International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Volume 8 Issue 2, February-2019, Impact Factor: 3.578

A Fortified Identity Based Encryption (FIBE) For E-Health Management System in Cloud

Anand R Mehta

ABSTRACT

Electronic health record maintenance is an evolving problem that we need to handle efficient information interchange. This system supports the patients to create their health relevant information, accomplish, govern and share certain information with hospital, Experts and others. Generally, the third party cloud service providers controls the EHR services which entails more interrelated operations. Here the challenge arises in the context of privacy preservation regarding patient's medical information. The patient needs to share their information with various organizations and the data is nominated for various query operations. Here we need to face many issues regarding the security of the personal medical data. Access Credentials, Secure Interaction, Authentication Policy Behavior and Verification of Security Attributes. In order to deal such problems a novel high secure e-health management framework is proposed. This framework handles Access policy control, Fortified Identity based encryption (FIBE) and user specific proxy re-encryption methods for secure EHR distribution. We additionally demonstrate these system's security and offer the Performance analysis. The result shows that our Novel High Secure E-Health Management Framework is predominantly great efficiency on behalf of re-encryption, which can be used to attain profitable cloud usage. Our comprehensive approach enhances the security, privacy and interoperability functions of EHR services.

Index Terms—Electronic health record, Interoperability, key management, Encryption, Access Control Policy

INTRODUCTION

Cloud computing techniques has created a huge impact in the medical field and it is effectively used for maintaining patient records for providing the medical assistances to the patient over internet. These patient records which are named as electronic health records can be either controlled by the patients (Patient centric) or by the hospital management admins. Though these information are shared to the cloud environment, those data has to be provided with the high level of security. These data is be highly sensitive due to the presence of the health reports and personal information of the user, on loss may lead to critical issues. The electronic health care system has superior benefits that include greater opportuneness and advance access to medical data. The result of thise-health management deployment significantly reduce treatment delays, very small level of medical errors, cost effective system, fraud detection mechanism where, shorter refund delays for patients covered by health insurance schemes.

A. Problem Identification

Although there are many benefits, [1]still there is a fear for people only because of privacy preservation. The hospital suffers to give assurance for safe handling of patient data and upholding privacy. When we deploy this e-health management in cloud based storage system, it seems more vulnerable because of third party involvement. Even though e-health management has additional security feature such as password protecting and audit tracking, there is a possible of huge inside and outside attacks when EHR exist in the cloud server. Henceforth, there is a necessity for proper strategies and measure for handling people data confidentially keeping both security and confidentiality in mind. Lot of Previous researches efforts to provide a secure storage environment for the electronic health records. E-health cloud systems with various specifications and security constraints have been proposed so far, which are effective in providing e -health data security. Though these security models are effective, many use public key infrastructure which makes the user's to find it hard to recall the public and private keys which are desired for encryption and decryption of the data.Several encryption and decryption algorithm were implemented with the algorithms like [2]identity based encryption, [3]Attribute based encryption,[4]Advanced Encryption Standard (AES), [5]Blowfish, [6]Data Encryption Standard (DES), [7]RC5, and [8]3DES are developed conventionally to ensure security in the cloud. [9]The limitations that were observed from these

mechanisms include inefficient revocation, unsigncryption outsourcing, data loss, Key management and lack of user authentication. Besides, the existing works followed basic secret generation and key generation procedures, which lead to minimal data security and increased computational complexity.

B. Objectives

It is essential to employ better Electronic health record maintenance mechanism which preserves three catalogs such as data availability, data integrity and data privacy. EHR services should be robust against attackers and maintain consistency in the circumstance of organization interoperability. Hence, these issues are taken into account for this work to develop an efficient EHR storage and retrieval mechanism in the cloud. Here, we introduce a Novel High Secure E-Health Management Framework based on secure encryption processes and interoperability. The major contributions of this paper are as follows:

- A novel Identity based Data Encryption Algorithm (FIBE) is proposed centered on Patient personal information or recognized identities. These information is considered as the key parameters for the generation of the key.
- Strict Policy Control Based Data Access model is proposed to verify the authentication of the user using access control Structures which are designed by the Attribute Authority
- A User Specific Proxy Re-encryption Algorithm is proposed to support the third party access and to provide secure access for the EHR.

C. Organization

The rest of the sections of this paper are organized as follows: The key generation and encryption mechanisms used for cloud data storage and security are discussed with its advantages and disadvantages in Section II. We present the system architecture and the proposed FIBE security model in Section III. The experimental results of both existing and proposed security mechanisms are analyzed and compared in Section IV. The overall summary and future enhancement of this paper are stated in Section V.

II. RELATED WORK

In this section, the security issues related to the EHR access control in the cloud and the methodologies that are used to provide a better solution for EHR data security are surveyed with its advantages and disadvantages. Commonly this could be ordered into two categories affording to their different access control mechanisms.

