Secure Electronic Health Record System Based on Online/Offline KP-ABE in the Cloud

Kun Liu

School of Mathematics and Information Science, Guangzhou University, 230 Guangzhou University City Outer Ring Road, Guangzhou, P.R. China

Keywords: Electronic Health Record, Online/Offline Key-policy Attribute-based Encryption, Cloud Computing.

Abstract: Online electronic health record(EHR) enables patients to centrally manage the own medical records, which greatly facilitates the storage, access and sharing of personal health data. With the emergence of cloud computing, it has succeeded in attracting attention and transferring their EHR applications to an efficient system for storing and accessing data. However, due to lose physically control of personal data in a cloud computing circumstance, it brings about a serious privacy problem for the data owner. Therefore, cryptography schemes offering a more suitable solution for enforcing access policies based on user attributes are needed. We have proposed a framework with fine-grained access control mechanism that protects electronic health data in varieties of devices, including smart mobile device. We make EHR security through designing online/offline key policy attribute-based encryption scheme which is an extension of identify-based encryption (IBE). This scheme can provide fine-grain access policy and efficiency for users' data. Especially, it's greatly reducing complexity and computational of encryption and key generation.

1 INTRODUCTION

Alone with progressively advanced of technology development, it brings more convenient to the whole society. At present, people is available to use majority kinds of portable equipment, which equip full accessing control performance, to administer their body's medical and health information. Everyone is available to observe themselves health records to great understand body situations bypassing their common action and exercise training, conveniently catching whether health maintains good conditions or not at any time. Technically, a personal health device has to necessitate the interaction of health records, as the data results are cared about by user with analyzing in the storage center. Consequently, those services permit a person to generate, manage and manipulate health records through the Internet anywhere and at any time. The feedback of analyzing reports plays the friend and benefit role in the process between users and data analysis center. At the same time, users can have overall control over their health records and be able to effectively compare their health data with other health care providers, not just their families and friends. In this way, physicians can take advantage of different physiological parameters to make diagnosis more accurate and efficient, while reducing the patient's medical expenses.

However, the EHR system must have charge of the burden of storage, computing and communication pressures from a growing number of user. Therefore, its services must have powerful computing ability. Nowadays, a new computing paradigm called the cloud has possession of the dynamic extension ability, which flexibly connects to the network by obtaining computing resources and services. For the reason of its virtually unlimited and flexible storage and computing ability (Fan et al., 2015), the cloud computing has attracted much concern to research and apply in academic and industry. It is obvious that the cloud holds gigantic saved space and application ability to turn into preferred data processing rather than running in the specialized data center. Thus, the EHR system is imperative to outsource its data and computations to cloud for storage and calculation. In addition, it also can heavily reduce the consumption of EHR operation. Likewise, an increasing number of patients and physician have transformed their habits to visit EHR system in smart mobile equipment, which is easier access and operation than traditional methods. We can take some applications of smart devices as an example, such as MediTouch EHR Software, Office

Liu, K.
Secure Electronic Health Record System Based on Online/Offline KP-ABE in the Cloud.
DOI: 10.5220/0006350101100116
In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*, pages 110-116
ISBN: 978-989-758-245-5

Practicum from mobile application providers.

Although we enjoy utilizing the convenience and intellect from EHR service in the cloud, our privacy is undergoing unprecedented menace in the process of information processing and communication. The EHR system and storage service have possessed a lot of sensitive information about user privacy, which is greatly anxious in data providers. That is to say, the user's sensitive data is in potentially dangerous circumstance which they don't know whether EHR would be leakage in the EMR system. These are tremendous security concerns that users have no way to trust its service and fully rely on the EMR system. That is to say, when the data is reserved in the cloud server, the most major anxiety of users is about the secret key management and authority issues because they have no idea who can be authorized to visit the data in the EHR system. At the same time, ever since the patients uploaded and outsourced their record into the cloud server, they have lost actual control about their medical and health data in physical. Just because of this, those important information could have no longer to be safely guaranteed full privacy assure. On the one hand, due to misbehave from the cloud inner servers, the patients' private data may leak to the outside. Such error behavior may also lead to reveal the worthy information in personal data, including telephone numbers and medical records. For instance, The malicious adversary can utilize those personal information to recommend special medicine for seeking illegitimate interests. On the other hand, cloud servers are more vulnerable suffering malicious attacks from outside, which is decided by its unique features that cloud servers calculus and store data on the open platform.

