Secure PHR Access Control Scheme in Cloud Computing

Chia-Hui Liu, Tzer-Long Chen, Han-Yu Lin, Fong-Qi Lin, Chih-Ming Liu, En-Ping Wu, Yu-Fang Chung, and Tzer-Shyong Chen

***Abstract*—With the development of medical technology and informationtechnology, the "personal health records (PHR)" is gradually developed as a up-to-date medical information exchange system. Aproper patient-centered PHR systemis able tooffer correct and complete personal health and medical summary through the Internet under the demands of privacy and security, and integrate personal medicalinformation from different sources. With the appearance of Cloud computing, a secure protection scheme is required to encrypt the medical records of each patient for storing personal health records into Cloud server. Therefore, we proposed in this study a new PHR access control scheme based on Lagrange interpolation polynomial under Cloud computing environments. This proposed scheme provides legitimate authorities to access to PHR, and dynamically supports multi-users in Cloud computing environments with personal privacy.**

***Index Terms*—Personal health records, cloud computing, access control, key management,Lagrange interpolation.**

I. Introduction

Continuing on past developments on Electronic Medical Record Systems, this project is carried out with the purpose of assisting medical professionals in dispensing medical care by prioritizing patients' health maintenance or management. M.Li et al [1] proposed a patient-centered, Personal Health Record (PHR) exchange architecture for patients to maintain and manage these health records, including medical records of professional diagnoses, voluntary health care programs, and other applications and services related to self-health management.PHR architectures are based on fundamental assumptions that:

1) The complete record is held in a central repository.
2) Patients retain authority over complete access to their own records.

Therefore, we propose the PHR to achieve the following:

1) Integration of patient's lifelong health information.
2) Provision of stable and secure data storage space.
3) Patient's right to complete access of his/herPHR.
4) Provision for precision access settings to various parts of the PHR for different users.
5) Provision for a complete, continuous, secure, and private health management mechanism.

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) [2]–[4] outlined legal privacy and security protection for PHR. Healthcare Organizations (HCOs) and e-health services covered by HIPAA face the problem of implementing effective and cost-efficient security and privacy policies, while having to constantly demonstrate compliance with HIPAA regulations. For these reasons, similar security and privacy policies are also applicable to PHR; PHR must adhere to HIPAA regulations for protecting patient's information. Aiming to improve spontaneous healthcare services and increase overall service quality and management efficiency for medical institutions, some healthcare systems are currently cooperating with the telecommunication industry to introduce cloud technology into healthcare application and services that include cloud electronic medical record, cloud nursing information system, Hospital Informatics Suite Cloud (HIS Cloud), and private cloud server plans by medical institutions.

Integration of PHR with cloud service provides the following benefits:

1) *Reduced cost:* Since cloud providers provide the basic infrastructure, platform, software, and storage space, hospitals no longer need to create their own medical data center, cutting back on hardware setup costs, as well as software and hardware upgrade costs.
2) *Medical resource sharing and exchange:* Cloud technology allows quick and spontaneous medical resource sharing and exchange from different sources upon users' connection to cloud servers via the Internet.
3) *Dynamic scalability of resources*: Cloud services are very flexible in scaling and adjusting to demands, and can support storage expansion demands for medical information systems when required.
4) *On-demand self-service:* In cloud computing, computation resource is a shared pool that can provide quick dynamic deployment to hospitals' demands upon purchase.
5) *Enhanced flexibility:* Medical documents stored in cloud servers can be accessed by authorized users anytime.
6) *Elimination of device limitation:* Irrespective of what computer or mobile services, users can enjoy services as long as they can connect to the Internet.
7) *High scalability and service integration:* Through cloud computation, services from different providers can all be integrated to create a single data center.

Cloud environment permits patient-centric structures to let patients manage their own Personal Health Records, which when stored in cloud environment is still at risk from that which the environment is exposed to. Also, security measures taken by the PHR service must also be trustworthy. Thus, a

Manuscript received October 16, 2012; revised November 20, 2012

Chia-Hui Liu is with the Department of Digital Literature and Arts , St. John's University, Taipei, Taiwan (e-mail: chliu@thu.edu.tw).

Tzer-Long Chen is with the Department of Information Management, Taiwan University, Taipei, Taiwan (e-mail: indurains5@yahoo.com.tw).

Han-Yu Lin, Chih-Ming Liu and Yu-Fang Chung are with the Department of Electrical Engineering, Tunghai University, Taichung, Taiwan (e-mail: kokokoko93lin@gmail.com, orsche_218@hotmail.com , yfchung@thu.edu.tw).