A. EHR system centered on Authentication

This type of EHR security schemes works based on the authentication related to the attributes. This type of controlled framework enforce the rights of the user and has complete trust on the aforementioned cloud server. Ghazvini and Shukur [10] Analyzed the various issues and key factors regarding different nations EHR data. It evaluated various approaches and concluded that cryptography methods and password enhancement is the only solution for the security of EHR data. Zhou, et al. [11]Offered a new authentication scheme AAPM. The user provides authorization using an authentication tree which need to satisfy the threshold predicates. Then identity based signature verifying concept identifies the direct and indirect authorizer. The unauthorized user cannot satisfy the constraints. Hamad and Abudalal [12] Suggested multi factor authentication scheme that used both identity related information like username, password and bio-metrics password system. Elgamal Elliptic Curve Cryptosystem is used for secure data transfer. It provided high security but it required a safe prime number that makes generation of large-enough keys super-longi.e the data encrypted with it is twice the size of the same data encrypted with RSA. ElGamal is slow and uncanny. Jaganathan and Veerappan [13]a new DASS model is suggested named as CIADS that delivers security for EHR data. The credentials are offered to the user authentication.

The certificates ensures the authorization which was given by certificate authority. The cryptography method supports the data confidentiality. Modified hash algorithm is responsible for the data integrity checking.Tong, et al.[14] Introduced the concept of auditing the access authorities along with attribute based authentication technique. The concept of threshold signing procedure identifies the proper authorization. This method promise its guarantee only with the secured private cloud. Gao and Iwane [15] mutual rating based multi-trust model is proposed using public key encryption, access control and pseudonymous authentication. The patients could control the exposed attributes in common. So that it makes a room for linkage attacks. Hong, et al. [16] utilized the Time and Attribute Factors Combined (TAFC) access control mechanism for providing security to the time-sensitive data in cloud. Here, the time released encryption mechanism was integrated with the Cipher-text Policy ABE (CP-ABE) technique, which efficiently fulfilled the security requirements of the data. The

major contribution of this paper was to analyze the fine-grained access control mechanism for the time-sensitive data. Further, it aimed to build a scalable and fine-grained access control system for outsourcing the data.

B. EHR system centered on Cryptography

This type of EHR security schemes works based on the cryptography mechanism regarding access control mechanism. Generally the EHR data are encrypted in the client side and the associated decryption key is provided to the authorized user for decryption. Kumar, et al. [17] offered multi-level privacy access control mechanism deploying AAPM for providing privileges to users and patient self-controllable cooperative authentication scheme (PSMPA) that implies load balancing method. The main drawback of this approach is single trusted authority which makes network bottleneck. *Li, et al* [18] leveraged an Attribute Based Encryption (ABE) technique to attain a fine-grained and scalable data access control on Personal Health Record (PHR). The intention behind using this technique was to secure the patient's data or file in an encrypted format. Here, multiple security domains were utilized to reduce the complexity of key management, which was preferable for both the users and owners. Additionally, this scheme enabled a dynamic modification of access policies or file attributes under emergency situations.

The security requirements that were addressed in this work were as follows: data confidentiality, on-demand revocation, write access control, efficiency, and utility. The paper enhanced the key policy generation rule with expressive access policy controls. Yet, this paper mandated the reduction of computational overhead of the system, which affects the overall performance of PHR storage and retrieval process.Wang, et al.[19] Developed improved two-party key issuing protocol which can produce the keys for both provider and user. Attribute based data sharing scheme involved to maintain the state of the data sharing. User's private key has associated attributes and cipher text policy. The authenticated user can decrypt when the attributes meet out the policy of cipher text.Loruenser, et al.[20] Suggested a new architecture ARCHISTAR for data sharing in cloud. It split the data into various segments and applied threshold limit to reconstruct the data. It is impossible for the intruder to fetch enough segmentation for reconstruction.Sun, et al. [21] Authorized keyword search technique for the user revocation of encrypted data in the cloud server. The experimental results shows that the verification seemed to be complete and correct. But there is no security in the cloud server side data.Dong, et al. [22] HIBE scheme for the interoperability of data that needs to merged for the classification.

The medical attributes has dependency which has influence over certain disease predictions. It is proved that the SECO approach is semantically secure in contrast to adaptive chosen cipher text attacks. This approach failed in the basis of data consistency and signature verification. Balasubramaniam and Kavitha [23]Criticize the key management issues and proposed a new Geometric Data Perturbation (GDP) based approach for EHR data transactions. This approach is suffered with outliers attack. Ali, et al. [24] developed a Secured Data Sharing (SeDaSC) mechanism for the cloud, which focused on the objectives of data confidentiality, integrity, access control, and data sharing. The motive of this paper was to secure the cloud data against the forward and backward access controls due to internal threats. In this paper, a single cryptographic key was maintained for each data file, where the key was partitioned into two parts by using various entities. However, it demanded the improvement of the system's performance by identifying the internal threats with varying key size, which was considered a major drawback of this work.

C. Interoperability of EHR system

The designed system should support the interoperability functions for accessing proper EHR services. Interoperability is the primary factor that enhances the functions of EHR systems. There will be always a need to export or import the EHR data for the health care providers. If there is lack of such functions, the total EHR system appears to be sluggish. Thatikayala, et al. [8] have proposed a middle layer approach for interoperability of PHR and EHR models. The ontology assisted approach supports to form various rules for matching the records. It suggested to change the information model which ensures the interoperability. Urbauer, et al. [25]have tested the use of IHE profiles and CHA Design Procedures in the perspective of PHRs. The complete comment on the applicability of IHE and CH Aconditions was affirmative, even though the presently accessible mobile stages may have deficiency in some of the necessary functionalities.

