International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 11, Issue 3 [May.-June. 2022] PP: 365-370

Improved Personal Secure Authentication Approach for Personal Health Records in Distributing Sharing System

CH. BALAKRISHNA[1], K. PREMA TEJA[2], V. SHIVA[3],
N. SIVANI[4], V. ANVITHA LAYA[5]

[1]*Assistant Professor, Dept. of CSE, Sai Spurthi Institute of Technology,Khammam,Telangana,India*
[2,3,4,5,6]*B.Tech Student, Dept. of CSE, Sai Spurthi Institute of Technology, Khammam,Telangana,India*

ABSTRACT:

The quick improvement of the Internet of Things (IoT) has prompted the rise of an ever increasing number of novel applications lately. One of them is the e-wellbeing framework, which can furnish individuals with top caliber and advantageous wellbeing care. In the interim, it is a central point of contention and challenge to secure the protection and security of the client's very own wellbeing record. A few cryptographic strategies have been proposed, for example, encode client's information prior to sharing it. In any case, it is convoluted to share the information with numerous gatherings (specialists, wellbeing divisions, and so forth), because of the way that information ought to be scrambled under each beneficiary's keys. Albeit a few (t, n) limit secret sharing plans can share the information just need one encryption activity, there is a limit that the decoding private key needs to be recreated by one party. To balance this weakness, in this paper, we propose an effective character based conveyed unscrambling plan for individual wellbeing record sharing framework. It is helpful to impart their information to various gatherings and doesn't need to reproduce the decoding private key. We demonstrate that our plan is secure under picked ciphertext assault (CCA). Besides, we execute our plan by utilizing the Java matching based cryptography (JPBC) library on a PC and an Android telephone. The trial results show that our framework is viable in the electronic individual wellbeing record framework.

Index Terms: Distributed decryption, identity-based encryption, security, privacy, e-health system.

Date of Submission: 02-06-2022 Date of Acceptance: 15-06-2022

---

1. INTRODUCTION

As the worldwide populace is maturing and individuals with constant infections are expanding, essential medical services might become inaccessible to many individuals. Because of the Internet of Things (IoT) strategy, it advances the fast improvement of ehealth frameworks and makes medical care more straightforward for clients who utilize compact gadgets. E-wellbeing is characterized as an interdiscipline which comprises of general wellbeing, clinical informatics and business. It can offer or upgrade medical services through the Internet utilizing implies like WiFi and 5G organizations. E-wellbeing frameworks bring clients a ton of advantages. They can save lives in crisis clinical circumstances, through the realtime checking of the associated gadgets; it is not difficult to distinguish the crisis circumstances, for example, asthma assaults, cardiovascular breakdown and diabetes. As the clinical information and wellbeing information are gathered by the associated gadgets. Then, at that point, the information is moved to the specialist or the medical services office by remote organization gadgets, like cell phones and tablets. Truth be told, these information are essential for individual wellbeing records (PHRs).

PHR incorporates wellbeing information, yet additionally some significant data connected with patient consideration. This information is overseen by the patient and normally put away in the cloud server (clinical servers). Not at all like the electronic clinical record, the PHR is not made and kept up with by foundations (like clinical foundations and medical clinics). The information assortment and transferring are finished by the patient. The motivation behind PHRs is to store a precise and complete outline of the singular's clinical history. They permit approved clients or establishments to get to the information over the Internet.

A new study shows that a larger part of clients use applications and different apparatuses to follow their wellness, sustenance and rest; 44% of individuals have gotten to their clinical records on the web. Like in a regular e-wellbeing individual wellbeing records (PHRs) engineering, the client's information are gathered and shipped off the clinical servers. At the point when the specialist needs to audit the client's PHRs (clinical

information, clinical record, and so forth), he wants to download the PHRs from the clinical server. By and by, the gigantic PHRs information are generally put away and handled in the cloud stage, like Amazon Web Services, Google Cloud. Because of the PHRs contains some delicate and high-esteem information; the cloud server has turned into an alluring objective for hacking.

