Hong et al. SpringerPlus (2016) 5:1320
DOI 10.1186/s40064-016-3002-y

SpringerPlus

SHORT REPORT Open Access

A practical application of CP-ABE for mobile PHR system: a study on the user accountability

Hanshu Hong[1], Di Chen[2] and Zhixin Sun[1*]

*Correspondence:
sunzx@njupt.edu.cn
[1] Key Lab of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Nanjing, China
Full list of author information is available at the end of the article

Abstract

Background: Attribute based encryption has been widely applied for secure data protection in PHR systems. However, since different users may share the same attributes in the system, a user may leaks his private key for illegal data sharing without being detected. This will add more threat to the private data stored in PHR system.

Finding: To help users achieve higher efficiency and more secure data sharing in mobile PHR system, based on previous works, we study the traitor tracing mechanism in attribute based cryptosystem and propose a high efficient attribute based encryption with user accountability in mobile PHR system. If a malicious PHR user exposes his private key for illegal data sharing, his identity can be accurately pinpointed by the system manager. During the whole process of data sharing, no bilinear pairing operations are needed, hence this will the mobile terminal devices from heavy computation burden.

Conclusion: As a further study, in this short report, we show that using a novel attribute based encryption with user accountability can help users achieve better efficiency and more secure data sharing in mobile PHR system.

Keywords: CP-ABE, Mobile PHR system, User accountability

Background

Personal health record (PHR) (Zuckerman and Kim 2009; Koufi et al. 2014) contains massive private data in terms of the user's health conditions, disease history, medication and other personal information. Due to the capability of improving the efficiency of healthcare, PHR has gained increasingly popularity nowadays and has been widely applied in the medical area such as diseases rehabilitation, disease prevention (McInnes and Shimada 2013), medical treatment, etc. Considering the private nature of PHR (Price et al. 2015), special encryption techniques should be implemented for protection in the PHR system (Liu et al. 2015; Sangeetha et al. 2014).

Ciphertext policy attribute based encryption (CP-ABE) (Goyal et al. 2006; Waters 2011) was proposed by Waters in 2006 and has been considered suitable for access control for PHR system, since it reduces the encryption cost for PHR data owner and can also provide flexible self-centric data access management (Hong and Sun 2016; Fuji and Abbott 2012) at the same time. Unlike identity based cryptosystem (Li and Khan 2012),

in CP-ABE, user's access privileges are defined by a set of attributes. A user can read the ciphertext on condition that the attributes he owns match with the policy (Price et al. 2015; Hong et al. 2016). An illustration of ciphertext access policy is shown in Fig. 1, the PHR data owner may not know the exact identity of users who have the privileges to access the data, but can describe those using attributes such as "family members", "Nurse". For instance, if a user owns the attributes of {Hospital 1, Physician}, then he can get access to the PHR data since the attributes he possesses satisfy with the access structure illustrated in Fig. 1.

Many schemes have applied attribute based encryption to design medical care systems such as PHR (Qian et al. 2015; Liu et al. 2013; Li et al. 2015; Xhafa et al. 2015) and BAN (Tan et al. 2011; Tian et al. 2014), but the efficiency is still unsatisfactory. One important factor is that a PHR user has to run many times of bilinear pairing operations when decrypting a ciphertext. When PHR users get access to the encrypted data using mobile devices with restricted computing resources such as cellphones, body area sensors, smart watches, the heavy decryption computation will add difficulty in the process of mobile PHR data sharing.

Key abuse is another obstacle to apply attribute based encryption to PHR system. ABE is an advanced type of broadcast encryption, users owing the same attributes share the same private key. However at the same time, a malicious user may expose his private key deliberately without being detected. Thus, a mechanism which provides user accountability and traitor tracing should also be introduced.