From the survey, the foremost disputes that affects the security of cloud are analyzed, and also the purpose of the aforementioned works are reconnoitered with its own advantages and disadvantages. Typically, the existing mechanisms supposed that the patients EHR data secret was secure, but this wasn't the case then, so it must be improved to increase the security. User identification is the major issue in the point of interoperability. An incorrect identity verification is a threat to the privacy of the user. It can also be very useful to share relevant health data with family members. Taking privacy in consideration, the user needs to have a choice to approve or disapprove regarding the scheme to share exact info. Also, several other research works addressed these issues by presenting well-organized mechanisms based on authentication and

access control policies, but it has increased the overhead and computational complexity. To solve the difficulties that were pointed out on this survey, this paper endeavors to develop A Novel High Secure E-Health Management Framework based oncloud by applying some effectual mechanisms.

III. PROPOSED METHOD

This section presents a clear description of the proposed Novel High Secure E-Health Management FrameworkFIBE by employing a novel Identity based Data Encryption Algorithm with Novel Strict Policy Control Based Data Access model approaches. Effective User Specific Proxy Re-encryption Algorithm is proposed to support the third party access and to afford secure access of data .This combined approach provides a comprehensive solution for EHR data security. Here, we start from an overview of the proposed attribute based key generation, and discuss the access control mechanism and its merits. As shown in Fig 1, the proposed framework contains the following parties: patients, hospital admin, attribute authority and Third party user. Hospital admin is known as health professional who takes care of patient's health. Generally the hospital admin is responsible for EHR data transaction and maintenance. Attribute authority is the group of authorized identities in charge for organizing healthcare evidence Exchange between healthcare systems. They are also responsible for distributing decryption keys to the aforementioned patient. Third party user is the person who is permitted to assess a patient's EHR. It can be a patient's family member, a patient's friend, a health insurance company, etc. The maneuvers of offered Novel High Secure E-Health Management Framework integrate Identity based Data Encryption and access policies These procedures could be well-organized in the following steps:

A. Fortified Identity based Data Encryption (FIBE)

A fortified Identity based Data Encryption Algorithm is employed among the E-Health management registered patient and the cloud storage system.The proposed algorithm supports hospital admin to collect all the health relevant information entered by the patient and generate keys based on the patient identity information for encrypting and uploading the data. These information is further uploaded into cloud storage for all corresponding registered patients.

Algorithm I: Fortified Identity based Data Encryption

Input: Input data (D), User Identity (I_n)
Output: Encrypted Data (Eny_D)
Procedure:
Let U_r be the user
Let I_n be the Identity of the User
Where n represent the number of identity attributes corresponding to the user.
Key Generation:
Step 1: For x= 1 to n
Step 2: For y= 1 to I_1.Size
Step 3: T_x=T_x+I_1(y)
Step 4: If (y <I_2.Size)
Step 5: T_x=T_x+I_1(y)
Step 6: End if y
Step 7: If (I_1.Size <I_2.Size)
Step 8: T_x=T_x+ I_2(I_1.Size)
Step 9: End if
Step 10: End for y
Step 11: End for x
Step 12: If (T_x>=K_l)
Step 13: $g_K \leftarrow T_x(K_l)$
Step 14: Else
Step 15: For j= 1 to K_l-T_x.size
Step 16: g_K=g_K+pad_j
Step 17: End for j
Step 18: End if

The concept of Identity based data encryption is introduced along with strict access policy control method. This process implicates encryption and authentication in order to access the EHR of the patient. This new fortified Identity based key encryption method permit a group of parties (Health care providers) within a huge and fully insecure public network to

access the secret key through cloud service provider and hospital admin. It guarantees each party that no other party apart from these parties can get that key. This key authentication technique works as follows.

Key-generation: Suppose U_r be the user and I_n be the Identity of the user. Here trusted party generate the private keys corresponding to the users in the system. General public key g_K is generated which can, in some sense, considered to be the "public key" of our key generation approach which has 56 bit in length. Therefore, on a high level, the aforementioned key generation setup can be regarded as a fast and secure key generation that provides the binding between the identity of a user and their secret key passably analogous to the certifying authority in the traditional public-key infrastructure. Our proposed key generation technique can compute secret key corresponding to any user, it can decrypt cipher text meant for any user.

