A reliable authentication scheme of personal health records in cloud computing

Chia-Hui Liu¹ · Tzer-Long Chen² · Chien-Yun Chang³ · Zhen-Yu Wu⁴

Accepted: 28 July 2021
© The Author(s) 2021

Abstract

A patient-centered personal health records system has been actively promoted in recent years. Its purpose is to maintain long-term personal records and health improvement plans. It combines a cloud computing environment to build a personal health records system to quickly collect personal information and transfer it to the back end for storage for future access. However, in a cloud environment, the message transmission process is more open. Therefore, a lack of an authority security mechanism for the users of such an architecture will result in distrust and doubt by the users. This adversely affects the implementation and quality of long-term health plans. To protect the crucial privacy of the users from malicious attacks or theft, it is necessary to ensure that the users have different authority to access their personal health records under the cloud computing environment and manage the openness of their authority to other users. A secured identify authentication mechanism can ensure that only legitimate users can log in to the system and obtain system service resources through verification. For a personal health records system in the cloud computing environment, this study proposes a secure and reliable user authentication mechanism allowing relevant users access to the user's PHR in the cloud based on their authority. The proposed authentication method uses a password combined with a smart card, allowing the owner and authorized users to log in to the system and access the relevant personal records. In this study, an authentication method based on bilinear pairing was used to verify the identity of users and to effectively prevent malicious intrusion and theft.

Keywords Personal health records · Cloud computing · ID authentication · Smart card · Bilinear pairing

1 Introduction

With the development and progress over time, medical institutions of all levels have transformed paper-based records into electronic medical records (EMRs) [1] as the main recording method. With EMRs, personal medical information, including personal health status and medical care received, can be recorded and stored perpetually. Authenticated, authorized medical staff may have access to the medical records to make additions, modifications, or to exchange records. Although many medical institutions have converted to EMRs, current systems focus on the effectiveness of management and transmission of the records. As for the exchange of records, many frameworks and methods have been proposed; however, none of them have been widely accepted. Therefore, achieving complete interoperability between medical institutions remains an important issue. In addition, the main scope of EMRs is to serve professional medical staff delivering clinical

✉ Tzer-Long Chen
tlchen1976@pu.edu.com

Chia-Hui Liu
ljh34@ulive.pccu.edu.tw

Chien-Yun Chang
yunj@teamail.ltu.edu.tw

Zhen-Yu Wu
zywu@gms.npu.edu.tw

¹ Department of Applied Mathematics, Chinese Culture University, Taipei, Taiwan

² Department of Finance, Providence University, Taichung, Taiwan

³ Department of Fashion Business and Merchandising, Ling Tung University, Taichung, Taiwan

⁴ Department of Information Management, National Penghu University of Science and Technology, Penghu, Taiwan

treatment, focusing on the healthcare of patients and management of the system. With the improvement and popularization of many basic information technologies and the rising self-awareness of the patients of their own healthcare, in addition to many diagnostic medical studies, services employing new IT and medical information systems have become more popular, deriving long-term healthcare models in subsequent sustained treatment, care, and the maintenance of personal healthcare records. The World Health Organization (WHO) advocates that the care of patients by medical institutions should be changed from a passive to preventive approach, i.e., patients are expected to actively participate in medical care. Thus, personal health records (PHRs) [2] could be feasible solution, because PHRs can not only store complete personal medical information but can also be initiatively maintained by the patient to subsequently effectively communicate with healthcare providers (e.g., physicians, caregivers). All records from medical visits can be sent to the PHR servers via the Internet; therefore, patients can check the data for each visit, and at the end of the medical procedure, a summary and other information can be provided to the patients. This effectively promotes patients' understandings of their own care and improves the relationship between the patients and care providers, increasing patient satisfaction and motivating patients to engage more in future healthcare plans. PHRs play an important role in effective communications between patients and the healthcare service providers. In addition to a complete record and preservation of personal medical information, more importantly, the patients can actively participate and maintain the records. All medical records received are transmitted to the PHR backend server through the network environment; therefore, patients can immediately access the information of each medical service anytime and anywhere after completing the authentication. Medical summaries can be provided to the patients in a timely manner after each stage of diagnosis and after treatment has ended. This can promote the patients' understanding of their own healthcare, increasing the clarity of communicating subsequent healthcare plans, effectively improving overall medical service satisfaction, and inspiring patients to engage more willingly in future healthcare plans.

