JOURNAL OF PURE AND APPLIED MICROBIOLOGY, Aug. 2015. Vol. **9**, p. 57-63
SPECIAL ISSUE ON RECENT RESEARCH CHALLENGES IN BIO-MEDICAL APPLICATIONS

An Efficient EMR Data Access Control in Cloud using Extended HABE (EHABE) Scheme

R. Manjusha[1] and R. Ramachandran[2]

[1]Department of Information Technology, Sathyabama University, Chennai, India.
[2]Department of ECE, Director (Research), Sri Venkateshwara College of Engineering, Chennai, India.

(Received: 03 March 2015; accepted: 06 May 2015)

An emerging cloud computing technology makes the task easier to store the Electronic Medical Record (EMR) data sets by achieving the reduction in processing timeand bandwidth (storage space). To store the sensitive EMR data sets in cloud is the challenging task. For secure storage, the EMR data sets are encrypted before it is getting outsourced and stored into cloud environment. The existing encryption approaches are still lacking to ensure security, scalability and efficiency. To overcome this issue, introduce a technique by combining the strongest and fastest Homomorphic encryption along with Hierarchal Attribute Based Encryption (EHABE) scheme. Utilization of Homomorphic encryption gives high security to sensitive data of EMR data sets in thecloud environment. The research is extendedto provide the scalability by establishing the efficient access control, while accessing the encrypted data from the cloud environment using the combination of hierarchical identity based encryption (HIBE) and a cipher text-policy attribute-based encryption (CP-ABE) i.e., HABE scheme. Thus, the performance analysis of this technique provides high security to the EMR data sets in the cloud environment.

Key words: Cloud Computing, Homomorphic Encryption, Hierarchal Attribute Based Encryption (HABE).

The Cloud computing technology is used to share the EMR data sets on cloud servers to share the patient's health details in a secure manner. In cloud environment the data confidentiality is obtained by encrypting the data sets before uploading those data sets into the cloud by using the encryptiontechniques[1]. Thus, it provides security for sensitive data in cloud by hiding all useful information about the plaintext. In spite of that, various existing data security systems are invalid because of the hacker's and data migrates to diverse servers. It is necessary to provide the security, in order to protect the EMR data sets. To secure the confidential datasets of EMR, the EHABE scheme is utilized.The HABE model, which incorporates the property of hierarchical generation of keys in the HABE system, and the property of flexible access control of the CP-ABE system.Homomorphic encryption technique provides high security to sensitive data[14] through computations and it is more applicable to the EMR data sets[15] in sharing and accessing the data sets from the cloud.

The secure data sharing of sensitive data sets in the cloud using Proxy re-encryption along with Cipher-text Attribute Based Encryption (CP-ABE) scheme[2]. The homomorphic encryption systems are used to perform operations on encrypted data without knowing the private key. The encryption scheme does not know the appropriate identities of the intended patientrather than that, the patient has to describe their descriptive attributes. Therefore, the adopted encryption system should support the HABE scheme. The flexible schemes such as a cipher text-policy attribute-based encryption (CP-ABE)[10,18] and hierarchical identity based encryption (HIBE) can be adopted to provide a fine grain access control

* To whom all correspondence should be addressed.
E-mail: manjushaphd14@gmail.com

for the encrypted data[3]. By using hierarchical scheme the data users are preferred on the basis of hierarchy and the level of the user node.Then the access rights are issued to the users, there by securing the data sets from unauthorized users. The HABE scheme[7] permits encrypted data in determining an access control policy than attributes, a patient with specific attribute set with particular identity fulfil the policy to decrypt the relative data sets.

While performing the encryption process sensitive data[17] are encrypted before sending it to the cloud. However to execute the operation the data must be decrypted each time. Up to this point it was difficult to encrypt sensitive data. So the Cloud provider permit to perform the functions on encrypted data without decrypting them by utilizing the cryptosystems corresponding to Homomorphic Encryption[3]. To attain the goal with enough privacy protection, reduce computation overhead and fine grained access control in cloud, this paper introduces a technique of EHABE scheme.

The remaining of this paper, Section II gives ahighlighted related work and Section III provides the clear methodology of proposed EHABE scheme. The performance and implementation results are discussed in Section IV and conclude paper in Section V.