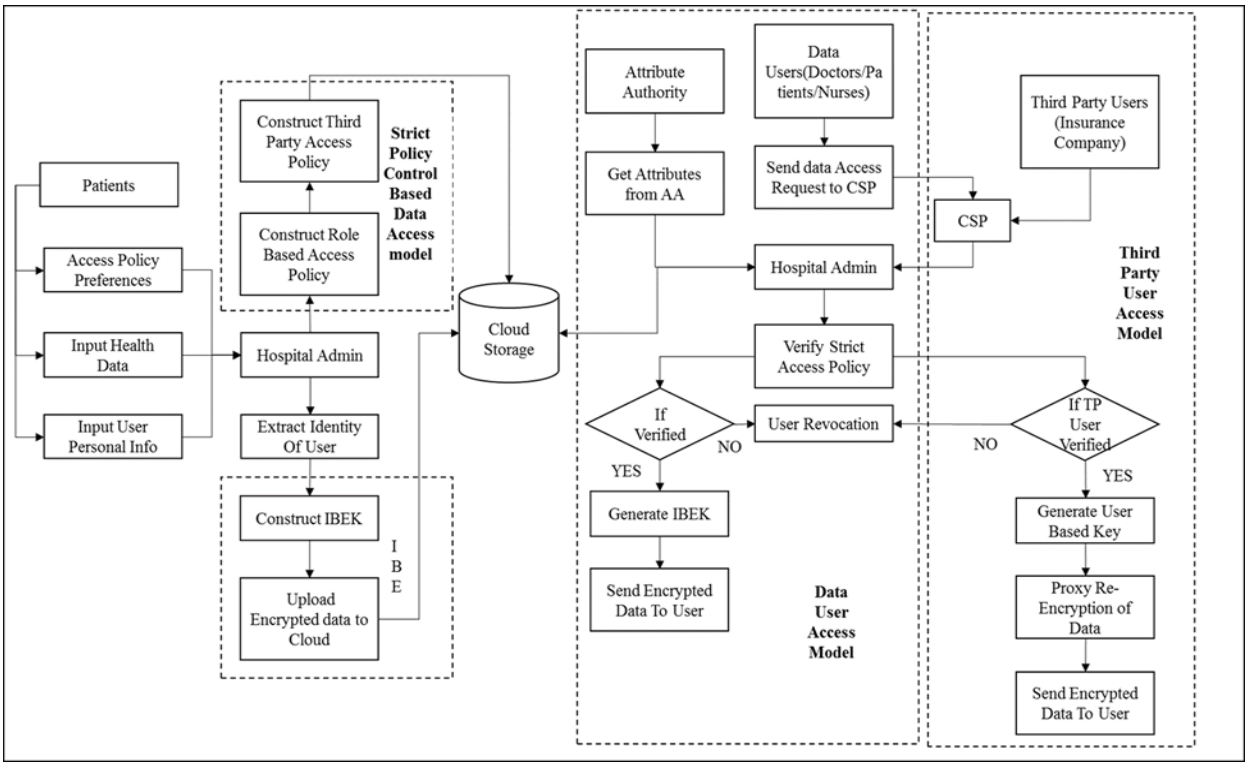

Fig 1: Overall Flow of the FIBE System

EHR Data Encryption: The electronic Health Records are encrypted using a new encryption algorithm. Identity based Data Encryption Algorithm is asymmetric key based block encryption technique which divides data into blocks of equal length and encrypts each block using a special f-function value.

Our Encryption algorithm operates on 64 bit blocks of data at a time. After an initial permutation, the block is broken into a right half and a left half, each 32 bits long. The bits of the plain text are enciphered based upon their placement in the text using identity based encryption Key. A high performance Identity based Data Encryption architecture has been proposed with XOR based substitution box (S-Box).A cryptographic technique exists at bit level by using block based substitution method, logical operations like XOR and shifting operations. The proposed technique used XOR operation and a pair of functions for thoroughly mixing and permuting the binary bits of the plaintext and the key in every round of the iteration process before the result assumes the form of the cipher text. The 4 generated S-boxes produces the 32-bit value of output. During the encryption process, the input data is considered as 64 bit blocks. This 64 bit is separated into 32 bit of two halves as left half and right half.

Algorithm II: EHR Encryption:

Step 1: Let D be the data to be encrypted
Step 2: $P_i \leftarrow$ Generated Key g_K
Step 3: $S_i \leftarrow$ Be the S-Boxes for i=1to 4
Step 4: Considering input data as 64 bit blocks
Step 5: Let L_t and R_t be the 32 bits of D

Step 6: For z= 1 to Rn_d
Step 7: $L_t \leftarrow L_t \oplus P_i$//Compute F-function
Step 8: Split$L_i \leftarrow L_t/4$
Step 9: $O_i = (L_i * S_i) + 2^{32} \oplus R_t$
Step 10: $R_t \leftarrow O_i$
Step 11: If ($Rn_d <= Rn_d - 1$)
Step 12: $T_t = R_t$
Step 13: $R_t = L_t$
Step 14: $L_t = T_t$
Step 15: Else
Step 16: $R_t = R_t \oplus P_{n-2}$
Step 17: $L_t = L_t \oplus P_{n-1}$
Step 18: End if
Step 19: $Eny_D \leftarrow (L_t, R_t)$

In every iteration, the bits of the identity based encryption key are shifted and then 48 bits are chosen commencing the 56 bits of the key. The right half of the information is extended to 48 bits through an extension permutation, joined by way of 48 bits of a shifted and permuted key by the use of an XOR, sent through 4 S-boxes producing 16 new bits and permuted again. After these four operations, the output is combined with the left half via another XOR. The swapping operation could be performed between the new right half and the old right half. These operations are repeated for length of the rounds considered. After the end of the iteration, the right and left halves are joined and a final permutation is accomplished which is the inverse of the initial permutation. Thus the encryption process finishes off and the cipher text is stored in the cloud storage. The same process is reversed to decrypt the data by generating the key using the exact identities of the users.

B. Strict Policy Control Based Data Access model

Policy control based data access algorithm provides the privileges whom to access the data. The encrypted uploaded data are accessed by several users based on the access control Structures which are designed by the Attribute Authority. When the Key generated by the user match the user identity based key then the user information will decrypted and used.