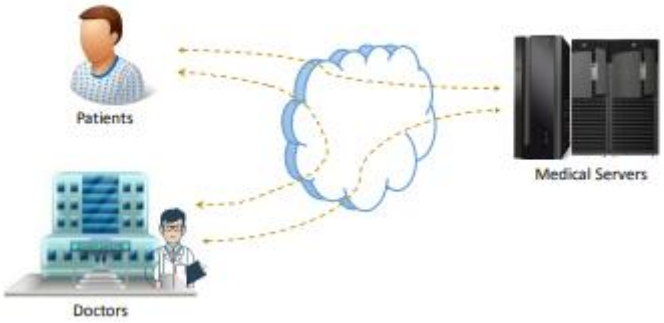

Fig. 1. A typical e-health PHR architecture

• RQ1: Can clients utilize a lightweight plan to keep the PHRs information secure?

Various cryptographic plans are secure for the clients to imparting their information to the specialists or on the other hand medical services offices. In any case, a significant number of them are confounded for the clients to utilize, for instance, in the conventional PKI design, the clients ought to acquire and confirm each authentication. Besides, in the event that the CA is assaulted or debased, both the declaration gave by the CA furthermore the CA root testament are not trusted.

• RQ2: if there should arise an occurrence of imparting the PHRs to different gatherings, can the gatherings unscramble the encoded PHRs without remaking the private key?

The (t, n) limit secret sharing plan can assist the clients with imparting the PHRs to numerous gatherings advantageously. The PHRs information as it were should be scrambled once. Be that as it may, the reproduced private key is generally a twofold document put away on a versatile medium, (for example, IC card or on the other hand USB gadget) or an electronic gadget, (for example, a cell phone or a PC). The private key is defenseless assuming a noxious application is introduced on the gadget.

2. RELATED WORK

A. Secure Storage of Personal Health Records

The individual wellbeing records (PHRs) are very touchy with crucial information which connects with client's protection. A few plans have been suggested that permit the patient to control the encryption of the PHRs information. For instance in Indivo, the patients can gather, keep up with and control a solid copy of their PHRs. In any case, to empower access control, a portion of these plans depend on a confided in outsider. In the writing, Hu et al. proposed a half and half open key framework (HPKI) plot. It permits the clinical benefit supplier to deal with the PHRs safely.

B. Identity-Based Encryption

In the conventional PKI system, it is convoluted to deal with the huge public keys. The character based cryptography (IBC) offers a clever decision. One of the most alluring properties is that the public key of an element is its personality. Also, in the IBC frameworks, the endorsements are no more required. By and large, the public key can be processed from its character string by a predefined calculation (like a hash work) for certain contributions of public boundaries.

Boneh and Franklin presented the principal personality based encryption conspire from pairings. In their plan, a trusted party named Key Generation Center (KGC) is involved, which can extricate client's private key by utilizing its lord secret key also the personality of the client. Moreover, the public key is a hash worth of the character, and can be utilized to scramble the messages. Following Boneh's idea, various IBE plans have been proposed.

3. SECURITY ANALYSIS

A. Security Model

Definition 5. *Let $\mathcal{A}$ be a P.P.T adversary, $\mathcal{C}$ be a challenger. If an identity-based encryption scheme is semantically secure against an adaptive chosen ciphertext attack, then a P.P.T algorithm $\mathcal{A}$ has a negligible advantage against $\mathcal{C}$ in the games described as follows:*