To address the potential risks of privacy exposures, EHR system needs to construct a kind of access control mechanism that permit patients to administer the entire control to do the selectively share their own EHR information rather than making the cloud encrypted the patients' data. In this respect, the access control of EHR should be provided in traditional way, apart from secured by the server (Benaloh et al., 2009). Generally, any decryption key should be generated by corresponding patient, which is available to be distributed for authorized users. Therefore, data owner should be granted permission to visit and revoke their record which possesses crucial effect to guarding data owner's privilege to their sensitive information while preserving their privacy (Mandl et al., 2001). To resolve the fine-grained access control and sharing issues, Sahai and Waters put forward a notion of attribute-based encryption (ABE), derived from a type of application Fuzzy-IBE scheme (Sahai and Waters, 2005). ABE targets to offer fine-grained and extensible access control to encrypt plaintext, which is according to a kind of one to multiple public key encryption schema attracting lots of attention to research. However, it is a significant drawback that the computational complexity of access control rule and account of attributes directly make a difference of efficiency of the encryption and the key generation phases. In protecting privacy of EHR system, these issues bring obstacles to preserving the privacy of EMR system, which leads to increase consumption in plaintext encryption phase and user key generation phase (Hohenberger and Waters, 2014).

This paper aims to eliminate this security and privacy problem through constructing online/offline key-policy attribute-based encryption scheme (OO-KP-ABE). By comparing with the previous KP-ABE, we split the encryption into different phases, online encryption and offline encryption, which enable to decrease the complexity and computation of encryption and key generation for data owner.

The remainder of this paper is arranged as follows. We recall the related work in section 2, including the development of EHR and OO-KP-ABE scheme. Furthermore, section 3 illustrates some preliminary nation about bilinear group, access control structure and online/offline key-policy attribute. In section 4, we present our main framework of EHR cloud system including security requirement and analysis. Finally, this paper is summarized in section 5.

2 RELATED WORK

In order to improve patients care, safety and costs saving, health record system is undertaking to achieve modernization for greater efficiency with advance side by side (Buck, 2007; Kim et al., 2008; Lohr, 2009; Tripathi et al., 2009; Health et al., 2008). Commonly, an EHR system contains a digital record about patients' fundamental medical and health data that is available to provide for authorized clinicians and staff to create, concentrate, manage and view. In general, Hospitals or research institutions usually have possession and store only one aspect of the patient's record. Patients and doctors are able to exert repeatedly checking and incurring unnecessary costs in EHR system.

We have implemented IBE scheme to encrypt data of a single user in EHR system, after which data owner must know the user's identity until send the encrypted data to the user. Previously, We constructed an IBE scheme for individual users to encrypt data. In other words, before data owner dispatches his en-

crypted personal data to user, he must know and confirm the identity (Boneh and Franklin, 2001). Actually, this IBE operation would not take effect when the sending part didn't verify the definite the user's identity. To solve the problem above, ABE is available to adapt to the one to many encryption scenarios. Especially, there has a tremendous tendency to use ABE for personal health record (PHR). Consequently, PHR system must satisfy fine-grained access control strategy and make efficient revocation possible, while KP-ABE can be achieve those requirements (Yan et al., 2016; Liu et al., 2016; Liu et al., 2016; Li et al., 2015). But the ciphertext length linearly increase the account of users, which also brings a heavy burden on the computational complexity and computation of the server.

The conception of attribute-based encryption was derived from fuzzy IBE by Sahai and Waters in (Sahai and Waters, 2005), which was coped with by Goyal et al at first. Then, ABE are available to allow data owner to transmit ciphertext to users based on certainly specified access policies. Simultaneously, there are categorized into two kinds of ABE scheme, key-policy attribute-based encryption (KP-ABE) (Goyal et al., 2006) and ciphertext-policy attribute-based encryption (CP-ABE) (Bethencourt et al., 2007). When correspondent ciphertext is satisfied the access control policy connected with a specific set of attribute, the private key can be generated accordingly. Namely, the secret key is connected to access control structure. The user can perform the decryption algorithm to obtain the plaintext through a corresponding private key whose attribute set is exclusively authorized a set of the private key?s access control structure. KP-ABE is a cryptography system based on bilinear map and Linear Secret Sharing Schemes (*LSSS*). On the other hand, the ciphertext relates the access control policy (Bethencourt et al., 2007) in CP-ABE.