Based on the previous works (Liu et al. 2013; Tan et al. 2011; Li et al. 2015; Tian et al. 2014; Xhafa et al. 2015; Li and Khan 2012; Hong and Sun 2016), to better solve the problems described above and help users achieve secure data sharing in mobile PHR system, the following constructions are established:

Firstly, we propose a user accountable ciphertext policy attribute based encryption without pairings (UA-CPABE-WP) for mobile PHR system. In our UA-CPABE-WP,

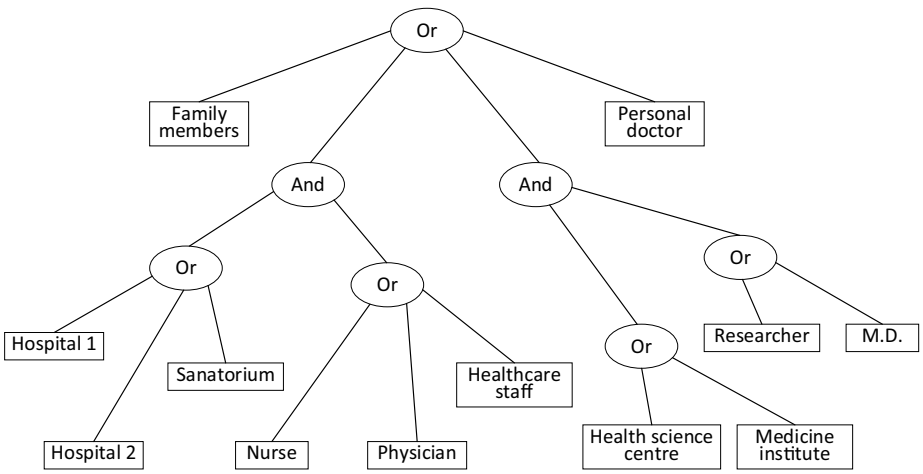

Fig. 1 An CP-ABE access control structure for PHR data

users can recover the plaintext on condition that the possessing attributes satisfy with the access policy.

Secondly, the mechanism of user accountability is introduced. If a malicious PHR user exposes his private key for illegal data sharing, his identity can be accurately pinpointed by the system manager.

Thirdly, no bilinear pairing are needed during data sharing, hence relieving the mobile terminal devices from large calculation.

Our studies

Implementation of the proposed UA-CPABE-WP

The implementation example of our scheme can be illustrated in Fig. 2. It consists of 6 entitles: AA (Attribute authority), PHR data center, data owner and receiver. Base station and data center are hardware architectures which are responsible for mobile communications and file storage. AA generates attribute private key for each user in the system. PHR data center stores massive PHR data and responds to user's data access request. Data owner and receiver are the two sides of communication, data owner encrypts the file with an access structure, while a receiver can decrypt the ciphertext using mobile devices if the attributes he owns match with the access structure. Tracer can pinpoint the exact identity of the traitor who leaks his private key deliberately.

Constructions

Before introducing the formulized definitions of our scheme, some notations are defined in Table 1 for the convenience and clearness of description.

