows break-glass access via the use of "emergency" attributes. However, it is not clear who will take on the role of issuing such a powerful decryption key corresponding to this attribute in practice.

Finally, we also remark that there are other cryptographic mechanisms for privacy-preserving access of general data stored in a cloud environment [24], [25].

III. Preliminaries

A. Threshold Secret Sharing

Secret sharing refers to a mechanism for distributing secret information to multiple entities to eliminate cryptographic power centralization and avoid single point of failure. Shamir [26] considered the problem of dividing some information I into n pieces $I_1, \cdots, I_n$, such that knowledge of any k or more of these I_i $(i \in [1,n])$ pieces can recover I while knowledge of $(k-1)$ or fewer pieces keeps I completely undetermined. Such a scheme is referred to as a (k,n) threshold scheme which is computed based on polynomial interpolation. Suppose the secret a_0 is in an additive group $\mathbb{G}$ of prime order q. Define a $(k-1)$ degree polynomial $y(x) = a_0 + \sum_{i=1}^{k-1} a_i x^i$ with $a_0 = I \in \mathbb{G}$, where $a_1, \cdots, a_{k-1}$ are randomly chosen from $\mathbb{G}$. Let $I_i = y(i), i \in [1,n]$ and $\Phi \subseteq \{I_1, \cdots, I_n\}$ with $|\Phi| \geq k$, where $|\cdot|$ denotes the cardinality of the given set. The I_i values in Φ and the indices i can be used to reconstruct the original information $I = y(0) = a_0$ by computing $y(x) = \sum_{j \in \Psi} \rho_{xj}^{\Psi} I_j$, where $\rho_{xj}^{\Psi} = \prod_{l \in \Psi, l \neq j} \frac{x-l}{j-l} \in \mathbb{Z}_q$ is the Lagrange coefficient for a set $\Psi \subseteq \{1, \cdots, n\}$ with $|\Psi| \geq k$.

B. Identity-Based Encryption

A practical identity-based encryption (IBE) scheme in the random oracle model was proposed by Boneh and Franklin [7]. Identity-based systems allow any party to generate a public key from a known identity value, for example, the string "alice@xyz.com" for Alice. IBE makes it possible for any parties to encrypt message with no prior distribution of keys between individuals. It is an important application of the pairing-based cryptography. Below we review some technical details of Boneh-Franklin IBE.

To set up IBE, we need to define the public parameters for the pairing groups. Let $\mathbb{G}_1$ be a group with prime order q, $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be a bilinear map, and g be a generator of $\mathbb{G}_1$. Let $\hat{g} = e(g,g) \in \mathbb{G}_2$. Let $h_1 : \{0,1\}^* \to \mathbb{G}_1$ and $h_2 : \{0,1\}^* \to \mathbb{G}_2$ be hash functions to be modelled as random oracles.

The Private Key Generator (PKG) in the IBE cryptosystems picks $s \overset{R}{\leftarrow} \mathbb{Z}_q$ as the the private master key and g^s as the master public key. When anyone wants to send a message m to Alice, she picks $r \overset{R}{\leftarrow} \mathbb{Z}_q$ and computes $\texttt{Encrypt}((g, g^s), \text{“}Alice\text{”}, m)$ by $(u,v) = (g^r, m \oplus h_2(e(h_1(\text{“}Alice\text{”}), g^s)^r))$ which in turns equal to $(g^r, m \oplus h_2(e(h_1(\text{“}Alice\text{”}), g)^{rs}))$ by bilinearity of e.

Before decrypting the message, Alice needs to get her private key from PKG, who computes and send to Alice through a secure channel $\texttt{KeyExt}(s, \text{“}Alice\text{”}) = h_1(\text{“}Alice\text{”})^s$. With this private key, denoted by $w = h_1(\text{“}Alice\text{”})^s$, and a ciphertext (u,v), Alice now can decrypt it as $\texttt{Decrypt}((u,v), w) = v \oplus h_2(e(w,u)) = m \oplus$

$h_2(e(h_1(\text{“}Alice\text{”}), g)^{rs}) \oplus h_2(e(h_1(\text{“}Alice\text{”})^s, g^r)) = m \oplus h_2(e(h_1(\text{“}Alice\text{”}), g)^{rs}) \oplus h_2(e(h_1(\text{“}Alice\text{”}), g)^{rs}) = m.$

Boneh and Franklin has also described how to secret share the master secret key s [7].