- *Setup (1^λ): On input the security parameter λ, $\mathcal{C}$ executes the Setup process to obtain the public parameters params and the master secrete key. Then, it sends params to $\mathcal{A}$ and saves the master secret key.*
- *Phase 1: The adversary $\mathcal{A}$ can make q_m times queries, the q_i $(1 \leq i \leq m)$ query can be either extraction query or decryption query. The queries are described as follows:*
  - *Extraction query (id_i). On input id_i, the challenger $\mathcal{C}$ executes Extract process, and outputs the corresponding private key D_i, then returns D_i to $\mathcal{A}$.*
  - *Decryption query (id_i, C_i). First, on input id_i, the challenger $\mathcal{C}$ executes Extract algorithm and gets the private key D_i. Next, $\mathcal{C}$ executes the Decrypt process by inputting the private key D_i and the ciphertext C_i, then the challenger $\mathcal{C}$ obtains the plaintext and sends it to $\mathcal{A}$.*
- *Challenge: After the adversary $\mathcal{A}$ terminates the Phase 1, it generates a challenge identity ID and challenge plaintexts (M_0, M_1). Note that, the identity ID have never been queried in any private key extraction in Phase 1.*
  The challenger $\mathcal{C}$ selects $b \xleftarrow{r} \{0, 1\}$ randomly, and computes the M_b's ciphertext C by runnning the algorithm Encrypt(params, ID, M_b), then the challenger responds $\mathcal{A}$ with the ciphertext C.
- *Phase 2: This phase allows the adversary $\mathcal{A}$ to make another q_n times queries. The i-th query q_i can be either extraction query or decryption query. The queries are described as follows:*
  - *Extraction query. It is same as in Phase 1, except that $id_i = ID$.*
  - *Decryption query (id_i, C_i). It is same as in Phase 1, except that $(id_i, C_i) = (ID, C)$.*
- *Guess: The adversary $\mathcal{A}$ outputs the value b' where $b' \in \{0, 1\}$. $\mathcal{A}$ wins the game if $b' = b$.*

B. Proof of Security

Theorem 1. *Assume that BF-IBE scheme is semantically secure under adaptive choosen ciphertext attack. Then our proposed distributed key generation protocol and distributed decryption protocol constitute a secure multiple-party identity-based decryption scheme of BF-IBE.*

Proof. In $DistEncrypt^b_{\mathcal{A},E}(1^\lambda)$, $\mathcal{A}$ is a P.P.T IND-ID-CCA adversary. Then, we build a P.P.T adversary $\mathcal{S}$ for $Encrypt_{\mathcal{A},e}(1^\lambda)$. The adversary $\mathcal{S}$ can utilize $\mathcal{A}$ to obtain the advantage $\epsilon/e(1 + q_E + q_D)$ to break BF-IBE scheme. Following Boneh's notion [12], first, the challenger generates a random public key such that $K_{pub} = (q, \mathbb{G}, \mathbb{G}_T, e, n, P, P_{pub}, id, Q_{id}, H_2, H_3, H_4)$, and the private key $D_{id} = sQ_{id}$. Then it sends K_{pub} to the adversary $\mathcal{S}$. $\mathcal{S}$ uses the help of algorithm $\mathcal{A}$ to mount an IND-ID-CCA attack on the public key K_{pub}.

- **Setup.** $\mathcal{S}$ first sends the system parameters $(q, \mathbb{G}, \mathbb{G}_T, e, n, P, P_{pub}, id, H_2, H_3, H_4)$ to the adversary $\mathcal{A}$. We let H_1 be a random oracle which is managed by $\mathcal{S}$ and described as below.
- **H_1-queries.** The algorithm $\mathcal{S}$ controls a list that (id_j, Q_j, b_j, c_j), we define this list as H_1^{list}, and initial it as an empty list. $\mathcal{A}$ can do multiple queries to the oracle H_1. When the adversary $\mathcal{A}$ sends the query identity id_i to the oracle H_1 , algorithm $\mathcal{S}$ works as follows to respond to the query:

1) If there is a matched tuple (id_i, Q_i, b_i, c_i) on the list H_1^{list}, then the algorithm $\mathcal{S}$ returns $Q_i \leftarrow H_1(id_i)$ to $\mathcal{A}$.
2) Otherwise, $\mathcal{S}$ randomly selects a $coin \xleftarrow{r} \{0,1\}$ and the $\Pr[coin = 0] = \delta$.
3) Algorithm $\mathcal{S}$ selects $b \xleftarrow{r} \mathbb{Z}_q^*$ randomly. If $coin = 0$, $\mathcal{S}$ computes $Q_i = bP$. If $coin = 1$, $\mathcal{S}$ computes $Q_i = bQ_{id}$.
4) Algorithm $\mathcal{S}$ sets a tuple $(id_i, Q_i, b_i, coin)$ and adds it to the hast list H_1^{list}, then returns $Q_i \leftarrow H_1(id_i)$ to $\mathcal{A}$.