Although ABE has possession of powerful function, there is a concern about efficiency drawback to confine it practical application. In most ABE system, the encryption and decryption costs grow with the account of attributes and the complexity of access structure. In particular, mobile devices must run encryption and decryption algorithms to protect their real-time data. The required time to run and cache may give rise to sustain problems for limiting battery power supply. In 2014, for sake of alleviating the custom of mobile instruments, Hohenberger et al. (Rouselakis and Waters, 2013) has proposed methods for online/offline encryption in ABE setting.

3 PRELIMINARIES

3.1 Bilinear Mapping

Definition 1 (Bilinear mapping (Boneh et al., 2004)) Let P_0, P_1 be two multiplicative cyclic groups of prime order p. Let g be the generator of P_0. Define a bilinear map $e : P_0 \times P_0 \to P_1$. It has the following properties:

- Bilinear: $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ for all $a, b \in \mathbb{Z}_p$ and $g_1, g_2 \in P_0$.
- Non-degenerate: $e(g, g) \neq 1$.

If the group operation in P_0 and the bilinear map e are both computable, the multiplicative cyclic group P_0 is a bilinear group. It is a remarkable fact that the map e is symmetric since $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab} = e(g_1^b, g_2^a)$.

3.2 Access Structure

Definition 2 (Access Structure (Beimel, 1996)) Let $U = \{U_1, U_2, \cdots, U_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\{U_1, U_2, \cdots, U_n\}}$ is monotone if $\forall B, C$, if $B \in \mathbb{A}$ and $B \subseteq C$ denote $C \in \mathbb{A}$. An access structure is a monotone collection $\mathbb{A}$ of non-empty subsets of $\{U_1, U_2, \cdots, U_n\}$ (that is $\mathbb{A} \subseteq 2^{\{U_1, U_2, \cdots, U_n\}} \setminus \phi$). The sets in $\mathbb{A}$ are called the authorized sets, and the sets not in $\mathbb{A}$ are called the unauthorized sets.
The access structure $\mathbb{A}$ plays a vital role in authorizing sets of attribute in our context. We constrict it as monotone access structures, formally.

3.3 Online/Offline KP-ABE Scheme

We illustrate the KP-ABE schema with online/offline encryption (Hohenberger and Waters, 2014) by the following five polynomial algorithms.

- Setup(λ, U): A security parameter λ and a universe U of attributes take account into the setup algorithm. We choose a bilinear group P of prime order $p \in \Theta(2^\lambda)$.It needs stochastically choosing generators $g, h, u, w \in P$ and picking a random exponent $\alpha \in Z_p$. Then, it sets up the keys as:

  $$PK = (P, p, g, h, u, w, e(g, g)^\alpha), MK = (PK, \alpha).$$

  Firstly, we suppose that the university of attributes can be encoded as elements in Z_p.
- Extract($MK, (M, \rho)$): The extract algorithm takes the master secret key MK and a Linear Serect Sharing Scheme access structure (M, ρ) from a user as an input. The trusted key generation center provides a corresponding private key $SK_{(M,\rho)}$ to give the user by working extract algorithm.

- Offline Encryption(PK): The offline encryption algorithm just needs the encrypter to take the public parameters PK as input. The encrypter will engender and store an intermediate ciphertext pool IT.
- Online Encryption(PK, IT, S): During the online encryption phase, the encrypter is available to output a ciphertext CT and produce a session key *key* which is kept to itself before inputting the public parameters PK , an intermediate ciphertext pool IT , and a set of attributes S.
- Decryption($PK, CT, SK_{(M,\rho)}$): A user utilizes the public parameters PK , its private key $SK_{(M,\rho)}$ for access structure (M,ρ) and a ciphertext CT associated with an attribute set S as input. It is decapsulated CT to recover a session key *key* or inputs the distinguished symbol $\perp$.