C. Attribute-Based Encryption

Attribute-based encryption (ABE) [27]can provide fine-grained access control for sensitive data, which is especially useful for data outsourcing. Typically, data is encrypted by the owner under a set of attributes. The parties accessing the data are assigned access structures by the owner and can decrypt the data only if the access structures match the data attributes.

Existing papers most relevant to our scheme have followed the approach to define a set of attributes for each single data file [16]. Each file is then encrypted under the associated attributes [16]. However, using the ABE-based access control alone cannot audit who has accessed which data. ABE serves as a gatekeeper to prevent unauthorized parties from decrypting the data. However, it does not provide any mechanism for auditability, *i.e.*, to record and prove that an authorized party has accessed certain data. Without auditability, it is not possible to identify the source of breach if authorized parties illegally distribute the health data which will be discussed in our future research issues. Furthermore, in our use of ABE, the user (and his/her primary physician) will have no clue about whether an authorized party has properly accessed the data without auditability.

IV. System and Threat Models

A. System Model

Our system model is depicted in Fig. 2. A user refers to a person and the associated computing facilities. Users collect their health data through the monitoring devices worn or carried, *e.g.*, electrocardiography sensors, health tracking patches. The computing facilities are mainly mobile devices carried around such as smartphone, tablet, or PDA. Emergency medical technician (EMT) is a physician who performs emergency treatment. It refers to the person and the associated computing device.

Each user is associated with one private cloud. Multiple private clouds are supported on the same physical server. Private clouds are always online and available to handle health data on behalf of the users. This can be very desirable in situations like medical emergencies.

We assume that at the bootstrap phase, there is a secure channel between the user and his/her private cloud, *e.g.*, secure home Wi-Fi network, to negotiate a long-term shared-key. After the bootstrap phase, the user will send health data over insecure network to the private cloud residing via the Internet backbone.

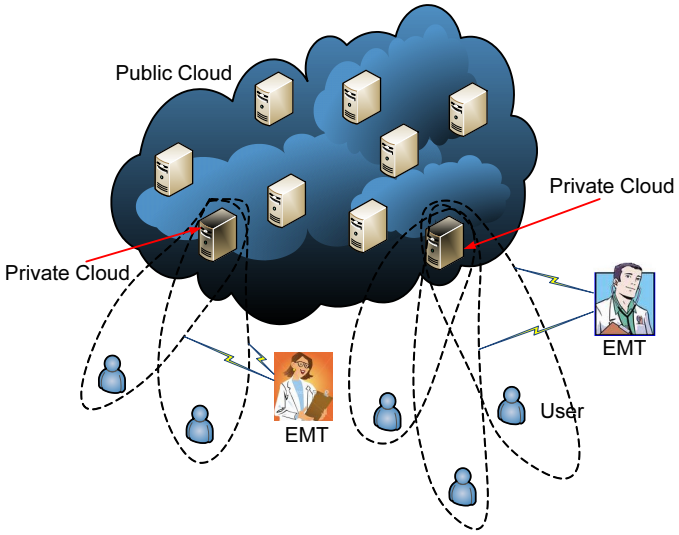

Fig. 2. Cloud-assisted Electronic Health System

B. Threat Model

The private cloud is fully trusted by the user to carry out health data related computations. Public cloud is assumed to be honest-but-curious, in that they will not delete or modify users' health data, but will attempt to compromise their privacy. Public cloud is not authorized to access any of the health data.

The EMT is granted access rights to the data only pertinent to the treatment, and only when emergencies take place. The EMT will also attempt to compromise data privacy by accessing the data he/she is not authorized to. The EMT is assumed to be rational in the sense that he/she will not access the data beyond authorization if doing so is doomed to be caught. Finally, outside attackers will maliciously drop users' packets, and access users' data though they are unauthorized to.

Under this threat model, we strive to achieve achieve the following security goals.

- **Data access privacy:** The user is enabled to authorize the access in a fine-grained manner, meaning that the data requestor, be it an EMT or other not-fully-trusted party can only access the data only pertinent to the treatment.
- **Auditability:** In emergency data access, the users may be physically unable to grant data access or without the perfect knowledge to decide if the data requestor is a legitimate EMT. We require authorized parties' access activities to leave a cryptographic evidence for auditing later.