With the advent of cloud computing, medical information technology and service providers began to provide their PHR services based on the cloud computing environment. The cloud provides storing space and software as a service, in which service providers can usage almost infinite and flexible storing space and computing resources. Therefore, instead of building a dedicated data center, PHR providers prefer a cloud computing environment for PHR systems to reduce their operating costs. The PHR system built by employing cloud computing collects and stores the

user's various physiological data, health information, and related medical information which are all related to the user's personal privacy. However, due to the openness of the cloud environment, how to ensure the security and privacy of user information, prevent malicious attacks on the Internet, and provide security authentication for users with different identities during the process of data transmitting or information update have become critical issues the cloud-based PHR systems encounter. PHR investments are usually based on the goals of profit and efficiency, increasing the system function for users, or improving users' health management. However, some of the patients' greatest concerns are the safety and confidentiality of PHRs and other healthcare systems. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) [3, 4] outlined the legal protection of PHRs' privacy and security. Therefore, introducing PHR services into the cloud requires the careful evaluation of the privacy and system security of PHRs. Although digital PHRs can offer further security features, such as password protection and record tracking, compared to paper-based records, outsourcing PHRs to cloud computing servers makes users' personal health information exposed on the internet. There are many threats in cloud services, including: no strict or careful verification of user identity; insufficient security in user interfaces for authentication and authorization; the abuse of cloud computing for illegal behavior; malicious inside staffs of cloud service providers; issues caused by shared environments; the theft of data or services, etc. To address to these concerns, this study proposes a cryptographic authentication scheme based on bilinear pairing for PHRs in the cloud computing. Bilinear pairing is a mapping relationship taking a cyclic group to correspond to another cyclic group; the security of the encryption and decryption mechanism based on it is constructed on the difficulty of trying to solve special problems.

In the PHR system in the cloud environment, the authorized users can manage the records at any time and place without been restricted to the availability of other users online to respond to the access requests. Therefore, if there is a lack of a comprehensive identity authentication security framework, it won't earn the trust of the users, leading to an impaired healthcare service quality. The innovation of this study lies in the proposal of a reliable identity verification mechanism with security and privacy protection and low computational cost suitable for wireless cloud environment. This authentication mechanism uses a smart card to store authentication information and a bilinear pairing password system for identify authentication, which ensures that only legitimate users can log in to the system, and the system service resources can be used after identify verification. The framework in this study also incorporated smart cards as a security identify

authentication mechanism, adding time stamps as a timeliness test to ensure that authentication processes can only be made within a specific timeframe, which greatly strengthens the security mechanism. In the subsequent security analysis, this study also explains that the proposed method can achieve effective security through ensuring the security and privacy of the path between the user and the server.

2 Literature review

2.1 Personal health records

According to the definition in [5], PHRs systems allow people to access and manage their own medical or health information. A user's PHRs can be stored in an electronic format and be translated into a standard format to comply with the security requirements of HIPAA and HL7 originally implemented by medical service providers. The online environment may also contain information to help users make the proper decisions and to improve the quality of their healthcare. PHR systems integrate patient health information from different sources, including the patient's own measurement records, physician records, hospital and laboratory records, etc. PHRs can also include medical-related reference materials, medical treatment, drug use, and other non-medical management materials. Part of the PHR may also include data from EMR databases. However, the most difference between PHR and EMR is that EMR must meet the absolute requirements of non-repudiation and integrity of medical documents. The main purpose of PHRs is to help people develop an in-depth understanding of their own health and use it as a tool for lifelong health management. The value of PHRs lies in the long-term accumulation of health records, which not only promotes personal health, but also provides sufficient reference for health caregivers in the future when dealing with medical conditions. PHRs are a digitalized integration and application of all personal medical and health-related records. [6] At present, most information systems of medical service organizations are based on HIPAA regulations and adopt the HL7 seven-layer structure, and PHR systems can conform to the information systems of medical institutions at all levels in a standardized storage format. They can update all the user's physiological conditions, medication information, health check results, and other information [7] for long-term retention. According to the definition of the American Health Information Management Association (AHIMA), the main purpose of PHRs is to record the complete health information of users, including short-, medium-, and long-term medical records, which can even be used as references in future medical

visits, medication consultations, or even diet and health plans. PHRs are also a highly portable, flexible, and expandable database; they can be extended to various levels of medical institutions, such as hospitals or local pharmacies. PHR systems can integrate diagnoses from medical institutions and the user's personal daily physiological health records. A long-term continuous health record is developed, including the user's diet status (content, calories, and nutrients in three meals), physiological status (heartbeat, blood pressure, and blood sugar), and exercise behavior (exercise frequency, and nature), and other related medical records, providing users with a clear understanding of their own physical conditions while the data can also be made available for medical research purposes. PHRs should possess the following characteristics [8, 9]: (i) the users should possess the absolute power to control their own PHRs, decide which sections can be made open-access for those who are authenticated, and set the timeliness status; (ii) the PHRs should cover all medical records and other healthcare information of the user; (iii) the PHRs must adhere to strict privacy and security in the process of access and transmission of data; and (iv) the PHR owner can clearly view when the records have been accessed, and the additions or modifications which have been made. The Health Information Technology for Economic and Clinical Health Act (HITECH) proposed in the United States greatly improved the relevant protection regulations for the privacy and security of medical information stipulated in the Health Insurance Circulation and Accountability Act (HIPAA) in 2009. PHR systems can collect patient health data from a variety of sources, including patient physiological state records (such as blood pressure, heartbeat, blood sugar, etc.) measured by automatic sensing devices or manual measurements, physician visit records, health check records (such as X-rays and other medical images), and other related documents, such as legal documents, power of attorney, insurance documents, etc. In addition, PHRs can also integrate other related medical knowledge on the system to provide users with reference standards when needed, such as emergency medical treatments, medication-related consultation materials, and even other non-medical health management knowledge.