The correctness condition as well as the model for defining the adaptive security for online/offline KP-ABE is provided in (Hohenberger and Waters, 2014).

3.4 Security Model of OO-AB-Key Encapsulation Mechanism

Based on hading a symmetric session key, the key encapsulation mechanism (KEM), which is able to use in the online/offline KP-ABE, can be utilized for encrypting data with arbitrary length at the symmetrical encryption scheme. The following selective-set model for online/offline KP-ABE scheme was given by Hohenberger et al. (Hohenberger and Waters, 2014), which illustrates the game as follows. Initiatorily, we define that $\Pi = (Setup, Extract, Off.Enc, On.Enc, Decryption)$ is an $AB-KEM$ (Rouselakis and Waters, 2013) for access structure space $\mathscr{P}$, and consider the below game for parameter λ, attribute universe U and an adversary $\mathscr{A}$.

- Setup: The public parameter PK is generated in the process of a challenger running the setup algorithm. Then he sends it to the adversary.
- Step 1: It is necessary to initialize an empty table T, an empty set D and an integer counter $j = 0$, which is performed by the challenger. Adaptively, the adversary is able to arbitrarily perform the following inquiry:
  1. Create (I_{key}): The challenger, who require to run the key generation algorithm on I_{key} after setting $j := j+1$, acquires the secret key SK and stores the entry (j, I_{key}, SK) in the table T. It is worthy noted that Create($\cdot$) operation could be inquired again and again with the same input.
  2. Corrupt (i): If there consists of an i^{th} entry in table T, after that the challenger is able to acquire the entry (j, I_{key}, SK) and sets $D := D$ and I_{key}. It is the next to return the private key of adversary SK. Then, it would return $\perp$, if no such entry exists.
  3. Decrypt (i, CT): When table T has an i^{th} entry in existence, the challenger could obtain the entry the entry (j, I_{key}, SK). Accordingly, he can return to the adversary the output of the decryption algorithm on input (SK, CT). Then, it would return $\perp$, if no such entry exists.
  4. Challenge: In order to make all $I_{enc} \in D$, $f(I_{key}, I^*_{enc}) \neq 1$, the provides a challenge value I^*_{enc} firstly. The challenger acquires (I_{key}, I^*_{enc}) bypass running the algorithm Online.Encrypt $(PK, Offline.Encrypt(PK), I^*_{key})$. After that, it chooses a bit b at random. If $b = 1$, it selects a random session key R in the session key space and returns (R, CT^*). If $b = 0$, it returns (key^*, CT^*) to the adversary.
- Step 2: Step 1 is associated with the constrictions that the adversary aren't able to trivially acquire a private key for the challenge ciphertext. Namely, it satisfies $f(I_{key}, I^*_{enc}) = 1$ being added to D. And it cannot also send a decryption query about the challenge ciphertext CT^*.
- Guess: While the adversary outputs a guess b' of b, the output of the experiment is 1 if and only if $b = b'$.

Definition 3 (Online/Offline AB-KEM Security) For all probabilistic polynomial-time adversaries A, there is attribute universe U if under chosen-ciphertext attack (CPA) for the semantic security, there exists a negligible function *negl* such that:

$$Pr[OOAB-KEM_{A,\Pi}(\lambda, U) = 1] \leqslant \frac{1}{2} + negl(\lambda)$$

CPA Security. If we take away the Decrypt oracle in both step 1 and 2, we view that a system satisfies *CPA*-secure (or secure against *chosen-plaintext attacks*).

4 THE FRAMEWORK OF EHR COULD SYSTEM

4.1 EHR System Illustration

The interaction between participants and EHR cloud system is precisely illustrated through the figure 1. It is included the health data producer, the data user and the trusted key generation *key* center and the cloud

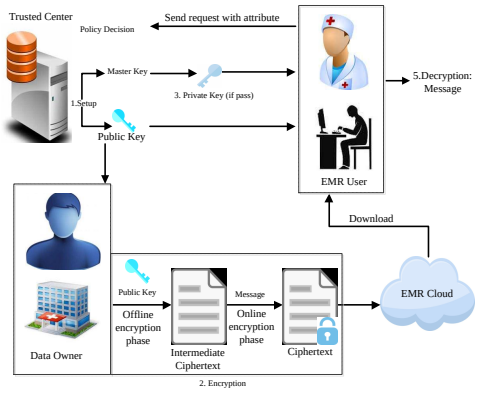

Figure 1: System CP-ABE and workflow.

service. The framework illustrates how the data owners store their personal data.