Note that, in $\mathcal{A}$'s view, Q_i is uniform in $\mathbb{G}$ and is independent.

- **Phase 1.** This phase allows the adversary to make both private key extraction query and decryption query.
  1) **Private key queries.** Assume the adversary $\mathcal{A}$ queries id_i in this query. Algorithm $\mathcal{S}$ works as follows to respond the query:
     a) $\mathcal{S}$ executes the algorithm $Q_i \leftarrow H_1(id_i)$ to obtain the private key and responds it to H_1-queries, sets $(id_i, Q_i, b_i, coin_i)$ as the corresponding tuple on H_1^{list}. If $coin_i = 1$, $\mathcal{S}$ returns $\perp$ and terminates.
     b) If $coin_i = 0$, $Q_i = b_iP$. We define that $d_i = b_iP_{pub}$, i.e., $d_i = sQ_i$. Hence, d_i is the private key associated with the identity id_i. Finally, $\mathcal{S}$ returns d_i to $\mathcal{A}$.

  2) **Decryption queries.** Assume the adversary $\mathcal{A}$ queries (id_i, C_i) in this query. Let $C_i = (U_i, V_i, W_i)$, $\mathcal{S}$ works as follows to respond the query:
     a) $\mathcal{S}$ executes the algorithm $Q_i \leftarrow H_1(id_i)$ to obtain the private key and respond $\mathcal{A}$'s H_1-queries. Then sets the tuple $(id_i, Q_i, b_i, coin_i)$ as the matched tuple on the hast list H_1^{list}.
     b) If $coin_i = 0$, $\mathcal{S}$ executes the algorithm on input the query identity id_i to get the private key. Then $\mathcal{S}$ returns the decryption query by using the private key.
     c) If $coin_i = 1$, then we have $Q_i = b_iQ_{id}$.
        - $\mathcal{S}$ sets $C_i' = (b_iU_i, V_i, W_i)$. Lets $d_i = sQ_i$ which is the corresponding private key of the identity id_i. To decrypt C_i by the private key d_i, it is same as to decrypt C_i' by using d_{id} in BF-IBE.
        - Returns the decryption query C_i' to the challenger, then sends the challenger's response to $\mathcal{A}$.

- **Challenge.** If the adversary $\mathcal{A}$ determines that the Phase 1 is finished, it will output a challenge identity id_{ch} and challenge messages (M_0, M_1). Algorithm $\mathcal{S}$ works as follows:
  1) The algorithm $\mathcal{S}$ sends the messages M_0 and M_1 to the challenger $\mathcal{C}$, then $\mathcal{C}$ returns a BF-IBE ciphertext such that $C = (U, V, W)$, which is a ciphertext of M_c, and c is randomly selected from $\{0,1\}$.

2) $\mathcal{S}$ executes the algorithm to respond $Q \leftarrow H_1(id_{ch})$ for the H_1-queries. Assume there exists a tuple $(id_{ch}, Q, b, coin)$ in the list H_1^{list} that corresponds to id_{ch}. If $coin = 0$, $\mathcal{S}$ returns $\perp$ and terminates.
3) If $coin = 1$, then $Q = bQ_{id}$. The algorithm $\mathcal{S}$ sets $C' = (b^{-1}U, V, W)$, then sends C' to $\mathcal{A}$.

- **Phase 2.** The queries on this phase are the same as in Phase 1. However, the adversary $\mathcal{A}$ cannot query the challenge ciphertext. If $\mathcal{A}$ queries the challenge ciphertext, $\mathcal{S}$ returns $\perp$ and terminates.
- **Guess.** Finally, the algorithm $\mathcal{A}$ outputs a guess c'. Algorithm $\mathcal{S}$ outputs c' as the guess for c.

Claim. In the simulation stage, if the algorithm $\mathcal{S}$ does not abort, and the view of adversary $\mathcal{A}$ is identical between the simulation and the real attack. Then we have $|\Pr[c = c'] - 1/2| \geq \epsilon$.