Fong-Qi Lin, En-Ping Wu, Tzer-Shyong Chen are with the Department of Information Management, Tunghai University, Taichung, Taiwan (e-mail: tonebeta@gmail.com , s974916@thu.edu.tw, arden@thu.edu.tw).

secure and efficient access control mechanism is needed to safeguard the privacy of users' medical information. As PHR emphasize availability, authenticity, and confidentiality of personal privacy over EMR's documental properties of non-repudiation and integrity, settings for allocating users' extent of right to use and access to part(s) of stored medical record cannot be compromised; also, unauthorized users should not have the corresponding keys. In addition, patients should have complete rights over access control which when necessary, can be set to add or remove access rights [1], [5]. In patient-centric medical record systems, patients can encrypt keys according to the authorized users. But this falls short of fulfilling the demands of multi-users. Although patients are the custodians of PHR, to ensure the integrity of their PHR, patients should not be allowed to modify medical reports. At the same time, doctors should have appropriate management rights to endorse PHR to bolster the content's credibility.

In this paper, we propose a dynamic access structure that can impart precise control access to cloud server's medical record under multi-user setting. To ensure every patient retains maximum control over their medical records, we adopted cryptography based on Lagrange multipliers for encrypting the records.

II. Related Work

A. Electronic Medical Record

Electronic medical records (EMR) is a type of medical record that electronically access, transmit, accept, save, retrieve, connect, and process multimedia information of past, present, and future records of patients' physiological and psychological conditions.

EMRs are increasingly in demand, necessitating legal and practical coordination needs to help institutions promote its employment. Various NGOs in the United States are currently outlining electronic medical record standards such as ASTM, HL7, and HIMSS. EMR standards in Europe are being overseen by TC/251 of CEN. The Internationalized TC215 has also taken into account standards setup by other organizations to setup standards of its own. On 24 November, 2005, Taiwan's Department of Health promulgated an approach to the production and management of EMRs by medical institutes specifying regulations and provisions on EMRs to order to implement and popularize EMRs among medical institutes at various levels. Amendments and improvements were also made to previous EMR regulations such as the Electronic Signature Act, the Physician Act, Medical Law, etc., establishing a legal basis for electronic medical records.

The personal health record (PHR) is proposed as an innovative solution to the problems of fragmented communication and lack of interoperability among diverse EMR systems. It provides for a single source (the patient's PHR) for authentication and remote access of the health information data from all EMR systems.

B. Personal Health Record

In 2005, the National Committee on Vital and Health Statistics (NCVHS) [6] outlined properties of the PHR and the PHR system as follows:

1) *Scope and Nature of Content:* All PHR systems must have consumer health information, personal health journals, and information about benefits and/or providers.

2) *Source of Information:* PHR data may come from the patient, caregiver, healthcare provider, payer, etc.

3) *Features and Functions:* PHR systems should offer a wide variety of features, including the ability to view personal health data, exchange secure messages with providers, schedule appointments, renew prescriptions, etc.

4) *Custodian of the Record:* The physical record may be operated by a number of parties, including the consumer or patient, an independent third party, or an insurance company.

5) *Data storage:* Data may be stored in a variety of locations, including an Internet-accessible database, provider's EHR, consumer/patient's home computer, or portable devices such as smart card or thumb drive.

6) *Technical approaches:* Current PHR and PHR systems are generally not interoperable, and they vary in how they handle security, authentication, and other technical issues.

7) *Party Controlling Access to the Data:* While consumers or patients always have access to their own data, they do not always determine who else may access it.

From the above listed properties, it can be inferred that the PHR data is compiled and integrated from diverse sources to provide a patient-centric health information exchange model that can be further distributed to different authorized users in part(s) or whole. As the PHR has broaden its scope, it is gradually being developed as a software, platform, or cloud application service integrating personal health services with the information and communications technology industry.

C. Medical Services and Cloud Computing

The fundamental service models of Cloud computing are:

1) *Software as a Service (Saas):* This service model provides software through the Internet with manufacturers installing applications on a cloud server. Clients do not acquire the software peruse, but rents web-based software that are updated and maintained by the vendor.

2) *Platform as a Service (PaaS):* Cloud providers offer a computing platform to its clients where they can deploy applications of its own, program languages of its own, all without having to maintain or control the cloud equipment.