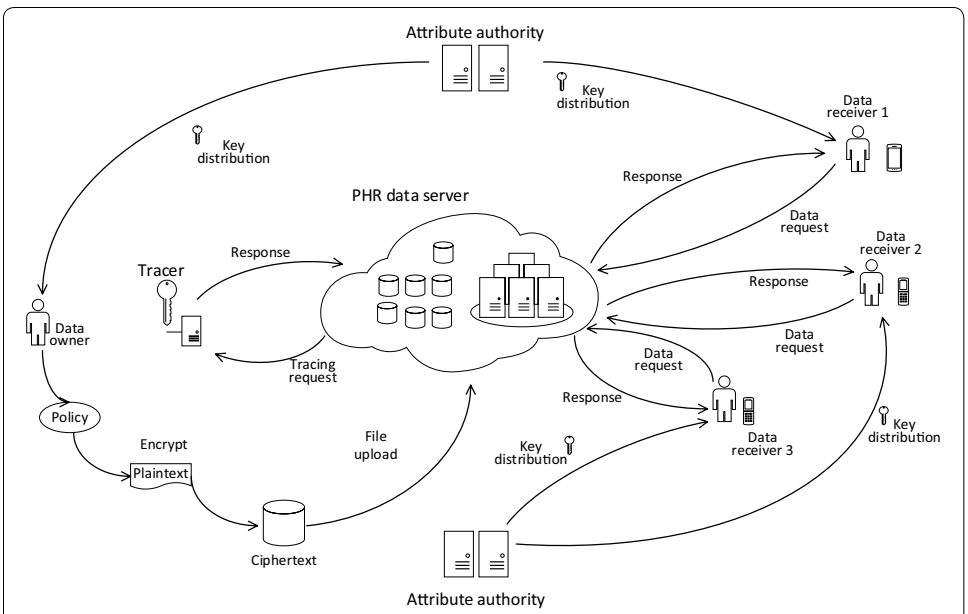

Fig. 2 The implementation of our UA-CPABE-WP

Table 1 Notations and their corresponding meanings

Notation	Meaning	Notation	Meaning
AA	Attribute authority	*PK*	Public parameters
MK	System master key	A_i	A single attribute *i*
MK_{id}	User's private key	*id*	User's identity
CT	Ciphertext	*M*	Plaintext

Our UA-CPABE-WP includes the following algorithms:

Setup: Let Let G to be a cyclic addition group with generator q and prime order p. Defines a global attribute set $\{A_i\}$ and picks $t_i \in Z_q^*$ for each attribute in $\{A_i\}$. Let $T_i = t_i p$. Picks secret numbers $h, y \in Z_q^*$ and calculates $Y = yp$, $H = hp$. Define a hash function $H_1 : \{0,1\}^* \to \{0,1\}^m$, m is the size of plaintext.

The system public parameters are $\{G, q, p, A_i, T_i, Y, H_1, H\}$ and the system master keys are $\{t_i, y, h\}$.

Private key generation: AA assigns a global unique identifier for each user in the PHR system. For a PHR user (without loss of generality, denote his identity by *id*) possessing attribute set S, AA generates his private key SK_{id} as follows:

$$SK_{id} : \left\{ K = \left(id \cdot y + r\right) h^{-1}, \forall A_i \in S, D_i = t_i - r \right\} \tag{1}$$

Encrypt: When a data owner wants to share his private PHR data with some people processing certain attributes, he works as described below:

Picks a polynomial q_x for each node x for access control structure. Denote the degree of q_x to be one less than the threshold value node. For the root node data owner sets $q_{root}(0) = s$. For any other node, let $q_x(0) = q_{parent(x)}(index(x))$. The ciphertext is constructed as:

$$C_0 = H_1(sY)M, \quad C_1 = sH$$

$$C_{2,i} = q_i(0)p, \quad C_{3,i} = q_i(0)T_i \tag{2}$$

Decrypt: Upon receiving CT, data receiver calculates:

$$M = C_0 \oplus H_1\left(id^{-1}\left(K \cdot C_1 + \sum_{i \in \gamma} \left(D_i \cdot C_{2,i} - C_{3,i} \right) \right) \right) \tag{3}$$

Correctness proof:

If x is a leaf node,

$$\begin{aligned} \sum_{i \in \gamma} \left(D_i \cdot C_{2,i} - C_{3,i} \right) &= \sum_{i \in \gamma} (t_i - r) q_i(0) p - q_i(0) T_i \\ &= -r q_i(0) p \end{aligned} \tag{4}$$

If x is a non-leaf node,

Let $i = index(z), S'_x = \left\{ index(z) : z \in S_x \right\}$

$$
\begin{aligned}
F_x &= \sum_{z \in S_x} F_z^{\Delta_{i,S_{x'}}(0)} \\
&= \sum_{z \in S_x} rp \cdot q_z(0)^{\Delta_{i,S_{x'}}(0)} \\
&= \sum_{z \in S_x} rp \cdot q_{parent}(z)^{(index(z))^{\Delta_{i,S_{x'}}(0)}} \\
&= \sum_{z \in S_x} rp \cdot q_z(x)^{\Delta_{i,S_{x'}}(0)} \\
&= -q_x(0) \cdot rp
\end{aligned} \tag{5}
$$

Then, the algorithm calculates the $F_{root} = -q_{root}(0) \cdot rp = -rsp$ by recursive function and computes:

$$
\begin{aligned}
M &= C_0 H_1 \left(id^{-1} \left(K \cdot C_1 + \sum_{i \in \gamma} \left(D_i \cdot C_{2,i} - C_{3,i} \right) \right) \right) \\
&= C_0 H_1 \Big(id^{-1} \Big(\big(id \cdot y + r \big) h^{-1} \cdot sH - rsp \Big) \Big) \\
&= C_0 H_1 \Big(id^{-1} \big(\big(id \cdot y + r \big) sP - rsp \big) \Big) \\
&= H_1(sY) M H_1 \big(syp \big) \\
&= M
\end{aligned} \tag{6}
$$