2.2 PHRs in cloud computing environments

Due to the many benefits of cloud computing, PHRs in the United States are becoming more popular. Health management's services such as context-aware health monitoring, personal health-aware devices, intelligent alert management, pervasive lifestyle incentive management, etc., are built on cloud computing frameworks. The U.S. government has also proposed a Health Cloud plan,

integrating personal healthcare information, clinical case history, hospital healthcare, and telehealth into cloud services. The Clinical Informatics Research of the University of Washington has developed the Patient-centered Health Record (PcHR) which the users own and controls. The trend of these cloud applications facilitates the development of PHRs as patient-centered health information exchange models. Based on the source for the PHRs, there are four different emerging PHR system types, which are defined as third-party/free standing, provider-tethered, payer-tethered, and interoperable PHR systems. However, the major concerns about PHRs pertain to security and stability. Cloud computing completely depend on the Internet as the operation medium. Based on the research of [10], this study briefly describes the major threats encountered in developing PHRs in cloud environments as follows: the manipulation of cloud computing; unconfident interfaces; fake users in the system; lost information; unidentified PHR profiles; and cloud account hijacking. In the face of threat, although there are legal protections provided by the information-related laws and regulations, healthcare systems also have administrative provisions, such as the U.S. Health Insurance Portability and Accountability Act (HIPAA) and the Canadian Personal Information Protection and Electronic Documents Act, which protect the data security and privacy of cloud users. However, considering the security of cloud environments, it is still necessary to strengthen information systems to effectively ensure confidentiality and only legitimate access to PHRs. In order to cope with the hazard of potential exposure to private information, rather than allowing PHR providers encrypt users' data, PHR services should allow users, i.e., PHR owners, complete control over the medical records they choose to share. Undoubtedly, employing encryption mechanisms can provide suitable solutions to protect the security of medical information. In addition to traditional practices of service providers encrypting medical record data, PHRs should also provide an access control mechanism for users [11]. However, in the past, the access control environments of these PHRs have not been targeted at cloud computing environments. In the cloud environments, patient's PHRs are stored in the facilities of outsourced service providers. The patients not only lose actual control over their own sensitive information; the risk of security breaches also increases. It is difficult to fully guarantee personal privacy and be trusted when patient centered PHR access models are uploaded to the cloud server to provide authorized user access [12]. Therefore, our major goal was to ensure the security of PHRs. The ideal PHR should be equipped with the characteristics of continuous real-time updates, as well as interactivity and interoperability. We need more flexible

access control mechanisms to strengthen each patient's personalized privacy policy.

2.3 Bilinear pairing

Shmair proposed an identify-based cryptosystem [13]. The concept was to take the user's personal information as a public key for encryption and decryption; however, due to the lack of an efficient encryption system, this concept was not successfully developed, until Boneh and Franklin [14] proposed Weil pairing-based cryptography. Weil pairing gradually became an encryption and decryption tool for the construction of identity authentications or digital signatures. Weil pairing can map a set of points on an elliptic curve to a multiplicative cyclic group in a finite area, by which a DLP (discrete logarithm problem) on the elliptic curve can be converted into a general discrete logarithm. Therefore, Weil pairing can play an important role because of its bilinear pairing function. Bilinear pairing is a relationship which takes two cyclic groups mutually corresponding to a linear mapping function, applying them to elliptic curves and forming group relationships in algebraic geometry. In the application of cryptographic geometry, bilinear matching has the following definitions and characteristics. G_1 is a group with an order as a large prime number of q and generator p ; G_2 is also a group whose order is a large prime number q , G_1 is an additive cyclic group and G_2 is a multiplicative cyclic group. The linear mapping function is $\hat{e}: G_1 \times G_1 \rightarrow G_2$. The mapping function of this pairing satisfies the following three points:

2.3.1 Bilinear

Assuming that P , Q , and R all belong to the points of G_1 :

$$\hat{e}(P, Q + R) = \hat{e}(P, Q)\hat{e}(P, R),$$

$$\hat{e}(P + Q, R) = \hat{e}(P, R)\hat{e}(Q, R),$$

In addition, any satisfying $a, b \in \mathbb{Z}_q^*$ will hold the following formula:

$$\hat{e}(aP, bQ) = \hat{e}(abP, Q) = \hat{e}(P, Q)^{ab}.$$

2.3.2 Non-degenerate

If P is a generator of G_1 , $\hat{e}(P, P)$ will also be a generator of G_2 , i.e., $\hat{e}(P, P) \neq 1$.