Proof of claim. The response of H_1-queries is uniform and independent distributed in $\mathbb{G}$. It is same as the real attack. For all the queries, the responses are true. Additionally, the ciphertext C' to be challenged is a BF-IBE ciphertext of M_c where c is randomly selected from $\{0, 1\}$. Thus, on the basis of the definition, we have $|\Pr[c = c'] - 1/2| \geq \epsilon$. □

4. PERFORMANCE AND EXPERIMENTAL RESULTS

We execute our proposed numerous unscrambling plan utilizing JPBC library. The trial assessment and results are displayed in this part. Also, we give the running time examination between our plan and the first BFIBE plot. The tests were carried out on a ThinkPad PC (with an Intel Core i5-520M double center processor, 4GB memory and Microsoft Windows 10 working framework) and an Android telephone (Google Nexus 6P with a Qualcomm Snapdragon 810 quad-center processor, 3GB Slam and Android Oreo 8.1.0 working framework). We pick the sort A bend (K = 12, rBits = 160) to execute the explore. We first show the time-utilization consequences of every calculation in the BF-IBE plot.

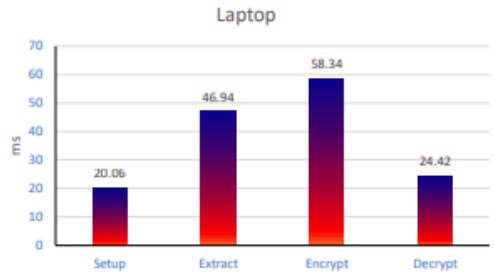

Fig. 3. Running time of Each Progress on Laptop

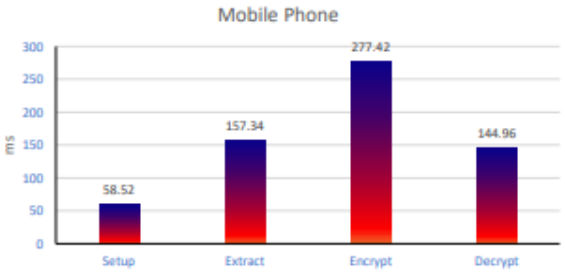

Fig. 4. Running time of Each Progress on Android Phone

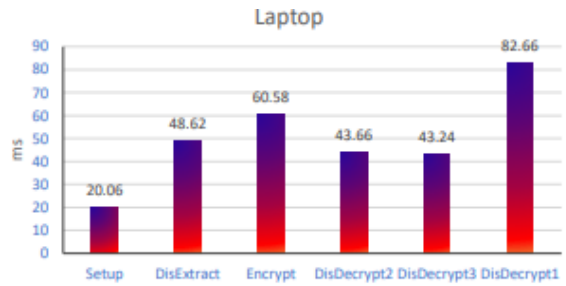

Fig. 5. Running time of Each Progress on Laptop

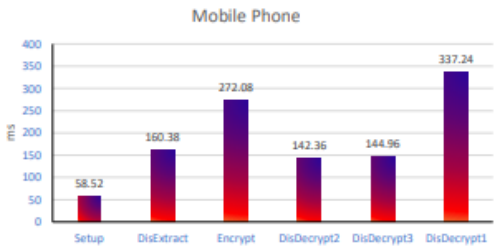

Fig. 8. Running time of Each Progress on Android Phone

Scheme \ Step	Setup	Extract	Encrypt	Decrypt
BF-IBE	20.06ms	46.94ms	58.34ms	24.42ms
Our Scheme	20.06ms	48.62ms	60.58ms	169.56ms

TABLE III TIME CONSUMPTION COMPARISON ON LAPTOP

Scheme \ Step	Setup	Extract	Encrypt	Decrypt
BF-IBE	58.52ms	157.34ms	277.42ms	144.96ms
Our Scheme	58.52ms	160.38ms	272.08ms	624.56ms

TABLE IV TIME CONSUMPTION COMPARISON ON ANDROID PHONE.