Table 1: Access Control Policy

Attributes / Users	Physician License	Practitioner License	Nursing License	ISO License	Group A(clinics)	Group B(clinics)	LIC
Physician	✓	×	×	×	✓	×	×
Attenders	×	×	✓	×	✓	×	×
Analyst	×	✓	×	×	✓	×	×
LIC executive	×	×	×	✓	×	×	✓

Input: user policy preferences, admin policy allocation
Output: Strict Access Policy Control Model
Procedure:

In the proposed model, [3, 26]there are two tier access policy allocation strategy which filters the authenticated user and revokes the unauthenticated users. When the user registers in a hospital and logins with his authentication credentials, the user tries to upload all his/ hers personal information, medical history and reports. Here in our scenario, since the user registers through cloud, the user can restrict the access of the data by either sharing the data to multiple hospitals or multiple doctors or multiple scan centres. So the user creates the access policy by restrict the user based on the attributes of the users.

Then the patient's Policy can be set using the following policy settings:
Role based policy users are physicians, attenders and analysts, whereas the LIC executive is a third party user, hence the policy differs. The Hospital Admin can further set strict access policy settings by classifying the patient in formations into

Personal data, Case Study, Current Reports, Coverage Claims and set policy as follows
For example for a patient: A

The Admin can set policy as

Users Records	Physician	Attenders	Analysts	LIC Exec.
Personal data	☑	☑	☑	☑
Case Study	☑	☒	☑	☒
Current Reports	☑	☑	☒	☒
Coverage Claims	☒	☒	☒	☑

C. User Specific Proxy Re-encryption and Decryption

The re-encryption is used to encrypt the encrypted data again. This provides more security to the medical information in cloud storage. An Effective User Specific Proxy Re-encryption Algorithm is proposed to support the third party access and to provide secure access for the data. The third party user who request the data will be authorized to access the data after authentication of corresponding patient. I fany data user (Doctor) request to access user data, initially user preference policy is verified, if the user is having an authenticated access, his strict policy is verified, else the user access is revoked, if the user who is requesting is having access to the specific file he is looking for, then the strict policy is verified, else the user access is also revoked. And the data is decrypted by the user.

Algorithm III: User Specific Proxy Re-encryption and Decryption

Input: Encrypted data, Strict Policy Verification status.
Output: Decrypted data (Dec_D)
Step 1: Let U_{rq} be any requesting user
Step 2: Let P_N be the selected patients whose information has to be accessed.
Step 3: Initially the user's policy preference is verified.
Step 4: Admin forwards request to the Attribute authority to authenticate the user.
Step 5: Using the attributes from attribute authority the following verification is done.
Step 6: If (U_{PP}(status) =AA_l)
Step 7: PP_{status} = satisfied
Step 8: The strict policy of the user is extracted and the verified with the requested data of P_N
Step 9: If (U_{STP} =verified)
Step 10: STP_{status} =satisfied
Step 11: If (U_{rq}.Role Based Policy &&PP_{status} = satisfied &&STP_{status} = satisfied)
Step12: User access granted
Step 13: I_n of the P_N is forwarded to the requesting user U_{rq}
Step 14: Key generation is done
Step 15: User data is decrypted using the reverse process of encryption methodology.
Step 16: ElseIf (U_{rq}.Third Party Policy &&PP_{status} = satisfied &&STP_{status} = satisfied)
Step 17: User access granted
Step 18: In the admin side, the encrypted data is decrypted, by the key
Step 19: Third party policy key is generated using the following steps
Step 20: Let I_{tp} be the identity of the U_{rq}
Step 21: For x= 1 to tp
Step 22: For y= 1 to I_1.Size
Step 23: T_x=T_x+I_1(y)
Step 24: If (y <I_2.Size)
Step 25: T_x=T_x+I_1(y)
Step 26: End if y
Step 27: If (I_1.Size <I_2.Size)
Step 28: T_x=T_x+ I_2(I_1.Size)
Step 29: End if
Step 30: End for y
Step 31: End for x
Step 32: If (T_x>=K_l)
Step 33: $g_K \leftarrow T_x(K_l)$

Step 34: Else
Step 35: For j= 1 to K_l-T_x.size
Step 36: g_K=g_K+pad_j
Step 37: End for j
Step 38: End if
Step 39: Encrypt the data using the generated g_K
Step 40: Forward the encrypted data to the third party user.
Step 41: Decryption is done by the requested user identity information
Step 42: End if
Step 43: Else If (U_{STP} =Not verified)
Step 44: U_{rq} is revoked
Step 45: End if
Step 46: Else if (U_{PP} (status)! =AA_l)
Step 47: U_{rq} is revoked
Step 48: End if

IV. PERFORMANCE ANALYSIS

We assess the performance of the proposed Identity based Data Encryption mechanism by using various evaluation metrics in this section. It includes encryption cost, Re-Encryption Cost, First level decryption Cost, Second level decryption Cost and efficiency of the algorithm.

A. Encryption cost.

The Encryption cost includes the Encryption key generation time, Key transmission time and Data encryption time. Encryption Key generation time is defined as the time taken by the mechanism to generate the key used for encryption. Encryption time is defined as the time taken by an encryption algorithm to generate the cipher data from the original data. These measures are calculated to evaluate the encryption cost of an encryption technique.