Results and discussion

Security proof

Theorem *UA-CPABE-WP is secure under chosen message attack if CDH assumption holds.*

Proof If there exists an *Adversary* can break our UA-CPABE-WP with an advantage (t, ε), then there exists a *Simulator* breaking the CDH assumption with an advantage of $\left(t', \varepsilon'\right)$ which satisfies:

$$
\begin{aligned}
t' &\leq t + \left(nq_p + 4n + 9 \right) \cdot t_{sm} + (nq_k + 2n + 2) \cdot t_a \\
\varepsilon' &\geq \frac{\varepsilon}{e(q_k + 1)} \cdot \left(1 - \frac{1}{2^l} \right)
\end{aligned} \tag{7}
$$

In lemma (7), q_p is the amount of public key queries in the challenge game.

The detail proof follows from that in (Liu et al. 2013).

PHR user accountability

When a malicious user (denote *mid* as his unique identity and SK_{mid} as the private key he owns) leaks his private key deliberately in the PHR system for illegal data sharing, then his identity can be exactly pinpointed by tracer. Two main methods can be adopted for traitor tracing as follows:

a. Since user'ds private key is unique, if the amount of users is not huge, tracer can build a list recoding each private key with its corresponding user's identity as Table 2 shows. When private key exposure happens, tracer searches the identifier which corresponds to the leaked private key in the list and the traitor is able to be exactly traced.
b. Upon receiving a legal private key $SK_{mid} = \{K = (mid \cdot y + r)h^{-1}, \forall A_i \in S, D_i = t_i - r\}$ from PHR system, tracer firstly recovers the attribute set belonging to the malicious user from D_i and calculates r as follows:

$$r = D_i - t_i \tag{8}$$

Then, the identity can be pinpointed by:

$$mid = (K \cdot h - r) \cdot y^{-1} \tag{9}$$

Efficiency evaluation

In this section, we will compare the efficiency of our scheme with other schemes which have also applied attribute based encryption to medical systems. In this report, the *Encrypt* algorithm will take $(2n + 2)$ times of multiplication operation, while the *Decrypt* algorithm will take $(n + 2)$ times of multiplication operation and $(n + 1)$ times of addition. Denote "Exp", "Pair", "Mul", and "Add" to be exponential operation, pairing operation, multiplication and addition respectively. The detailed comparison results in terms of computation costs are shown in Table 3.

Since the computation cost of bilinear pairing is much larger than that of multiplication and addition, it can be seen that the efficiency of our UA-CPABE-WP is higher since no bilinear pairings are needed.

Table 2 List of each private key with its corresponding user's identity

User's identity	Corresponding private key
id_1	SK_{id_1}
id_2	SK_{id_2}
…	…
id_n	SK_{id_n}

Table 3 Efficiency comparison

Scheme	Encrypt cost	Decrypt cost	User accountability
Li et al. (2015)	4n + 2 Exp	4n Pair	Yes
Tian et al. (2014)	(n + 3) Exp + 1 Pair	2n Pair + n Exp	No
Ours	(2n + 2) Mul	(n + 2) Mul + (n + 1)Add	Yes

Conclusion

In this report we provide a high efficient data sharing method using attribute based encryption with user accountability (UA-CPABE-WP). In our scheme, data owner can achieve secure and self-centric access control over the PHR data. Besides, the mechanism of user accountability is introduced. If a malicious PHR user exposes his private key for illegal data sharing, his identity can be pinpointed exactly. The better efficiency and security makes UA-CPABE-WP to be a promising method for data protection in mobile PHR system.

Authors' contributions

All the authors contributed equally to this work. All authors read and approved the final manuscript.

Authors' information

Dr Zhixin Sun is the dean of Internet of Things institute, Nanjing University of Posts and Telecommunications. He has published more than 50 literatures on journals worldwide. His research area includes information security, computer networks, computer science, etc. Dr Hanshu Hong is a PHD candidate in Nanjing University of Posts and Telecommunications. His research area includes information security, cryptology. Dr Di Chen is a PHD candidate in Genetics at the Pennsylvania State University, he works in the Huck Institutes of the Life Sciences. His work engages statistical modeling and bioinformatics tools to explore the regional variation of mutation rate in human genome.