Related Work

The identity-based cryptography was proposed by Adi Shamir to provide the identities for all the users. Key management is fine and good in the identity-based cryptography. In an identity-based encryption the sensitive data are encrypted by utilizing an arbitrary finite sequence of character as the key. The authority of decryption key is depict to the authority of encryption key and there is one and only private key generator (PKG) to disperse the private keys to every user, which is undesirable for an extensive network[4]. To avoid this Boneh and Boyen proposed HIBE Scheme, It develops the length of the cipher text by using the private keys. The HIBE constructions are linearly with the depth of a beneficiary in the hierarchy. The proposed HIBE scheme gives better execution over identity-based cryptography[19].

Bethencourt *et al*,[5] proposed a cipher text policy attribute-based (CP-ABE) scheme with the access policy, in accessing the encrypted data. The access control method of this scheme is similar to the key policy attribute-based encryption (KP-ABE). In this scheme, the access policy is constructed from the user's private key. The set of the descriptive attributes are associated with the user's private key, and the access policy is built for each encrypted data. The access structure of the encrypted data is corresponding to the user's private key with a set of descriptive attributes. If a set of attributes in user's private key satisfies the access structure of the encrypted data, the data user can decrypt the cipher text, otherwise the data user cannot obtain the original plain text. However, the CP-ABE scheme is applied in proxy re-encryption field to increase the security in cloud environment[6].

To enable high security to the sensitive data in cloud Maha TEBAA *et al*.,[8,20] have suggest an encryption technique to perform functions on encrypted data without decrypting them, which will give the same outcomes without analyzing the data sets, such techniques is referred to as ahomomorphic . The Homomorphic Encryption[13] frameworks are utilized to perform functions on cipher text without knowing the exact private key. In this paper, thesystem model utilizes the homomorphic encryption in cloud computing for security, this encryption concept which empowers the outcomes of computation on encrypted data without knowing the raw data. Additionally, Xiao *et al*.,[9] recommended protocol for Multi User frameworks, which focuseson the symmetric Homomorphic Encryption[16] that could estimate the operations on polynomials and their procedures are tightly coupled. Such restriction to client and server model, make them acceptable for outsourcing scientific calculation but not for cloud applications. The cloud storage offers many advantages like flexible, efficient and secure sharing of data, but it lacks in the case of variable sized ciphertext. Thus, the paper[23] proposes a Key aggregate cryptosystem- a public key encryption technique that format the constant size cipher text and decryption rights to each of the cipher text to maintain the confidential data sets.

Efficient Access Control of EMR Data Sets Using Homomorphicand HABE Encryption Techniques

This section describes a cloud security and fine grained access controlby the utilization of EHABE scheme. The homomorphic encryption

technique is used for data security in cloud environment. The Hierarchical Attribute Based Encryption (HABE) is utilized to generate the hierarchal level, attribute key and identity key to encrypt the data through the homomorphic encryption techniques.

Hierarchical attribute based encryption (HABE) is integrated with the Homomorphic encryption (EHABE) scheme to accomplish the fine-grained access control in the cloud environment. The HABE scheme is derived from HIBE and CP-ABE scheme[11]. In this scheme, there are various keys with distinctive usages. Initially this system gives a brief statement of the most significant keys to serve as a fast references. The HABE accepts all the characteristics within a single conjunctive provision. The utilization of EHABE scheme assists the attributes with respect to the flexible set of attribute combinations. Though, it gives more flexible, scalable and fine grained access control[12] for cloud computing environment.

Hierarchical Attribute Based Encryption Model

Fig 1.Describes the working of HABE model, which combines the properties of Hierarchical Idendity Based Encryption (HIBE) and Cipher-text Policy Attribute Based Encryption (CP-ABE) which comprises the EMR data sets[21].The CMA (Cloud Medical Admin) handles the public key in EHABE scheme, whichcontrolsthe distribution and generation system ofparam and domain keys. CMA's perceives keys for a subjective number of disjoint attributes of each and every patient, and have a full control over the semantics and structure of their properties. In the HABE model the attributes with unique identity, is maintainedfor all the patients, with their ID and a descriptive attribute set, where identity is a finite string inanalysing any particular patient.

Homomorphic Encryption

The homomorphic encryption gives solution for security by encrypting the EMR data sets. In this encryption technique, the CMA can encrypt the EMR data set (n) and transmits the encryption E(*n*) to the server to obtain theciphertext by assessingthe operation f on the underlying n acquiring the encrypted outcome E(f(n)).

A homomorphic encryption scheme consists of following tasks:

KeyGen(*k)*

On input *n*the algorithm k outputs an encryption/decryption key pair (k_e, k_d) =*k*€ *k*, Where *k* denotes the key space.