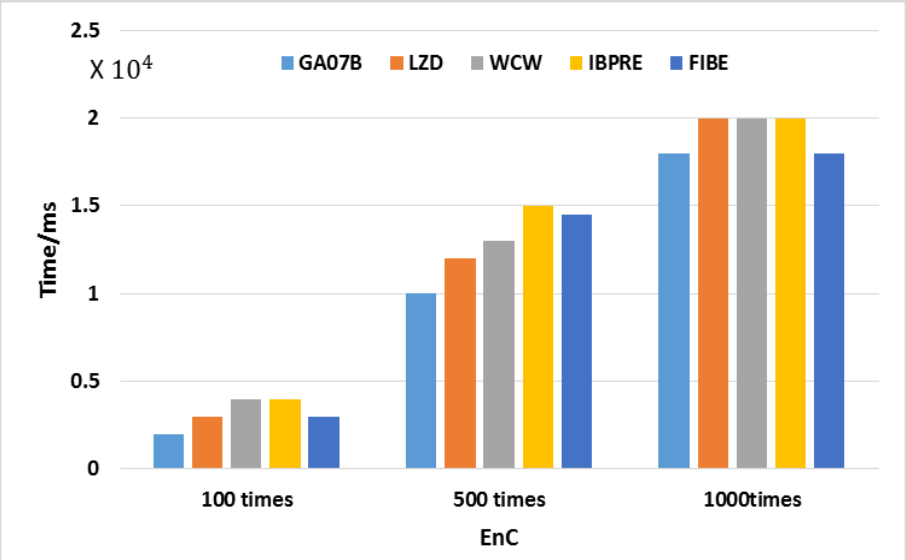

Fig. 2: Encryption cost.

Fig.2 shows the encryption cost of the existing GA07B[27], LZB[28], WCW[29], IBPRE[26] and proposed mechanisms with respect to varying encryption rounds. From the evaluation, it is observed that the proposed mechanism requires very lesser encryption cost compared to the existing schemes. Since this technique uses identity based key generation and encryption that reduces the required key size for attaining appropriate security. In the 1000 round, the encryption cost of every algorithmis assessed with the values of GA07B- 1.8 ms, LZD- 2 ms, WCW- 2ms, IBPRE- 2ms and Proposed- 1.8 ms. Our FIBE framework achieved equal encryption cost with the existing algorithm GA07B and 10% much lesser encryption cost than the LZD and WCW algorithm.

B. Re-encryption cost

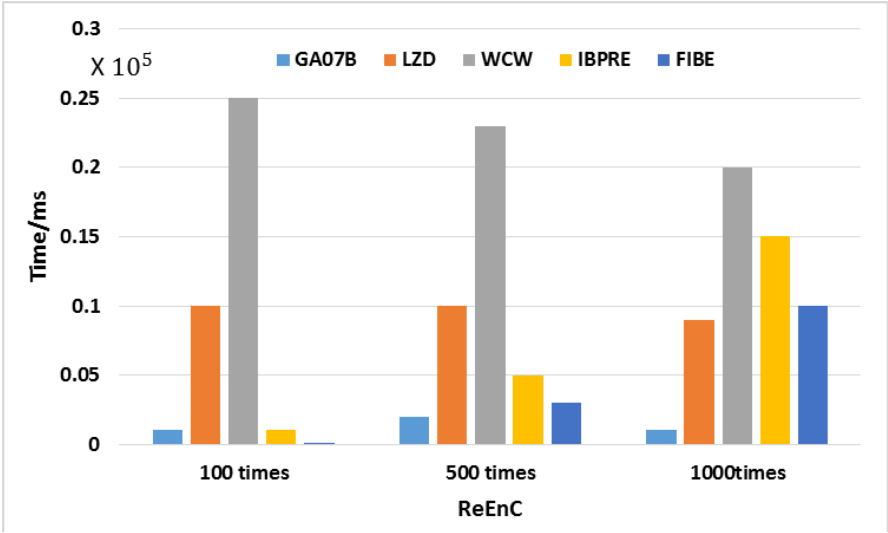

Fig. 3: Re-encryption cost

Fig. 3 shows the re-encryption cost of all evaluated algorithms. The cloud storage always involve re-encryption mechanisms regarding the security and EHR data sharing of data. Thus our FIBE scheme is the most proficient one for the cloud and can accomplish cost effectiveness Compared with others mechanisms.

C. Security comparison analysis

The security comparison analysis is conducted amongst the existing and proposed schemes with respect to the processes of encryption, security, authority control, Access policy, means of revocation, privacy preserving, and integrity as shown in Table 3. In the proposed mechanism, the secret keys are linked with the identity, hence the transmitted message is updated when the user is invalidated.

Table 3: Proposed efficiency comparison.

Scheme	Encryption	Security	Central authortiy	Access Policy	Revocation means	Privacy preserving	Integrity
Multi-authority attribute based **encryption**	KP-ABE	Not against user–server collusion	Yes	Threshold	N/A	No	No
threshold multi authority attribute based encryption	KP-ABE	Not against user–server collusion	No	Threshold	N/A	No	No
multi authority attribute-based encryption.	KP-ABE	Against N-2 authority collusion	No	Threshold	N/A	Yes	No
Huiling**et al**	CP-ABE	Against N-1 authority collusion	No	Access Tree	Attribute-level, immediate	Yes	No
FIBE	**Strict Policy based IBE**	**Against authority collusion**	**Yes**	**Access Rules**	**Attribute-leve l, User preference**	**Yes**	**Yes**