V. Our Design for Cloud-assisted Access of Encrypted Health Data with Auditability

Upon receiving the health data from users, private cloud processes and stores it in the public cloud with related secure mechanism such as [11] such that storage privacy and efficient retrieval can be guaranteed. Following the storage in the public cloud, the private cloud engages in the bootstrapping of data access and auditability scheme with users so that it can later act on the users' behalf to exercise access control and auditing on authorized parties.

Data access privacy during emergencies where the emergency medical technician (EMT) requests data through the private cloud. The proposed approach is for the general data access, although we focus on the emergency access since it is more challenging. Our preliminary work [11] for emergency access is based on a personal device which is subject to theft, loss and dead battery and cannot meet the requirement of anytime anywhere accessibility.

A. Approach Overview

To overcome this problem, we propose to combine threshold signature with ABE-based access control. A (k, n) threshold signature (*e.g.*, [28]) guarantees that a valid signature on a message can be generated as long as there are k valid signature shares. For instance, we can set $n = 5$ representing the private cloud, the primary physician, the EMT, the specialists (*e.g.*, pediatrician, urologist), and the insurance provider. The private cloud and primary physician are fully trusted by the user. Let $k = 2$ such that any not-fully-trusted party must perform the threshold signing with either fully-trusted party. In reality, for example, the EMT better performs the signing with the private cloud because the primary physician may not be available online at all times. On the other hand, a pediatrician better performs the signing with the primary physician since users normally rely on their primary physicians for referral to a specialist. We do not further elaborate on this issue but use the emergency access case to describe the detailed design. The user serves as the trust dealer in the threshold signature to assign each participating party a secret share that is essential for generating the valid signature share.

In our design, users can use their favorite mechanism to encrypt their health data. For example, [11]. For the emergency access, users also uses an IBE to encrypt the data. We note that such kind of break-glass access mechanism does not need to invoked as frequent as other daily operations, but it requires auditability which is not a concern for daily decryption. Hence, it may not be desirable to be tightly coupled with the regular encryption mechanism, in contrast to existing approach such as [16].

For this second part of the encryption, the master key of the IBE will be shared among a number of authorized parties. Upon emergency access, a threshold number of them must be contacted to generate shares of the IBE decryption keys which can be used for decrypting an IBE ciphertext. Note that each share of the decryption key will serve as a signature from the corresponding authorized party. In other words, this will provide the auditability since the share-issuing party cannot later deny having done so. In particular, these parties should check that a) the request was due to a true medical emergency, and b) the EMT has requested data only pertinent to the treatment, In doing so, users avoid the daunting task of determining who can access which data file(s). Instead, only the encryptor needs to prepare beforehand an IBE ciphertext for the same data, and the job of determining who can access their data and assign a secret share correspondingly will be performed by the authorized parties.

B. Enabling Protocols and Cryptographic Mechanisms

Here we use Boneh-Franklin IBE [7] for concreteness of discussion. Any IBE supporting threshold decryption can do, *e.g.*, see [29], [30], [31].

1) Bootstrap Stage: Through bootstrap stage, the user secret-shares a key to n participating parties.

- User defines some parameters for threshold signing controlled IBE. Let $H : \{0,1\}^* \rightarrow \mathbb{G}$ be a hash function. Let $\mathbb{G}_1$ be a bilinear group of prime order p_1, g be a generator of $\mathbb{G}_1$, and $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a bilinear map.
- In our design, user serves as the PKG of cryptographic system in the sense that user picks $x \overset{R}{\leftarrow} \mathbb{Z}_q$ as the the private master key and computes g^x as the public master key. For EMT, user computes $\texttt{KeyExt}(x, \text{“}EMT\text{”}) = H(\text{“}EMT\text{”})^x$ as the private key. However, note that EMT's private key $H(\text{“}EMT\text{”})^x$ will not be sent to the EMT, at least not in a direct way, which is different from the regular use of IBE.
- User (k, n)-shares x such that any subset S of size k or larger can reconstruct x. We denote each secret share by x_i, which is obtained in the way we detailed in Section II. To do that, user first defines a secret $(k-1)$ degree polynomial $y(s) = x + \sum_{i=1}^{k-1} a_i s^i$. Then, x_i is given by $x_i = y(i)$.
- The secret shares will be issued to the set of authorized parties, such as the private cloud, the primary physician, the EMT, the specialists, and the insurance provider, as we previously mentioned.
- User setups the ABE mechanism, and issues the decryption keys according to the decryption right each entity is entitled to.