Author details

[1] Key Lab of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. [2] Inter-College Program in Genetics, Pennsylvania State University, University Park, PA, USA.

Acknowledgements

This research is supported by the National Natural Science Foundation of China (60973140, 61170276 and 61373135).The authors thank the sponsors for their support and the reviewers for their helpful comments.

Competing of interest

The authors declare that they have no competing interests.

Received: 14 May 2016 Accepted: 5 August 2016
Published online: 11 August 2016

References

Fuji KT, Abbott AA (2012) Standalone personal health records in the United States: meeting patient desires. Health Technol 2(3):197–205

Goyal V, Pandey O, Sahai A, Waters B (2006) Attribute based encryption for fine-grained access control of encrypted data. In: ACM conference on Computer and Communications Security, 2006, pp 89–98

Hong H, Sun Z (2016) High efficient key-insulated attribute based encryption scheme without bilinear pairing operations. SpringerPlus 5(1):1–12

Hong H, Sun Z, Liu X (2016) A key-insulated CP-ABE with key exposure accountability for secure data sharing in the cloud. KSII Trans Internet Inf Syst 10(5):2394–2406. doi:10.3837/tiis.2016.05.024

Koufi V, Malamateniou F, Vassilacopoulos G (2014) Privacy-preserving access control for PHR-based emergency medical systems, concepts and trends in healthcare information systems, vol 16 of the series annals of information systems, 2014, September, 61–78

Li F, Khan MK (2012) A biometric identity-based signcryption scheme. Future Gener Comput Syst 28(1):306–310

Li J, Xhafa F, Feng J (2015) Privacy-aware attribute-based PHR sharing with user accountability in cloud computing. J Supercomput 71(5):1607–1619

Liu X, Ma J, Xiong J (2013) Personal health records integrity verification using attribute based proxy signature in cloud computing. In: Internet and distributed computing systems vol 8223 of the series lecture notes in computer science, 2013, pp 238–251

Liu X, Liu Q, Peng T (2015) HCBE: Achieving fine-grained access control in cloud-based PHR systems, algorithms and architectures for parallel processing, vol 9530 of the series lecture notes in computer science, 2015, pp 562–576
McInnes DK, Shimada SL (2013) Personal health record use and its association with antiretroviral adherence: survey and medical record data from 1871 US veterans infected with HIV. AIDS Behav 17(9):3091–3100
Price JM, Bellwood P, Kitson N (2015) Conditions potentially sensitive to a Personal Health Record (PHR) intervention, a systematic review. BMC Med Inf Decis Mak. http://link.springer.com/article/10.1186/s12911-015-0159-1
Qian H, Li J, Zhang Y (2015) Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation. Int J Inf Secur 14(6):487–497
Sangeetha D, Vijayakumar V, Thirunavukkarasu V (2014) Enhanced security of PHR system in cloud using prioritized level based encryption, recent trends in computer networks and distributed systems security, vol 420 of the series communications in computer and information science, 2014, pp 57–69
Tan Y-L, Goi B-M, Komiya R (2011) A study of attribute-based encryption for body sensor Networks. In: Informatics engineering and information science, communications in computer and information science, vol 251, pp 238–247
Tian Y, Peng Y, Peng X (2014) An attribute-based encryption scheme with revocation for fine-grained access control in wireless body area networks. Int J Distrib Sensor Netw. http://www.hindawi.com/journals/ijdsn/2014/259798/
Waters B (2011) Ciphertext policy attribute based encryption: an expressive, efficient, and provably secure realization. In: Proceedings of international conference PKC 2011, March, pp 53–70
Xhafa F, Li J, Zhao G (2015) Designing cloud-based electronic health record system with attribute-based encryption. Multimed Tools Appl 74(10):3441–3458
Zuckerman AE, Kim GR (2009) Personal health records. In: Lehmann CU, Kim GR, Johnson KB (eds) Pediatric informatics, part of the series health informatics. Springer, New York, pp 293–301