2.3.3 Computable

If both P and Q belong to the generator of G_1 , $\hat{e}(P, Q)$ can be calculated efficiently.

The security and reliability aspects in this article are based on the assumption of the bilinear Diffie–Hellman problem, referred to as BDH. Using BDH for bilinear

pairing [15], the problem is to assign to $(P, aP, bP, cP)(a, b, c \in \mathbb{Z}_q^*)$; when a , b , and c are unknown, calculating $W = \hat{e}(P, P)^{abc} \in G_2$ is infeasible. $\hat{e}$ is a mapping function: $\hat{e}: G_1 \times G_1 \rightarrow G_2$ and P is the generator of G_1 . There is no known method that can effectively solve the BDH problem. Therefore, it can be concluded that the bilinear pairing problem hypothesis is a difficult problem with reasonable security and confidentiality.

3 Methodology

With the continuous promotion of PHRs and other related programs in recent years, patient-centered self-maintenance and management of the patients' own health condition and care plan have been advocated. More and more medical institutions are adopting PHRs; this does not only strengthen patients' communication with medical care personnel but can also effectively reduce costs and increase operational efficiency. Coupled with the continuous improvement of cloud environments, personal health statuses are more quickly and accurately recorded and transmitted to the cloud backend servers through wireless network environments for information integration. In cloud environments, applying PHRs in healthcare can bring many advantages and increase users' initiation in participating in healthcare plans. However, PHR systems record a wide range of information (e.g., records of medical visits, medication records, physiological information, etc.) which can be used by multiple users (such as the patient, the attending physician, family members, caregivers, etc.) as well as in many extended platforms (such as homes, hospitals, and even local pharmacies, etc.); therefore, to satisfy the needs of multiple users in different locations, the dynamic access mechanism on the PHR system must be quite comprehensive to ensure that the user can pass identity verification when accessing the data—privacy and security of the data must be ensured during the transmission. Therefore, considering the above-mentioned security issues, this study proposes an effective identity authentication mechanism to verify legitimate users.

Under any circumstances, it is very important that PHR systems have a comprehensive mechanism to protect users' privacy; for example, some patients with particular diseases do not want to be publicized. This is especially when such systems mostly use cloud computing-based architecture as the method of transmitting data information. These factors and environments make traditional security architectures and protocols incompatible. Therefore, this study designed an authentication method which can be used in cloud computing environments by means of a secure identity authentication mechanism to ensure that user information security and privacy are protected. In addition,

time parameters can be added to link data access actions, which limit authorized personnel to complete authentication within a specific time frame, as well as to read the data within a specified time frame without repeating identity verification to increase efficiency. The complete identify verification mechanism in this study adopted the dual identify authentication of a smart card and password. The verification process consisted of four stages: the initial stage, the registration stage, the login stage, and the verification stage. This is further explained in the subsequent sections.

Before the users or the doctors, nurses, or healthcare staff in the healthcare institutions utilize the PHR system in the cloud computing environment, they must first register with the central authority. When the registration is successful, the central authority will issue a smart card to the user through the safety channel of the institution, including a user identity and require the user to set a password. The smart card will be distributed through personnel check and identity verification to ensure the card holder is the registered user which means the central authority assign the user smart card securely. Then, the user can use this smart card with a wireless mobile device, e.g., PDA or Notebook, to log in to the system. After confirming, through the proposed identity authentication mechanism, the log-in user is a legitimate user who can access the data, the user can query and use the user's PHR data in the cloud in the hospital or healthcare institution within a limited time to legitimately obtain the physiological information and related medical and health information of the care recipient.

3.1 Initial phase

Every user in the PHR system needs to register with the central authority (CA).

Step 1: Let p be a random large prime number, such that $q|p-1$ for some large prime number q . CA selects a random number $a \in \mathbb{Z}_q^*$ and a bilinear map $\hat{e}: G_1 \times G_1 \rightarrow G_2$. Let G_1 and G_2 be two cyclic groups of order q where G_1 is a group of point of an elliptic curve E over F_p and G_2 is a multiplicative subgroup of F_p^* . G_1 and G_2 have the same order q . Let $P_0 \in G_1$.

Step2: CA computes $P_{\text{pub}} = a * P_0$. P_{pub} is a public key. CA generates two hash functions, H_1 and H_2 , as $H_1: \{0, 1\}^* \rightarrow G_1$ and $H_2: G_2 \rightarrow \{0, 1\}^*$.

These system parameters will be written into the smart card of the legitimately registered users.

3.2 Registration phase

Step 1: The user registers with CA a legitimate uid and sets the password upw .