2) Encryption Stage:

- The data originator ABE-encrypts the health data according to the data nature.
- The data originator also IBE-encrypts the same piece of health data, under the identity “EMT”.

- The ciphertext $(ABE(m), IBE_{\text{“}EMT\text{”}}(m))$ for health data m will be uploaded to the cloud.

3) Decryption Stage:

- Regular decryption can be trivially done via the use of ABE.
- When EMT needs to access the health data in emergency, EMT contacts a threshold number t of authorized parties. For example, when party i decided to grant this access, $\sigma_i = H(\text{“}EMT\text{”})^{x_i}$ will be sent to the EMT.
- The EMT submit the requests together with a sufficient number of shares $\{\sigma_i\}$ to the private cloud.
- The private cloud then generate the decryption key $\sigma = \prod_{i \in S}(\sigma_i^{L_i})$ where $L_i = \prod_{l \in \Psi, l \neq j} \frac{s-l}{j-l}$ with Ψ being the set of participants that grant their secret shares to the data requestor. Its validity can be verified by checking if $(g, g^x, H(\text{“}EMT\text{”}), \sigma)$ is a valid Diffie-Hellman tuple via the use of the bilinear map e. To be more specific, the private cloud check if $e(g^x, H(\text{“}EMT\text{”})) = e(g, \sigma)$ holds. If EMT collects sufficient number of valid secret shares, he/she should be able to recover $\sigma = H(\text{“}EMT\text{”})^x$. By the definition of bilinear map, $e(g^x, H(\text{“}EMT\text{”})) = e(g, H(\text{“}EMT\text{”}))^x = e(g, H(\text{“}EMT\text{”})^x)$
- Private cloud retrieves the relevant ciphertexts, possibly from the public cloud, decrypts it with σ, and send it back to the EMT.

The computational load on the mobile user is light since secret sharing needs to be performed once and for all.

C. Analysis

Since the user has no way of knowing which specific person will request data access in case of emergency, it is impossible for the user to use complicated mechanism such as ABE for break-glass access. On the other hand, in reality, a party trusted by all users is unlikely to exist. With these two observations, we use a simpler IBE mechanism, but secret-share its secret such that no single point of trust is assumed.

Fine-grained access control is achieved by the underlying ABE mechanism. The threshold signature exchange used in our scheme enables the private cloud to record evidence that is signed by the authorized parties which can be used as audit logs. By employing a mechanism which a signature can also be used as a decryption key, users can later check whether the request is legitimate and appropriate, and simultaneously, be assured that the EMT cannot deny a request and the private cloud cannot falsely accuse an EMT.

Since the mobile users outsource most of their computations to the private cloud and most storage to the public cloud, the computation and storage costs at the mobile side are expected to be highly practical. Due to the space limitation, we omit our simulation results on these costs of the mobile users, which should be apparent from the simplicity of our approach. Note that a downside of being cost-efficient is the potential security breach if the private cloud acts maliciously. With our current schemes, as long as the private cloud is honest, our privacy guarantees cannot be broken even if all entities collude. We argue that a private cloud, by definition, should be highly trustworthy. Otherwise, it is difficult to attract users to pay for the service.

VI. Conclusion

In this paper, we proposed to build access privacy and auditability into electronic health systems with the help of private cloud. We investigated techniques that provide access control (in both normal and emergency cases) and auditability of the authorized parties to prevent misbehavior, by attribute-based encryption, identity-based encryption, and threshold signing. As our future work, we plan to devise mechanisms that can detect whether users' health data has been illegally distributed, and identify possible source(s) of leakage (*i.e.*, the authorized party that did it).