- EHR system setup: EHR system running the setup algorithm requires that the trusted private key generation center chooses a security parameter λ to product public key PK and master secret key MK by a random oracle model. Then, the trusted center is able to transmit the public key PK to the data owner. Consequently, the trusted center holds the master key MK to itself.
- Encryption: The traditional encryption phase is divided into two sessions. On the offline encryption phase, the data owner runs the offline encryption algorithm to generate intermediate ciphertext IT. Especially, IT must be store securely by the user in the local side. On the online encryption phase, the data owner has to run the online encryption algorithm through taking as the message M, the public parameter PK, the assess control structure (M, ρ) and the set of attribute U into input. After that, the user is able to outsource their ciphertext into the cloud.
- The request: The authorized request is sent to the trusted center by the data user, who takes as his attributes into input. If the request would be verified into the truth, the trusted center could give a ?pass? answer to the data user. If answers were negative, the trusted center would refuse this request from the data user.
- Key Extract: If the attribute of user satisfies the access control assess control structure (M, ρ), the trusted center would be obtained a "pass" answers. As a consequence, the trusted center will run Extract algorithm of OO-KP-ABE schema to gain the private SK. Then, it sends SK to the user to decrypt the ciphertext CT.
- Decryption phase: When the data user obtains the positive answer, the trusted center immediately transforms the private key to him. With taking as privacy key and the ciphertext CT from the cloud into input, the data user is available to compute the message through running the decryption algorithm of online/offline KP-ABE.

The data user sends an authorized request which the mobile device data producer and medical institution, for the beginning, the trusted center utilize the Extract algorithm to generate a privacy key SK, which takes parameter key PK and master key MK as input.

4.2 Security Requirements

In the following, We introduce four characteristics of the main security requirements in the EHR cloud system.

- Data Confidentiality: When electronic health record of data owner stores in the cloud, it couldn't be arbitrarily consulted if someone doesn't own private key and possess patients' authorization. Thus, the EHR has to be encrypted before uploading to the cloud server. Owing to encrypt data though patients' attribute, only someone obtains the private key who have been authorized.
- Authenticity: Data owner reserves their information in the EHR system, which implements varieties of operation in the third cloud platform. Patients don't permit their valuable and sensitive record to be compromised and distorted by malicious attackers. Hence, The cloud server has to guarantee the authenticity of data for data provider. Similarity, we can ensure the authenticity of data for verifying the information and improving access control in especial scheme, such as (Meng et al., 2016; Yan et al., 2016), respectively. For another approach, the user accesses data used to study or treat other patients. If the patient's EHR is not reliable, this will be a big hidden dangers.
- Privacy protection for patients: The number of access control population should be confined by the purpose of the visitor. According to the user's attribute differences, he has different access permissions. For instance, doctor, nurse and researcher, they have possession of authority to access data based on their usage purpose in the EHR system.
- Revocation: If a user want to revoke his attribute, after that immediately the user will not be available to access EHR using that attribute, known as attribute revocation. There is another situation users can no longer use corresponding private key

when the data owner makes a time limit for his one of access control.

5 CONCLUSIONS

In this paper, we construct a scheme for uncertain users and a fine-grained access control of EHR system by attribute policy in the cloud. Traditional public key encryption system is unsuitable to encrypt multiple to one or multiple to multiple situation. Previously, access control is aimed to a single known user who only delegates a known identity. Nowadays, people are available to record their health data in EHR system by moving electronic devices. This function isn't limited by time and place, which only needs device having sufficient power and communication Internet. Consequently, a semi-trusted third cloud platform provides these service in our schema. Moreover, the patient must have complete control power over their own data, such as specifying a particular person viewing the data set, and those who do not match the attribute policy do not have access to the data set.

As above, the OO-KP-ABE scheme is that the promising technology should speed up the utilization of EHR cloud platform in other related works in an electronic health field.