3) *Infrastructure as a Service (IaaS):* Vendors integrate basic infrastructure such as IT systems and database and then rents them to clients.

Cloud computing contains several features. Computation resources gathered through resource pooling allows vendors to feature multi-tenant mode. Rapid elasticity grant unlimited possible configuration in dynamic distribution of resources according to user demand. Measured service can also monitor resource use to achieve automatic control and optimization of the cloud system. Users can also connect anywhere to cloud computing services, reducing user's dependence on terminal management equipment and related information technology expertise. There have been serious privacy concerns about outsourcing patients' PHR data to cloud servers, not only because cloud providers are generally not covered entities under HIPAA, but also due to an increasing number of cloud data breach incidents breaking out in recent years.

According to recent studies [7], we list some of the major concerns facing PHR development in cloud environment:

1) Abuse and nefarious use of cloud computing
2) Insecure interface and application programming interface
3) Malicious insiders
4) Shared technology issues
5) Data loss or leakage
6) Account or service hijack
7) Unknown risk profile

To deal with the risk of potential exposure of privacy, they should allow patients, the custodians of PHR full control of choice and options to medical record sharing. Undoubtedly, the use of encryption mechanisms can provide appropriate solutions to protecting medical information; but in addition to the traditional disposition of having service providers encrypting the data for the custodians, the PHR dispense users with access control mechanism [8].As under cloud environment patients' PHR are stored with outsourced providers, patients not only lose real control of these sensitive data, but faces elevated security risks. It has been difficult to achieve assurance on individual privacy when these patient-centric PHR access models are transferred to cloud servers to provide user access. Thus, our primary goal is to ensure the security of PHR, and provide for an ideal PHR with desired features of continuous real-time update and interactivity, as well as interoperability.

D. Cryptography and Encryption Systems

Following is a brief introduction to cryptography and encryption systems. [7], [9] [10] [11] [12]

1) *Basic cryptography:* Generally speaking, to oversee system security, a password system must at least have the following four functions:confidentiality, authentication, integrity, and non-repudiation.

In accordance with mathematical variances in keys, cryptography systems are divided into two major systems: private key cryptosystem, and public key cryptosystem.

2) *Private key cryptosystem:*By using the same secret key for encryption and decryption, private key cryptosystems facilitate efficient, quick, and low computation load. However, it has the following disadvantages:

- *Key distribution problem:* During the negotiation process of what private key is to be used between the message sender and the receiver, the ultimate decided private key has to be transmitted between the two parties, thus subjecting to security concern of possible theft during the key distribution process.
- *Key management issues:* As both sender and receiver must possess the secret key, when the number of users increases, the number of senders and receivers possessing the secret key will also increase.
- *Difficulty in achieving non-repudiation*: As both sides of the communication end possess the same encryption and decryption key, the encryptor can disavow previously encrypted sent messages, making it impossible for the third party to distinguish who is the real encryptor.

3) *Public key cryptosystem:* Public key cryptosystemis also known as asymmetric cryptosystem, or two-key cryptosystem. Public key cryptography has the following advantages:

- *Protects information privacy*: Anyone can use the public key of the recipient to encrypt plaintext messages into ciphertext.
- *Simplifies allocation and management of keys*: As the sender and recipient only need to store their own key pairs, and do not have to store other private keys even with the increase in the number of users, this simplifies key distribution and management problems.
- *Possess non-repudiation*: If the message is first signed with a private key, from the resulting signature, anyone can use the corresponding public key for verification.

III. The Proposed Scheme

This paper proposes a secure and effectively dynamic access scheme which allows users manage, access, or share PHR in Cloud computing environments. In the environment, multi-users can access to PHR for appending, revision, deletion, and inquiry. The proposed scheme consists of three phases, namely Initialization, Key generation and Derivation. The details are described in the following sub-sections.

A. Initialization

This study applies partially ordered access. A central authority (*CA*) builds the set-up for the partially ordered. A partially ordered set is a pair (S, $\preccurlyeq$), where $\preccurlyeq$ appears a reflexive, anti-symmetric, transitive binary relation with the set S.*CA* establishes a structure for these users, where there are n users which form two sets $S = \{S_1, S_2, ..., S_n\}$ and $H = \{H_1, H_2, ..., H_n\}$, as below:

S_1	S_2	…	S_i	…	S_n	
H_1	H_2	…	H_i	…	H_n	←secret & distinct

CA will build a structure that there are m files which form a set $file = \{file_1, file_2, ..., file_m\}$, and *CA* generates a corresponding decryption key to each $file_u$, for $u = 1, 2, ..., m$. The encrypted files are protected by the key from being randomly accessed. The decryption key is shown as DK_u, for $u = 1, 2, ..., m$.