Encryption

The plaintext *n*, *k* and an element m € **N** the encryption algorithm E outputs a ciphertext c € C,whereCdenotes the cipher text space.

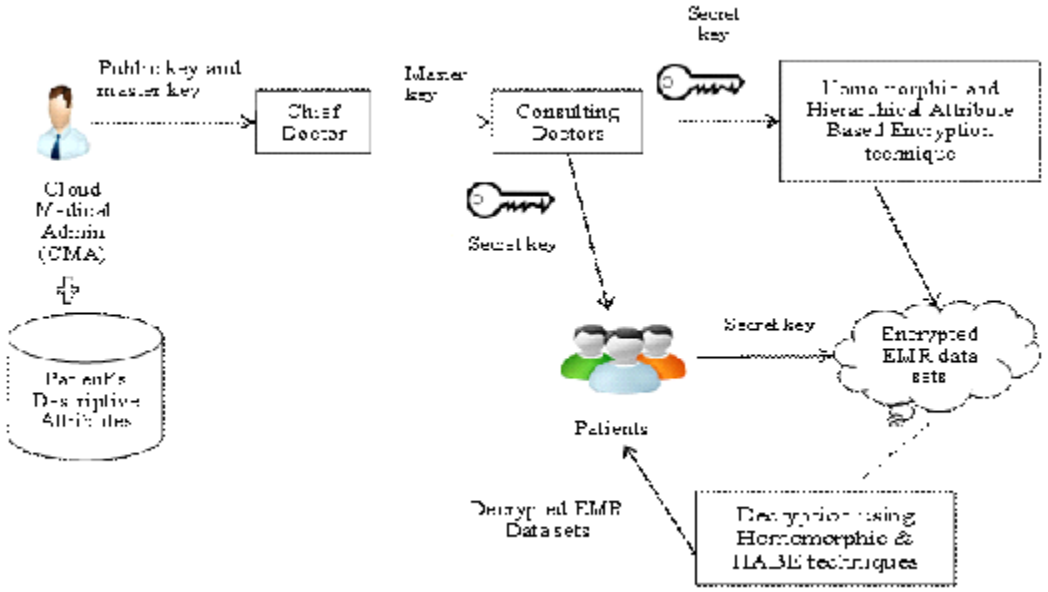

Fig. 1. Homomorphic and HABE techniques for secure and efficient access control

Decryption

The decryption algorithm D is deterministic. On plaintext*n, k*, and an element*c* € C, it results an element in the message space M so that for all m € **N** it holds: if*c=E* (*n*, k_e, *m*).

EHABE Scheme

TheEHABE schemeis responsible for generating master keys, public keys, patient's identity key and patient's attribute key. The EHABE scheme provides the privilege to each patient for accessing the confidential EMR data sets in the cloud. In a hierarchical way of approach,the patient'scan access the EMR data sets from cloud on the basis of privilege, which differs from one patient to other patient. The data owner (CMA) encrypts the data with a public key by using the set of descriptive attributes of each patient. A data receiver's (patient) role is to decrypt the encrypted data with their identity key and private key to obtain the needed confidential data sets of EMR.

In this EHABE model, initially defines each patient's attribute along with a unique identifier (*ID*). The entities of public key, which denotes its position in the HABE model, to identify the patient consisting of the public key (*PKi*) to access their EMR data set details, for example the public key of patient with *IDi*is in the form of (*PKi"1; IDi*), the public key of patient*u* with *IDu*is in the form of (*PKi; IDu*), and the public key of attribute *a* with *IDa*is in the form of (*PKi; IDa*), where *PKi"1*, and *PKi*are assumed to be the public keys of the users that administer the all users, *u*, and *a*, respectively.

Construction of Hirerachal Identification Based onEHABE

Key Setup

CMAtakes the security parameter (â) as input and outputs the public parameter (*PK*) and master key (*MKi*) for all the chief doctor. The public parameters (*params*) will be publicly available, while *MK0 = (mk0)* will be kept secret.

$$CMA \xrightarrow{\beta} PK + MKi \quad ...(1)$$

Key Generation

Generation of Master key

The chief doctor generates the master keys *MKi+1* for the consulting doctors by using the public key *PK*, the patient's public key *PKi+1*, and its master key *MKi*.