D. First Level Decryption

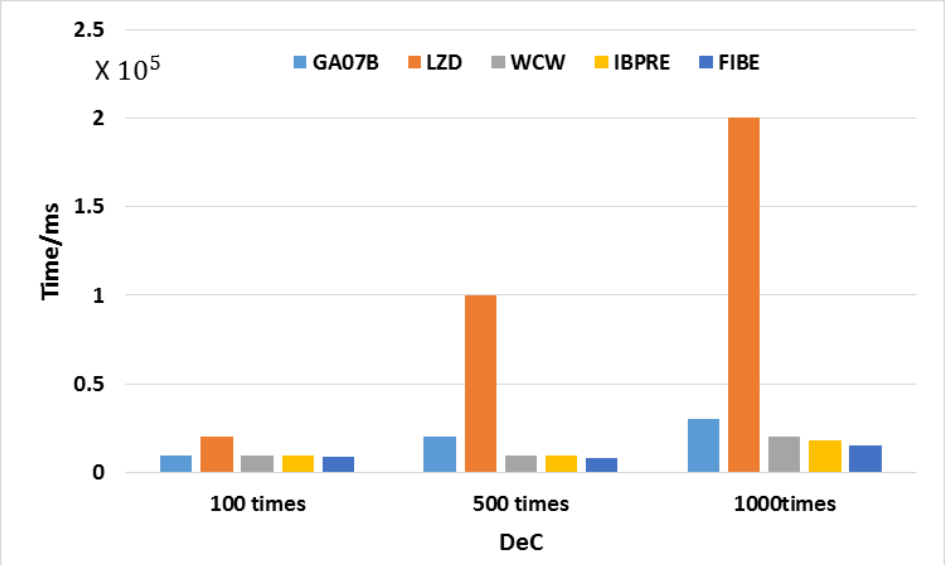

Fig. 4: First level decryption cost.

Fig 4 shows the first level decryption cost of all evaluated algorithms. The plotted graph indicates that the decryption time is reduced in our algorithm. In the 1000 round, the first level decryption cost of every algorithm is assessed with the values of GA07B- 0.3 ms, LZD- 2 ms, WCW- 0.2ms, IBPRE- 0.18ms and FIBE- 0.15ms.In our proposed algorithm the sizes of public key and general key grow linearly with the number of identity given by the patient. The results shows that our algorithm achieved much lesser decryption cost than the existing algorithms. This is due to the patients generate their own decryption keys and distribute it to their authorized users.

E. Second level decryption cost

Fig 5 shows the second level decryption cost of all evaluated algorithms in the cloud storage. In the 1000 round, the Second level decryption cost of every algorithm is assessed with the values of GA07B- 0.4 ms, LZD- 0.8ms, WCW- 0.4ms, IBPRE- 0.4ms and FIBE- 0.3 ms. The result illustrates that our algorithm attained much lesser decryption cost than the existing algorithms.

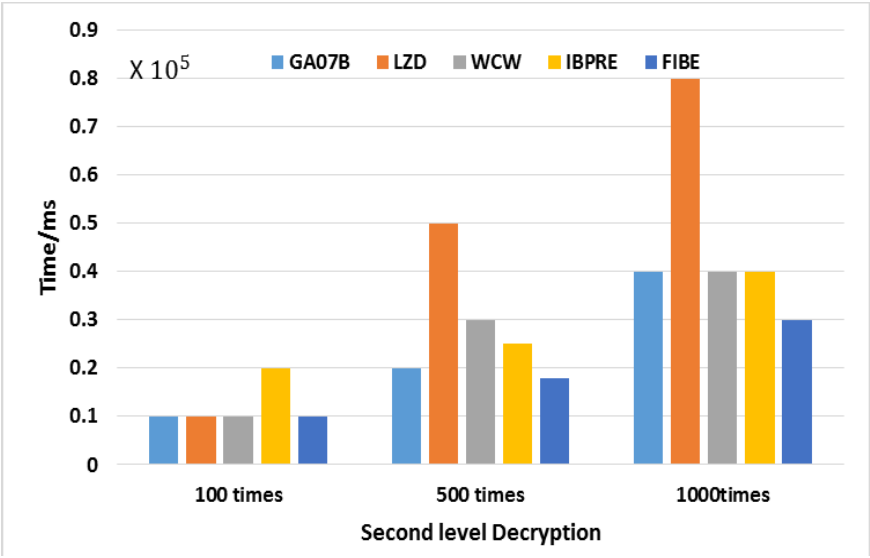

Fig. 5: Second level decryption cost.

CONCLUSION AND FUTURE WORK

We introduced a new E-Health management system which enforces security to the patient's EHR in cloud assisted environment. Our proposed framework is the combination of both Fortified identity based encryption (FIBE) and strict access control policy approaches. Generally the cloud servers are less trustworthy because of security issues. This work supports the patients to preserve their secret medical information using suitable cryptographic techniques. The patients could take advantage of our framework regarding strict access control policies. The proposed patient-centric access control divides the access policy into two domains namely user policy preferences and admin policy allocation. In the first method, the user can set the access control policy according to the privileges they want to be given for the data user or third parties (Insurance). In the second method, the hospital admin provides privileges for the data user and third parties. The simulation results shows that our E-Health management system provides better security than the existing algorithms. Our comprehensive approach also enhances the interoperability operations of EHR services among the patients, Hospital admin, data users and third parties. In future, we have idea to make dynamic access control mechanism which provides better key management and policy control.