ACKNOWLEDGEMENTS

This work was supported by National Natural Science Foundation of China (No. 61472091), Natural Science Foundation of Guangdong Province for Distinguished Young Scholars (2014A030306020) and Science and Technology Planning Project of Guangdong Province, China (2015B010129015).

REFERENCES

Beimel, A. a. (1996). *Secure schemes for secret sharing and key distribution*. Technion-Israel Institute of technology, Faculty of computer science.

Benaloh, J., Chase, M., Horvitz, E., and Lauter, K. (2009). Patient controlled encryption: ensuring privacy of electronic medical records. In *Proceedings of the 2009 ACM workshop on Cloud computing security*, pages 103–114. ACM.

Bethencourt, J., Sahai, A., and Waters, B. (2007). Ciphertext-policy attribute-based encryption. In *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pages 321–334. IEEE.

Boneh, D., Di Crescenzo, G., Ostrovsky, R., and Persiano, G. (2004). Public key encryption with keyword search. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 506–522. Springer.

Boneh, D. and Franklin, M. (2001). Identity-based encryption from the weil pairing. In *Annual International Cryptology Conference*, pages 213–229. Springer.

Buck, C. F. (2007). Designing a consumer-centered personal health record. Technical report, Technical report, California Health Foundation.

Fan, K., Huang, N., Wang, Y., Li, H., and Yang, Y. (2015). Secure and efficient personal health record scheme using attribute-based encryption. In *Cyber Security and Cloud Computing (CSCloud), 2015 IEEE 2nd International Conference on*, pages 111–114. IEEE.

Goyal, V., Pandey, O., Sahai, A., and Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 89–98. Acm.

Health, U. D., Services, H., et al. (2008). The nationwide privacy and security framework for electronic exchange of individually identifiable health information. *Office of the National Coordinator for Health Information Technology*.

Hohenberger, S. and Waters, B. (2014). Online/offline attribute-based encryption. In *International Workshop on Public Key Cryptography*, pages 293–310. Springer.

Kim, G. R., Lehmann, C. U., on Clinical Information Technology, C., et al. (2008). Pediatric aspects of inpatient health information technology systems. *Pediatrics*, 122(6):e1287–e1296.

Li, J., Li, J., Chen, X., Jia, C., and Lou, W. (2015). Identity-based encryption with outsourced revocation in cloud computing. *Ieee Transactions on computers*, 64(2):425–437.

Liu, J. K., Au, M. H., Huang, X., Lu, R., and Li, J. (2016). Fine-grained two-factor access control for web-based cloud computing services. *IEEE Transactions on Information Forensics and Security*, 11(3):484–497.

Lohr, S. (2009). Ge and intel join forces on health technologies. *New York Times*, 3.

Mandl, K. D., Markwell, D., MacDonald, R., Szolovits, P., and Kohane, I. S. (2001). Public standards and patients' control: how to keep electronic medical records accessible but privatemedical information: access and privacydoctrines for developing electronic medical recordsdesirable characteristics of electronic medical recordschallenges and limitations for electronic medical recordsconclusionscommentary: Open approaches to electronic patient recordscommentary: A patient's viewpoint. *Bmj*, 322(7281):283–287.

Meng, D., Wang, W., Luo, E., and Wang, G. (2016). Attribute-based traceable anonymous proxy signature strategy for mobile healthcare. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage: 9th International Conference, SpaCCS 2016, Zhangjiajie, China, November 16-18, 2016, Proceedings 9*, pages 178–189. Springer.

Rouselakis, Y. and Waters, B. (2013). Practical constructions and new proof methods for large universe

attribute-based encryption. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 463–474. ACM.

Sahai, A. and Waters, B. (2005). Fuzzy identity-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 457–473. Springer.

Tripathi, M., Delano, D., Lund, B., and Rudolph, L. (2009). Engaging patients for health information exchange. *Health Affairs*, 28(2):435–443.

Yan, H., Li, J., Li, X., Zhao, G., Lee, S.-Y., and Shen, J. (2016). Secure access control of e-health system with attribute-based encryption. *Intelligent Automation & Soft Computing*, 22(3):345–352.