Step 2: The user sends a registration request to the server through a secure channel; the request content contains $\{uid, upw\}$.

Step 3: After the CA receives the registration request from the legitimate user, it calculates a public parameter $Q_i = H_1(uid)$ and $D_i = a * Q_i$ as a private parameter.

Step 4: CA selects a random number r_i and calculates R_i, V_i for the user.

$$F_i = (D_i + r_i * Q_i)^{-1} \quad (1)$$

$$V_i = r_i * F_i \quad (2)$$

$$R_i = r_i P_0 \quad (3)$$

Step 5: CA personalizes the user-specific smart card; the card contains the parameters $\{uid, upw, R_i, V_i\}$.

Step 6: The server delivers the smart card to the user securely and privately.

3.3 Login phase

The user inserts the smart card into the device and enters uid' and upw' to log in. Then, the smart card will perform the following steps:

Step 1: Check whether the user input $\{uid', upw'\}$ is the same as the $\{uid, upw\}$ stored in the smart card; if yes, execute the next step; otherwise, terminate the login.

Step 2: Use the current login time stamp T_i and parameter R_i to calculate the $AUTH_i$.

$$AUTH_i = U_i * V_i, \text{ where } U_i = (P_{pub} + R_i)H_2(T_i)^{-1} \quad (4)$$

Step 3: Send $\{uid, T_i, AUTH_i\}$ to CA as a login request.

3.4 Verification phase

After the CA receives the login request and parameters $\{uid, T_i, U_i, V_i\}$, it will verify the user's identity through the following protocol:

Step 1: When CA receives the login request, it will first check whether $T_{now} - T_i < \Delta T$ is established. T_{now} represents the current time of the system, and ΔT represents the transmission delay time. If the judgment is true and the login request is verified as legitimate by the server, proceed to step 2. Otherwise, terminate the request.

Step 2: CA verifies whether $\widehat{e}(Q_i, H_2(T_i))^{AUTH_i}$ is equal to $\widehat{e}(P_0, r_i)$. If the conditional formula is equivalent, the

user's login request is approved and confirms that the user is valid. Otherwise, the request is terminated.

$$\widehat{e}(Q_i, H_2(T_i))^{AUTH_i} = \widehat{e}(P_0, r_i) \quad (5)$$

Example This section exemplifies the application and context of the PHR identity authentication method in the cloud. At first, a hypothetical context will be set up; then, the details of the entire verification process will be described. A PHR may store data on a back-end server or on the cloud and requires total management of the user. It may allow access to multiple users, such as doctors, family, nurses, caregivers, etc. who must apply for a personal account and an exclusive smart card and use the smart card to log in to the system. Only after the verification is completed can they access and use the server data. Namely, in the PHR system, the PHR from different sources are appropriately encrypted and stored in the cloud server. CA assigns patients, doctors, nurses, medical research units, health insurance units, and family members to different security classes; at the same time, the personal information of individual users will be recorded. The method proposed in this study mainly focuses on the PHR system in the cloud environment. Because PHR may also contain more private medical information, it is necessary to log in to the system through a smart card and then verify through the proposed authentication algorithm. Compared to the proposed algorithm in [11], this study adopts a two-factor authentication model to improve user privacy security. Below is a real-life example for the proposed method:

Step1: Suppose there is a medical worker, Alice, who needs to access and view the patient's PHRs through the cloud to assess the patient's health and give suggestions to improve the patient's health.

Step2: She must first register a legitimate account ID_{Alice} with CA and set a password PW_{Alice} . CA will then calculate V_{Alice} and R_{Alice} by calculating her public parameter Q_{Alice} , secret parameter D_{Alice} , and random number r . CA uses these parameters to customize a personalized smart card and delivers it to user Alice.

Step3: To log in to the system, User Alice first inserts the exclusive smart card into the device for reading; then types in her own ID_{Alice} and password PW_{Alice} . The log-in time T_{Login} and the parameter R_{Alice} are used to calculate $AUTH_{Alice}$ and the result of $\{ID_{Alice}, T_{Login}, AUTH_{Alice}\}$ is sent to CA as a login request.

Step4: CA will calculate and verify whether $\widehat{e}(Q_{Alice}, H_2(T_{Alice}))^{AUTH_{Alice}}$ is equal to $\widehat{e}(P_0, r_i)$

It will accept the user's login request message only when it is equal.