$file_1$	$file_2$	…	$file_u$	…	$file_m$	
1	2	…	u	…	m	file ID, public
DK_1	DK_2	…	DK_u	…	DK_m	decryption keys, secret and distinct

A security class S_i presents authorization to access to $file_u$, written as $S_i=\{u: u$ is the file ID of S_i with access authority$\}$. For example $S_1=\{1, 2, 3, 4\}$, $S_2=\{1, 2, 3\}$, $\{1, 2, 3\} \preccurlyeq \{1, 2, 3, 4\}$, and then $S_2 \preccurlyeq S_1$. The following adjacency matrix can explain the access relationship.Assuming that there are six security classes and four files, put the {security classes}×{files} data in the two-dimensional array.

	$file_1$	$file_2$	$file_3$	$file_4$
S_1	1	1	1	1
S_2	1	1	1	0
S_3	0	1	1	1
S_4	1	1	0	0
S_5	0	1	1	0
S_6	0	0	1	1

The indicate function $I(x, y)$ is defined to present user i with authorization to obtain DK_u for accessing to $file_u$.

$$I(x,y)=\begin{cases}1 & \text{, if user } x \text{ has access to file } y\\ 0 & \text{, otherwise}\end{cases}$$

Variable x represents user's superkey$H$ID i and variable y represents *file* ID u. In each row, user i uses his secret superkeyH_i to access to row i. Row i, by construction, contains the set of *file* ID's which user i is authorized to visit.

B. Key Generation Phase

Step1: *CA* refers to the user i in $S = \{S_1, S_2, ...,S_n\}$ establishing individual and non-repeated superkeyH_i, for $i = 1, 2, ..., n$ to keep H_i in secret.

Step2: *CA* manages superkeysH_i of all users and sets indices for legal superkeyH_i,

$$I_{\{H_1,...,H_n\}}(x)=\begin{cases}1 & ,if \quad x\in\{H_1,...,H_n\}\\ 0 & ,o.w.\end{cases}.$$

$I_{\{H_1,...,H_n\}}(x)$ means the indicate function of set $H = \{H_1, H_2, ..., H_n\}$.

The legality of H_i is verified by $I_{\{H_1,...,H_n\}}(x)$.

Step3: *CA* establishes function $A_i(x)$ for each user i.

Let $$A_i(x)=\left\{\prod_{\substack{k=1\\k\neq i}}^{n}\frac{(x-H_k)}{(H_i-H_k)}\right\}\times I_{\{H_1,...,H_n\}}(x)$$

for$i = 1, 2, \ldots, n, x \in R$.

Step4: *CA* selects non-repeated random integers $\{DK_1, DK_2, \ldots,DK_m\}$(supposing there are m confidential files) as the decryption key for encrypting/decrypting confidential files. *CA* keeps DK_u in secret and publishes the public parameter u.

Step5: *CA* sets $J_i = \{u: 1 \le u \le m, u$ is the file ID of S_i with access authority$\}$. There are n users for $i = 1, 2, ...,n$ and m files for $u = 1, 2, ..., m$. J_i is the set of *file* ID which user i is authorized to visit.

Step6: *CA* sets the index $I_{J_i}(y)=\begin{cases}1 & ,if \quad y\in J_i\\ 0 & ,o.w.\end{cases}$ to present user i with authorized access to DK_u and each user i establishes function $B_i(y)$,

Let $B_i(y)=\left\{\sum_{u\in J_i}DK_u\left[\prod_{\substack{t=1\\t\neq u}}^{m}\frac{(y-t)}{(u-t)}\right]\right\}\times I_{J_i}(y)$ $y, u, t \in R$

Step7: *CA* establishes function,

$$G(x,y)=\sum_{i=1}^{n}A_i(x)B_i(y),\ x, y \in R.$$

That is:

$G(x, y) = A_1(x)B_1(y)+A_2(x)B_2(y)+\ldots+A_n(x)B_n(y)$ for $(x, y) \in R\times R$ and declares it publicly.

C. Key Derivation Phase

Step1: User i substitutes personal superkey$H_i$into $I_{\{H_1,...,H_n\}}(x)=\begin{cases}1 & ,if \quad x\in\{H_1,...,H_n\}\\ 0 & ,o.w.\end{cases}$. When the superkey$H_i$ appears in the legal verification list of *CA*, $H_i \in \{H_1,...,H_n\}$, then $I_{\{H_1,...,H_n\}}(H_i)=1$.