Acknowledgement

The work of J. Sun was supported by the Engineering Research Center Program of the National Science Foundation and the Department of Energy under NSF Award Number EEC-1041877 and the CURENT Industry Partnership Program. Sherman Chow is supported by the Early Career Scheme and the Early Career Award of the Research Grants Council, Hong Kong SAR (CUHK 439713), and Direct Grant (4055018) of the Chinese University of Hong Kong. The work of P. Li was supported by the U.S. National Science Foundation under Grant CNS-1149786.

References

[1] U.S. Department of Health & Human Service, "Breaches Affecting 500 or More Individuals." http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

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

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

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

[5] L. Zhang, G. J. Ahn, and B. T. Chu, "A role-based delegation framework for healthcare information systems," *SACMAT, Monterey, California*, pp. 125–134, 2002.

[6] 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.

[7] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM J. of Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[8] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Trans. Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227–1239, 2010.

[9] J. Sun, X. Zhu, and Y. Fang, "Preserving privacy in emergency response based on wireless body sensor networks," *Proc. IEEE Globecom Conf.*, Dec. 2010.

[10] J. Sun, X. Zhu, and Y. Fang, "Privacy and emergency response in e-healthcare leveraging wireless body sensor networks," *IEEE Wireless Communications*, vol. 17, pp. 66–73, Feb. 2010.

[11] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," *IEEE Intl. Conf. on Distributed Computing Systems (ICDCS'11)*, June 2011.

[12] L. Guo, C. Zhang, J. Sun, and Y. Fang, "PAAS: Privacy-preserving attribute-based authentication system for eHealth networks," *IEEE Intl. Conf. on Distributed Computing Systems (ICDCS'12)*, June 2012.

[13] J. Sun, X. Zhu, C. Zhang, and Y. Fang, *Security and Privacy for Mobile Healthcare (m-Health) Systems*. in *S. Das, K. Kant and N. Zhang (Eds.): Handbook on Securing Cyber-Physical Infrastructure*, 2011.

[14] W.-B. Lee and C.-D. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," *IEEE Trans. Information Technology in Biomedicine*, vol. 12, pp. 34–41, Jan. 2008.

[15] 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.

[16] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.

[17] X. Liang, R. Lu, X. Lin, and X. Shen, "Patient self-controllable access policy on PHI in ehealthcare systems," *Proc. Advances in Health Informatics Conference (AHIC 2010)*, Apr. 2010.

[18] J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic-health-record system," *IEEE Trans. Parallel and Distributed Systems*, vol. 21, no. 6, pp. 754–764, 2010.

[19] M. Katzarova and A. Simpson, "Delegation in a distributed healthcare context: A survey of current approaches," in *ISC 2006, Palermo, Italy*, pp. 517–529, 2006.

[20] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in *Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09)*, pp. 103–114, ACM, 2009.

[21] C.-K. Chu, S. S. M. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 99, no. PrePrints, 2013.

[22] M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in *ACM Conference on Computer and Communications Security*, pp. 121–130, 2009.

[23] S. S. M. Chow, *New Privacy-Preserving Architectures for Identity-/Attribute-based Encryption*. PhD thesis, New York University, 2010.

[24] S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE - Simple Privacy-Preserving Identity-Management for Cloud Environment," in *ACNS*, pp. 526–543, 2012.

[25] S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng, "Dynamic Secure Cloud Storage with Provenance," in *Cryptography and Security*, pp. 442–464, 2012.

[26] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612–613, 1979.

[27] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attributed-based encryption for fine-grained access control of encrypted data," *ACM Conference on Computer and Communications Security (CCS)*, pp. 89–98, 2006.

[28] A. Boldyreva, "Efficient threshold signatures, multisignatures and blind signatures based on the Gap-Diffie-Hellman-group signature scheme," in *Public Key Cryptography*, pp. 31–46, 2003.

[29] S. S. M. Chow, "Removing Escrow from Identity-Based Encryption," in *Public Key Cryptography*, pp. 256–276, 2009.

[30] S. S. M. Chow, J. K. Liu, and J. Zhou, "Identity-Based Online/Offline Key Encapsulation and Encryption," in *ASIACCS*, pp. 52–60, 2011.

[31] T. H. Yuen, C. Zhang, S. S. M. Chow, and J. K. Liu, "Towards Anonymous Ciphertext Indistinguishability with Identity Leakage," in *Provable Security*, pp. 139–153, 2013.