4 Security analysis

4.1 Correctness

The verification of the correctness of the authentication mechanism proposed in this paper is as follows: Assuming that the time when the CA receives the user's login request is T'_i , CA verifies whether $\hat{e}(Q_i, H_2(T_i))^{AUTH_i}$ is equal to $\hat{e}(P_0, r_i)$ as the following. If $T_i = T'_i$, it can be verified that $\hat{e}(Q_i, H_2(T_i))^{AUTH_i}$ is equal to $\hat{e}(P_0, r_i)$ if the conditional formula holds.

$$\begin{aligned}
 & \hat{e}(Q_i, H_2(T_i))^{AUTH_i} \\
 &= \hat{e}(Q_i, H_2(T_i))^{U_i * V_i} \\
 &= \hat{e}(Q_i U_i, H_2(T_i) V_i) \\
 &= \hat{e}\left(Q_i H_2(T_i)^{-1} (P_{pub} + R_i), H_2(T_i) * r_i * f_i\right) \\
 &= \hat{e}\left(Q_i H_2(T_i)^{-1} (P_{pub} + R_i), H_2(T_i) * r_i * \frac{1}{(D_i + r_i * Q_i)}\right) \\
 &= \hat{e}\left(Q_i H_2(T_i)^{-1} (P_0(a + r_i)), H_2(T_i) * r_i * \frac{1}{(Q_i(a + r_i))}\right) \\
 &= \hat{e}\left(P_0 * Q_i * (a + r_i), r_i * \frac{1}{(Q_i(a + r_i))}\right) \\
 &= \hat{e}(P_0, r_i)
 \end{aligned}$$

4.2 Password protection

The purpose of a PHR system built on cloud computing is to improve users' health conditions through user's self-management and integration with other healthcare resources. Therefore, in addition to the owner, users of the records may also include authorized persons, such as family members, physicians, and related caregivers. The user of each system has a personal ID and set password. One must key in the set password to log in to the system. However, when using the password to log in, one must ensure that the password will not be stolen by an actor intent on invading the system. Therefore, reliability and security required for the corresponding protection are relatively important. In addition, it is necessary to ensure that the password will not be leaked, and the protection mechanism must be comprehensive. Several common attack methods used to steal user ID and password details to log in to such systems are listed as follows:

- 1) The attack stealing password authentication: the purpose of this type of attack is to steal the user's authentication data from the server, such as the values of uid and upw stored in the backend. In the method proposed in the study, the server does not need to store the user's verification information; it is instead stored in the smart card. The user cannot know the information after the hash processing; thus, this method protects from this attack method of verification form theft;
- 2) Connection- and password-guessing attack: the method of this attack is to connect to the target host and then log in to the target account through password guessing, tracking, etc. However, during the login process, the parameter value of V_u calculated by the smart card and the user's private parameter D_u must be obtained and deciphered to obtain the user's password. The private parameter is encrypted using Bilinear Map $\hat{e}$; therefore, anyone who wants to decrypt the assumption must solve a difficult bilinear problem. Such an attack method would be very unlikely to succeed in this study, especially because it must solve the problem within a limited time (ΔT) so that it is not denied access by the server. Therefore, it would be impossible to use the connection- and password- guessing attack method to gain access to this system.

4.3 Replay attacks

This attack method intercepts the message mid-communication, tampers with it, and resends it to the destination. In this study, gaining authentication with this attack method would be almost impossible. The system verifies whether the time interval ΔT is within a reasonable delay after receiving the login request. If the judgment is not valid, the uid will be directly identified as illegitimate; thus, access to the login system will be denied. Intercepting messages and resending the login request would take too long; therefore, the attacker would not conform with the time difference verification, meaning that this attack technique would fail in this system developed in this study.

4.4 Legitimate user forgery attack

Forging a legitimate user is a typical attack and common method. After the attacker intercepts the request message, a forged user may use the current timestamp to calculate $H_2(T_i)$ and use the message to disguise their request as one from a legitimate user and log in to the system to access data. However, the forged user lacks the upw of the legitimate user and the parameter R_i that the CA has stored in

the smart card, making it impossible for an attacker to log in to the system. It is very difficult to determine the user password from the interception of a login request or from a smart card. Therefore, it is difficult to forge the registration information of a legitimate user. One must first solve the difficult assumption to decrypt the user's private key D_i ; the alternative is that one could obtain D_i by physically stealing the smart card and using it fraudulently. However, due to the multiple authentication parameters, forgery attacks are not a threat to the security system presented in this study.

4.5 Performance evaluation

In the proposed study, it is assumed that the user's mobile device is equipped with sufficient computing resources to support this operation. In the registration stage, the user only needs to register with the CA once to obtain a smart card. There is no computational cost involved at this stage. In the login and verification stages, if the amount of computation of the user and the CA can be saved, the user can quickly obtain the information he wants within the limited time (Figs. 1 and 2). Thus, our goal is to reduce the computational cost to optimize this method in the PHR system in the cloud environment (Table 1). In the performance evaluation, the proposed authentication method was compared with other three methods [16–18] in terms of computational cost, as the Table 2. The computation cost of a bilinear pairing is more time-consuming than other operations. In [19], the results of T_{e_mul} and T_{e_add} were smaller than T_e . In Table 2, we express a comparison

between our authentication scheme with some others. Although our method needs more computational resources during the key construction phase, the differences in computation power needed for T_{e_add} and T_h are trivial. In the computation cost for the user, our scheme only needed $T_{e_mul} + T_h$. This is better than [16] and [17]; however, it extracts greater T_{e_mul} than [18]. In the computation cost for the CA, our computation cost is less than others. In summary, the performance of our scheme is better than others and more suitable for PHRs in the cloud computing environment.