When Hi of user i is not an authorized superkey in the list, $I_{\{H_1,...,H_n\}}(H_i)=0$.

Step2: User i substitutes personal superkey$H_i$into $A_i(x)=\left\{\prod_{\substack{k=1\\k\neq i}}^{n}\frac{(x-H_k)}{(H_i-H_k)}\right\}\times I_{\{H_1,...,H_n\}}(x)$.

When the personal superkey H_i of user i is legally verified in CA, the user substitutes $I_{\{H_1,...,H_n\}}(x)=1$ for calculation, and then $A_i(H_i) = 1$ and $A_i(H_k) = 0$ for $k \neq i$

Step3: User i substitutes $file_u$ ID u for $I_{J_i}(y)=\begin{cases}1 & ,if \quad y\in J_i\\ 0 & ,o.w.\end{cases}$, $J_i = \{u: 1 \le u \le m, u$ is the file ID of S_i with access authority$\}$. When user i presents authorization to access to DK_u, $y \in J_i$then $I_{J_i}(y)=1$.

Step4: User i substitutes $file_u$ ID u for $B_i(y)=\left\{\sum_{u\in J_i}DK_u\left[\prod_{\substack{t=1\\t\neq u}}^{m}\frac{(y-t)}{(u-t)}\right]\right\}\times I_{J_i}(y)$.

When user i is authorized to access to DKu, then $B_i(y) = D_{ky}$ if $y \in J_i$ and $B_i(y) = 0$ if $y \notin J_i$.

Step5: User $i$calculates $G(x,y)=\sum_{i=1}^{n}A_i(x)B_i(y)$.

If $x \in \{H1, H2, \ldots,Hn\}$ and $y \in Jx.$, $G(x, y) = D_{Ky}$. The user could successfully obtain the decryption key, and $G(x, y) = 0$, otherwise.

IV. Example

This section would explain the access of PHR scheme in medical environments. *CA* distributes patients, doctors, nurses, medical research units, health insurance units, and family into various security class S_i and distributes the corresponding superkey H_i to each user. Different PHR records, such as blood pressure, electrocardiogram, major operations, drug allergy, and health insurance records, are stored in $file_1 \sim file_5$, respectively for encryption and generating the corresponding decryption keys $DK_1 \sim DK_5$. The relations between the encrypted file and the access relationship are shown in Table II. Function $I(x, y)$ is used for presenting that user i is authorized to obtain DK_u for access to $file_u$. $I(3, 4) = 1$ presents that the nurse S_3 is authorized to access to $file_4$, and $I(5, 4) = 0$ shows that S_5 cannot access to $file_4$.

V. Conclusion

The proposed scheme is able to access to PHRssystem accurately, and is suitable for immense dynamic multi-users.The constructed formula $G(x, y)$ could immediately adding and deleting user authorization for subjoining and altering personal health records during dynamic updates. To face the threats of Cloud, a more secure and more efficient access control scheme is constructedto protect patients' privacy, ensure the security of users' medical information, andenhance the reliability of PHR encryption.The achievements in this study are presented as follows:

1) The proposed scheme is able to resist internal and external attacks.
2) It is convenient for managingCA by using only one public formula $G(x, y)$.
3) The generation of keys and the algorithms are simple, andthe public parameters are only $G(x, y)$ and u.
4) The PHR system allows patients to determine the access users, and remove the outdated authorization.
5) The proposed scheme overcomes the dynamic access control problems.

TABLE I: THE DEFINED SYMBOL AND PARAMETER

Notation	Definition	Function
S_i	Security class, S_i = {u: u is the file ID of authorized S_i}, for i = 1, 2, ..., n	To classify the security class of users
H_i	SuperkeyH_i , for i = 1, 2, ..., n	To obtain the key authoring $file_u$
DK_u	Decryption key, for u = 1, 2, ..., m	To decrypt the key of $file_u$
$file_u$	$File_u$, for u = 1, 2, ..., m	The DK_u-encrypted file
$I_{\{H_1,...,H_n\}}(x)$	The indicate function of set $\{H_1, H_2..., H_n\}$	To calculate whether H_i is in the legal verification list of CA
J_i	J_i= {u: 1 ≤u ≤m, u is the file ID of authorized S_i}	The set of files authorized by the users