REFERENCES

[1] X. Wu, R. Jiang, and B. Bhargava, "On the security of data access control for multiauthority cloud storage systems," *IEEE Transactions on Services Computing*, vol. 10, pp. 258-272, 2017.
[2] C.-J. Wang, X.-L. Xu, D.-Y. Shi, and W.-L. Lin, "An efficient cloud-based personal health records system using attribute-based encryption and anonymous multi-receiver identity-based encryption," in *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on*, 2014, pp. 74-81.
[3] 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, pp. 487-497, 2015.
[4] F. Xhafa, J. Feng, Y. Zhang, X. Chen, and J. Li, "Privacy-aware attribute-based PHR sharing with user accountability in cloud computing," *The Journal of Supercomputing*, vol. 71, pp. 1607-1619, 2015.
[5] G. Logeswari, D. Sangeetha, and V. Vaidehi, "A cost effective clustering based anonymization approach for storing PHR's in cloud," in *Recent Trends in Information Technology (ICRTIT), 2014 International Conference on*, 2014, pp. 1-5.
[6] D. A. Gondkar and V. Kadam, "Attribute based encryption for securing personal health record on cloud," in *Devices, Circuits and Systems (ICDCS), 2014 2nd International Conference on*, 2014, pp. 1-5.
[7] R. L. GV and B. Annappa, "An Efficient Framework and Access control scheme for cloud health care," in *Cloud Computing Technology and Science (CloudCom), 2015 IEEE 7th International Conference on*, 2015, pp. 552-557.
[8] S. Thatikayala, J. Sandhyarani, and J. Sravanthi, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans Parallel Distrib Syst*, vol. 3, pp. 4912-4917, 2014.
[9] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, pp. 222-233, 2014.
[10] A. Ghazvini and Z. Shukur, "Security challenges and success factors of electronic healthcare system," *Procedia Technology*, vol. 11, pp. 212-219, 2013.
[11] J. Zhou, X. Lin, X. Dong, and Z. Cao, "PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributedm-healthcare cloud computing system," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, pp. 1693-1703, 2015.
[12] H. M. Hamad and W. A. Abudalal, "The Two secured Factors of Authentication," *IUG Journal of Natural Studies*, vol. 24, 2016.
[13] S. Jaganathan and D. Veerappan, "CIADS: a framework for secured storage of patients medical data in cloud," *Int J WSEAS Trans Inf Sci Appl*, vol. 12, pp. 22-35, 2015.
[14] Y. Tong, J. Sun, S. S. Chow, and P. Li, "Towards auditable cloud-assisted access of encrypted health data," in *Communications and Network Security (CNS), 2013 IEEE Conference on*, 2013, pp. 514-519.
[15] C. Gao and N. Iwane, "A Social Network Model with Privacy Preserving and Reliability Assurance and its Applications in Health Care," *social networks*, vol. 6, 2015.
[16] J. Hong, K. Xue, Y. Xue, W. Chen, D. S. Wei, N. Yu, *et al.*, "TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud," *IEEE Transactions on Services Computing*, 2017.
[17] A. S. Kumar, K. Srinivas, and K. Obulesh, "PSMPAL: Patient Self-Controllable, Multi-Level Privacy-Preserving Cooperative Authentication and Load balancing in Distributed M-Healthcare Cloud Computing System," 2016.
[18] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, pp. 131-143, 2013.
[19] S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu, and W. Xie, "Attribute-based data sharing scheme revisited in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 1661-1673, 2016.
[20] T. Loruenser, A. Happe, and D. Slamanig, "ARCHISTAR: towards secure and robust cloud based data sharing," in *Cloud Computing Technology and Science (CloudCom), 2015 IEEE 7th International Conference on*, 2015, pp. 371-378.
[21] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, pp. 1187-1198, 2016.

[22] X. Dong, J. Yu, Y. Zhu, Y. Chen, Y. Luo, and M. Li, "SECO: Secure and scalable data collaboration services in cloud computing," *computers & security*, vol. 50, pp. 91-105, 2015.
[23] S. Balasubramaniam and V. Kavitha, "Geometric data perturbation-based personal health record transactions in cloud computing," *The Scientific World Journal*, vol. 2015, 2015.
[24] M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A. V. Vasilakos, K. Li, *et al.*, "SeDaSC: secure data sharing in clouds," *IEEE Systems Journal*, 2015.
[25] P. Urbauer, S. Sauermann, M. Frohner, M. Forjan, B. Pohn, and A. Mense, "Applicability of IHE/Continua components for PHR systems: learning from experiences," *Computers in biology and medicine*, vol. 59, pp. 186-193, 2015.
[26] X. A. Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, "Cost-effective secure E-health cloud system using identity based cryptographic techniques," *Future Generation Computer Systems*, vol. 67, pp. 242-254, 2017.
[27] J. Zhang, X. A. Wang, and X. Yang, "Identity based proxy re-encryption from BB1 IBE," *Journal of computers*, vol. 8, 2013.
[28] A. S. Sidhu and E. M. Garg, "An Advanced Text Encryption & Compression System Based on ASCII Values & Arithmetic Encoding to Improve Data Security," *International Journal of Computer Science and Mobile Computing*, vol. 3, 2014.
[29] J. Shao and Z. Cao, "Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption," *Information Sciences*, vol. 206, pp. 83-95, 2012.