Storing PHR in a cloud computing environment cannot completely eliminate threats from the cloud nor can it ensure that PHR service providers are safe and trustworthy. Therefore, it is necessary to construct a comprehensive security framework to protect the privacy of users to gain their trust leading to the upgrade of healthcare service quality and the protection of patients' privacy. In particular, PHR emphasizes the confidentiality, availability, and access authentication of personal privacy protection. Therefore, how to protect user information security and privacy, how to prevent malicious attacks on the Internet, and how to provide security authentication between devices during the process of user data transmission have become important issues. Through security analysis, it is verified that the mechanism proposed in this study can resist prevalent security attacks. It uses smart card to store authentication information, designs a bilinear pairing password system for identity authentication, ensures that the password used to log in to the remote care system is

Fig. 1 PHR system architecture under cloud computing environment

Fig. 2 Application scenario of the example **Table 1** Notation definitions table

Notation	Definition
uid	The user's Identity
upw	The user's password
G_1	a group an elliptic curve E over F_p
G_2	a multiplicative subgroup of F_p^*
H_1	One way hash function: $\{0, 1\}^* \rightarrow G_1$
H_2	One way hash function: $G_2 \rightarrow \{0, 1\}^*$

safe and reliable, and will not be maliciously stolen while resisting security.

5 Conclusions

Personal health record systems built using cloud computing require comprehensive identity security mechanisms to protect users' privacy records to ensure sufficient trust from the user and still use PHRs to improve the quality of personal health and future health planning. In cloud computing environments, effective identity authentication technology can protect the security and privacy of users' private data during the user's access to data; therefore, the identity authentication mechanism was a key factor in the application of the PHR systems in this study. A secure and

legitimate authentication system can ensure that only users who have passed identity verification can log into the system and access the resources. Therefore, based on a PHR system built on sensor networks and cloud computing, this study has proposed an identity authentication mechanism based on bilinear pairing. When users record their daily health and physiological conditions at home, medical records in hospitals, medication prescription records, etc., the information can be documented continuously as a long-term record on the system and store it in backend servers. In the future, users and their family members or healthcare service providers from medical institutions can view these health records in the cloud environment. Observing long-term changes in patients' physiological conditions can improve healthcare diagnoses, prognoses, and treatments, possibly preventing avoidable deteriorations or unnecessary therapy. These records can be used in future clinical visits, allowing doctors, nurses, and other medical personnel in different institutions understand the physical condition of the patients more quickly and provide appropriate medical services. The PHR system combined with complete identity authentication not only allows medical service providers to more quickly confirm the health status of users, but more importantly, it can protect users' private personal and sensitive information. In this study, a smart card was used to store information and parameters that needed to be verified, and an authentication scheme based on bilinear pairing was used to verify the

Table 2 Computation comparison

Protocol	Key construction	Computation cost for the user	Computation cost for the CA
[16]	$T_e + 2T_{e_mul}$	$T_e + T_{e_mul}$	$2T_e + 2T_{e_mul}$
[17]	$T_e + 2T_{e_mul}$	$T_e + T_{e_mul} + 2T_{e_add} + T_h$	$T_e + 3T_{e_mul} + 2T_{e_add} + T_h$
[18]	$T_e + 2T_{e_mul} + T_h$	$2T_h$	$2T_e + 2T_{e_mul} + T_{e_add} + 3T_h$
Our scheme	$T_e + T_{e_mul} + T_{e_add} + T_h$	$T_{e_mul} + T_h$	$2T_e + T_{e_mul}$

T_e The computation cost of a bilinear pairing operation $\hat{e}$

T_{e_mul} The computation cost of a multiplication operation in the bilinear pairing

T_{e_add} The computation cost of an addition operation in the bilinear pairing

T_h The computation cost of one-way hash function operation

legitimacy of the user. A complete identity verification phase would enable hospital staff to protect the privacy and security of patients while accessing patient information. The user password used to log in to the personal healthcare system must be secure, reliable and resilient to malicious attacks, and therefore guarantee the security of the whole system.