TABLE II: EXAMPLE

	$file_1(DK_1)$ Blood pressure	$file_2(DK_2)$ Electrocardiogram	$file_3(DK_3)$ Major operation	$file_4(DK_4)$ Drug allergy	$file_5(DK_5)$ Health insurance
$S_1(H_1)$: Patient	1	1	1	1	1
$S_2(H_2)$: Doctor	1	1	1	1	0
$S_3(H_3)$: nurses	1	0	0	1	0
$S_4(H_4)$:Medical researcher	0	0	0	1	0
$S_5(H_5)$: Health insurance unit	0	0	0	0	1
$S_6(H_6)$: Family	1	0	0	0	0

ACKNOWLEDGEDGEMENT

The work is partially supported by a project from NSC, Taiwan with grant no. 101-2410-H-029-004.

REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and Fine-grained data access control in multi-owner settings," *Security and Privacy in Communication Networks,* pp. 89-106, 2010.
[2] *Health Insurance Portability and Accountability Act of 1996*, US Public Law, 104th Congress, Public Law 104–191, 1996.
[3] C. M. Yanga, H. C. Lina, P. Changb, and W. S. Jianc, "Taiwan's perspective on electronic medical records' security and privacy protection: Lessons learned from HIPAA,"*Computer Methods and Programs in Biomedicine*, vol. 82, pp. 277– 282, 2006.
[4] CASE STUDY: Geisinger Health System-Bringing HIPAA Compliance to an Electronic Medical Record System. *Qualys on Demand Vulnerability* Management. [Online]. Available: http://www.qualys.com/docs/geisinger.pdf
[5] K. Anastasakis, B. Bordbar, G. Georg, I. Ray, and M. Toahchoodee, "Ensuring Spatio-Temporal Access Control for Real-World Applications," in *Proc. the 14th ACM symposium on Access control models and technologies*, 2009.
[6] *Personal Health Records and Personal Health Record Systems*, National Committee on Vital and Health Statistics, US Department of Health and Human Services, pp. 15, 2006.
[7] X. Lai, and J. Massey, "A Proposal for a New Block Encryption Standard," in *Proc. Eurocrypt'91, Springer-Verlag, LNCS,* vol. 473, pp. 389-404, 1991.
[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in *Proc. the ACM workshop on Cloud Computing Security*, pp. 103–114, 2009.
[9] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme based on Discrete Logarithms," *Advances in Cryptology-Crypto'85, Springer-Verlag, LNCS,* vol.196, pp. 10-18, 1985.
[10] N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203-209, 1985.
[11] V. Miller, "Use of Elliptic Curves in Cryptography," *Advances in Cryptology- Crypto'85, LNCS,*vol. 218, pp. 417-426, 1985.
[12] D. E. Denning, "Cryptographic Checksums for Multilevel Database Security," in *Proc. the 1984 IEEE Symposium on Security and Privacy*, pp. 52-61, 1984.

Chia-Hui Liu received her PhD degree in Electrical Engineering from National Taiwan University, Taipei, Taiwan. She is now an assistant professor in the Department of Digital Literature and Arts at St. John's University, Taipei, Taiwan.

Tzer-Long Chen received his PhD degree in Information management from National Taiwan University, Taipei, Taiwan. He works as an assistant professor in several colleges in Taiwan.

Han-Yu Lin received his bachelor degree in Electrical Engineering from Tunghai University, Taichung, Taiwan. He is currently working toward the master degree in Electrical Engineering at Tunghai University, Taiwan.

Fong-Qi Lin received his bachelor degree in Computer Science from Tunghai University, Taiwan. His is working toward the master degree in Information Management at Tunghai University, Taichung, Taiwan.

Chih-Ming Liu received his bachelor degree in Electronic Engineer from Ming Chuan University, Taoyuan, Taiwan. He is working toward the master degree in Electrical Engineering at Tunghai University, Taichung, Taiwan.

En-Ping Wu received her bachelor degree in Information Management from Tunghai University, Taichung, Taiwan.

Yu-Fang Chung received her PhD degree in Electrical Engineering from National Taiwan University, Taipei, Taiwan. She is now an associate professor in the Department of Electrical Engineering at Tunghai University, Taichung, Taiwan.

Tzer-Shyong Chen received his PhD degree in Electrical Engineering from National Taiwan University, Taipei, Taiwan. He is now a professor in the Department if Information Management at Tunghai University, Taichung, Taiwan.