5. CONCLUSION

Electronic Personal Health Record Sharing Systems are being broadly utilized. Security and protection issues are becoming basic in such frameworks and conditions. Getting delicate information of clients, like prescriptions, constant medical issues, inoculation history and the private keys in these conditions is critical and testing. We utilized the Boneh Franklin character based encryption plan to plan a proficient and secure e-wellbeing individual wellbeing record sharing framework in this paper. In our proposed plot, patient can scramble the PHRs under the character of a specialist or an office. The ciphertext can be unscrambled safely by numerous gatherings, (for example, various gadgets of a specialist, or the specialists in an equivalent office). In particular, our plan is lightweight for the cell phones, and it permits the gatherings to unscramble the ciphertext without remaking the private key. The security examination exhibited that our plot accomplishes the CCA2 security. As per the trial results, our proposed conspire is pragmatic in genuine world individual wellbeing recording sharing framework. Later on, we will concentrate on some more effective methodologies, for example, disposal of the zero-information verification in the plan, furthermore appropriation of the mystery without utilizing a mysterious channel.

6. REFERENCES

[1]. G. Eysenbach, "What is e-health?" Journal of medical Internet research, vol. 3, no. 2, p. e20, 2001.
[2]. M. Obaidat and N. Boudriga, Security of E-systems and Computer Networks. Cambridge University Press, 2007
[3]. R. Pifer, "Patient use of digital health tools lags behind hype, poll finds," https://www.healthcaredive.com/news/patient-use-of-digitalhealth-tools-lags-behind-hype-poll-finds/562778/, accessed Sept 12, 2019.
[4]. J. L. Fernandez-Alem ´ an, I. C. Se ´ nor, P. ˜ A. O. Lozoya, and A. Toval, ´ "Security and privacy in electronic health records: A systematic literature review," Journal of biomedical informatics, vol. 46, no. 3, pp. 541–562, 2013.
[5]. H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation," International Journal of Information Security, vol. 14, no. 6, pp. 487– 497, 2015.
[6]. M. S. Obaidat, I. Traore, and I. Woungang, Biometric-Based Physical and Cybersecurity Systems. Springer, 2019, vol. 368.
[7]. M. Focus, "Voltage securemail on-premises on-premises email encryption," https://www.microfocus.com/en-us/products/emailencryption-security/
[8]. X. Boyen and L. Martin, "Identity-based cryptography standard (ibcs)# 1: Supersingular curve implementations of the bf and bb1 cryptosystems," RFC 5091, December, Tech. Rep., 2007.
[9]. K. D. Mandl, W. W. Simons, W. C. Crawford, and J. M. Abbett, "Indivo: a personally controlled health record for health information exchange and communication," BMC medical informatics and decision making, vol. 7, no. 1, p. 25, 2007
[10]. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009, pp. 103–114
[11]. J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson, and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices. ACM, 2011, pp. 75–86.
[12]. Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving fusion of iot and big data for e-health," Future Generation Computer Systems, vol. 86, pp. 1437–1455, 2018.
[13]. D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," in Advances in Cryptology – CRYPTO 2004, ser. Lecture Notes in Computer Science, M. Franklin, Ed., vol. 3152. Springer, Heidelberg, Aug. 2004, pp. 443–459.
[14]. B. R. Waters, "Efficient identity-based encryption without random oracles," in Advances in Cryptology – EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed., vol. 3494. Springer, Heidelberg, May 2005, pp. 114–127.
[15]. D. Boneh, C. Gentry, and M. Hamburg, "Space-efficient identity based encryption without pairings," in 48th Annual Symposium on Foundations of Computer Science. IEEE Computer Society Press, Oct. 2007, pp. 647–657.
[16]. S. Agrawal and X. Boyen, "Identity-based encryption from lattices in the standard model," Manuscript, July, 2009.
[17]. B. Waters, "Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions," in Advances in Cryptology – CRYPTO 2009, ser. Lecture Notes in Computer Science, S. Halevi, Ed., vol. 5677. Springer, Heidelberg, Aug. 2009, pp. 619–636.
[18]. L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, "A type-and-identitybased proxy re-encryption scheme and its application in healthcare," in Workshop on Secure Data Management. Springer, 2008, pp. 185–198.