Declarations

Conflict of interest The author declared that there is no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Miller, R. H., & Sim, I. (2004). Physician's use of electronic medical records: Barriers and solutions. *Health affairs*, 32(2), 116–126.
2. Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., & Sands, D. Z. (2006). Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption. *Journal of American Medical Informatics Association*, 13(2), 121–126.
3. US Public Law. (1996). Health Insurance Portability and Accountability Act of 1996, 104th Congress, *Public Law*, 104–191.
4. Yang, C. M., Lin, H. C., Chang, P., & Jian, W. S. (2006). Taiwan's perspective on electronic medical records' security and privacy protection: Lessons learned from HIPAA. *Computer Methods and Programs in Biomedicine*, 82, 277–282.
5. Kaelber, D. C., Jha, A. K., Johnston, D., Middleton, B., & Bates, D. W. (2008). A research agenda for personal health records (PHRs). *Journal of the American Medical Informatics Association*, 15(6), 729–736.
6. Joux, A. (2002). The weil and tate pairings as building blocks for public key cryptosystems. *International Algorithmic Number Theory Symposium*, pp. 20–32.
7. AHIMA, J. (2007). The value of personal health records: A joint position statement for consumers of healthcare. *Journal of the American Medical Informatics Association*, 78(4), 22–24.
8. Kim, M. I., & Johnson, K. B. (2002). Personal health records: Evaluation of functionality and utility. *Journal of American Medical Informatics Association*, 9(2), 171–180.
9. Yujin, P., & Hyung-Jin, Y. (2020). Understanding personal health record and facilitating its market. *Healthcare Informatics Research*, 26(3), 248–250.
10. Li, M., Yu, S., Ren, K., & Lou, W. (2010). Securing personal health records in cloud computing: Patient-centric and _ne-grained data access control in multi-owner settings. *Security and Privacy in Communication Networks*. https://doi.org/10.1007/978-3-642-16161-2_6
11. Benaloh, J.C., Chase, M.P., Horvitz, E.J., Lauter, K.E. (2009). Patient controlled encryption: Ensuring privacy of electronic medical records. *CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security*, 103–114.
12. Liu, C. H., & Chung, Y. F. (2017). Secure user authentication scheme for wireless healthcare sensor networks. *Computers & Electrical Engineering*, 59, 250–261.
13. Shamir, A. (1985). Identity-based cryptosystems and signature schemes. *Advances in Cryptology-Proceedings of CRYPTO'84*, Springer-Verlag LNCS 196.
14. Boneh, D., & Franklin, M. (2001). Identity-based cryptosystems and signature schemes. *Advances in Cryptology-Proceedings of Crypto*, 2139, 213–229.
15. Fan, C. I., Sun, W. Z., & Huang, V. S. (2010). Provably secure randomized blind signature scheme based on bilinear pairing. *Computers & Mathematics with Applications*, 60(2), 285–293.
16. Chen, L., Cheng, Z., & Smart, N. P. (2007). Identity-based key agreement protocols from pairings. *International Journal of Information Security*, 6, 213–241.
17. Wang, S., Zhenfu, C., & Feng, C. (2008). Efficient identity-based authenticated key agreement protocol with pkg forward secrecy. *International Journal of Information Security*, 7(2), 181–186.
18. Wu, S. Y., & Tseng, Y. M. (2010). An ID-based mutual authentication and key exchange protocol for low-power mobile devices. *The Computer Journal*, 53(7), 1062–1070.
19. Chan, C., Duan, P., Cui, S. (2006). An efficient identity-based signature scheme with batch verifications. *InfoScale '06: Proceedings of the 1st international conference on Scalable information systems*, 22–28

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Chia-Hui Liu received her Ph.D. in electrical engineering from National Taiwan University in 2011. She is an Associate Professor at the Department of Applied Mathematics, Chinese Culture University, Taiwan. Her research interests include big data, machine learning, wireless sensor network, information security, and medical information (ljh34@ulive.pccu.edu.tw).

Tzer-Long Chen received his B.S. Computer Science and Information Engineering, Tam Kang University, Taiwan, in 2004. M.S. Department of Communication Engineering, National Chung Cheng University, Taiwan, in 2006. Ph.D. degrees from the Department of Information Management, National Taiwan University, Taiwan, in 2012. From 2013 to 2019, he was an assistant professor at Ling Tung University, Taiwan. Since 2019, he has

been an assistant professor at Providence University. His research interests are in Information Security, Internet of Things, and Block Chain (tlchen1976@pu.edu.com).

Zhen-Yu Wu received the Ph.D. degree in Computer Science from National Taiwan University in 2011. He is currently an Associate Professor with the Department of Information Management at National Penghu University of Science and Technology, Taiwan. His current interests focus on information security, cryptography, Internet of Things, and medical information (zywu@gms.npu.edu.tw).

Chien-Yun Chang received his B.S. National Kaohsiung University of Science and Technology, Taiwan, in 2001 and his M.S. and Ph.D. degrees from the National Kaohsiung University of Science and Technology, Taiwan, in 2003 and 2008 respectively. From 2005 to 2009, he was an assistant professor at Hsiuping University, Taiwan. Since 2018, he has been an associated professor at Ling Tung University. His research interests are in

Finance, Marketing, Information Application and research method (yunj@teamail.ltu.edu.tw).