$$Cheif\ Doctor \xrightarrow{PK,MKi,PKi+1} Mki + 1 \quad n \quad ...(2)$$

Generation of Secret key

The CMAfirst checks whether the Chief doctor*u* is authorized to diagoniseparticular attribute *a* with the unique identity key, when a Chief doctor requests to the CMA for the patient's identity secret key *SKi;u*and the patient's attribute secret key on *Ski,u,a*. If so, it creates the patient's identity secret key and patient's attribute secret key by using the public key of consulting doctor, master key (*MKi*), patient's identity of public key (*PKu*), patient's attribute of public key (*PKa*). Likewise the consulting doctors generates the secret keys for each and every patient.

$$Consulting\ doctors \xrightarrow{PK,MKi,PKu,PKa} SKi,u,a \quad ...(3)$$

Encryption

Using the encryption technique called homomorphic encryption technique, which used to encrypt the plaintext and produce the cipher text using public and private keys[22]. Now the Chief doctor wants to send a message to the consulting

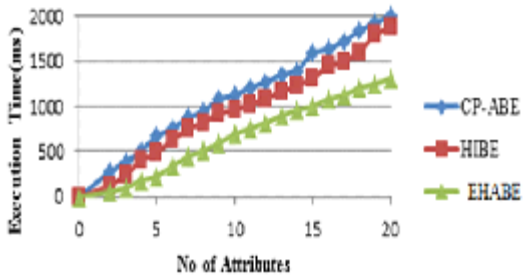

Fig. 2. Execution Time Vs Number of Attributes

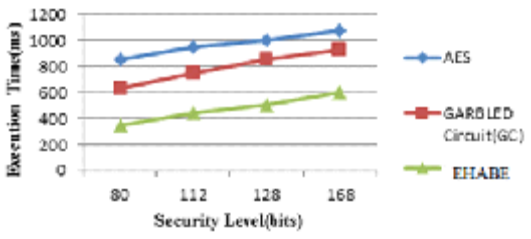

Fig. 3. Execution Time Vs Security Level

doctors, which means first the CMA has to encrypt the plaintext message (*M*) and sends to a cloud service provider. The cloud service provider receives the encrypted plaintext (*C*) but, does not know about the original plain text. Although the cloud service provider uses functions on the encrypted message. Here the cloud service provider uses the reversing function on the encrypted plaintext (*C*) and sends the cipher text (*C'*) to the chief doctors. By receiving the cipher text (*C'*) uses the public key (*PK*), set of attributes (á) to decrypt the EMR data sets.

$$Consulting\ doctors \xrightarrow{M\ (plaintext),PK,a} CT\ (Ciphertext) \quad ...(4)$$

Decryption

Consulting doctors wants to decrypt the *C'* using their secret key and chief doctor's public key. Then the consulting doctors convert the *C'* and into the original plaintext and provides them to the patient, using the Encryption technique which encrypts the plain text and produce the cipher text using public and secret key.

$$Patient \xrightarrow{CT,SKi,PK} M\ (plain\ text) \quad ...(5)$$

This EHABE scheme can satisfy the property of security and fine-grained access control of EMR data sets in the cloud environment.

Performance Evaluation and Implementation Result

In this section, security ofEHABE Scheme was experimentally analyzed and it enables to execute the arbitrary number of operations. The focus is mainly on performance metrics which related to security parameter, computation complexity and round complexity. The computation complexity is assessed on the basis oftime's basic operations that must be executed. The round complexity is based on quantifies the requirement for establishment between the Doctor and Patient.To the concern based on the performance, lengths of cipher text don't depend on the function complexity that is assessed over the encrypted data. The computational time depends straightly on the amount of operations performed. Therefore, the method is unrealistic for various applications, because cipher-text size and time of computation increases rapidly as expands the security level.To

Table 1. Comparison Table for HABE scheme

Technique	Access control	Efficiency	Computational Overhead	Encryption rate	Decryption rate	Policy	Based on	Collusion resistant
KP-ABE	Low, High if there is re encryptiontechnique	Average for broadcast typesystem	Most of computational overheads	Medium	Medium	AND, OR, threshold	KP-ABE	Good
CP-ABE	Average Realization of complexAccess Control	Not efficient for modern Medical record environments	Average computational overheads	Medium	Medium	AND, OR, threshold	CP-ABE	Good
HIBE	Lower than CP-ASBE	Better, Lower as compared toABE schemes	Most of computational overheads	High	High	AND, OR, threshold	IBE	Good
EHABE	Good Access control	Flexible and scalable	Some of overhead	High	High	AND, OR, threshold	HIBE and CP-ABE	Good

get 2k security, the cipher-text size and computation time are high-degree polynomials in k.

Let us consider m number of patient. The homomorphic encryption is implemented with single patient at a time while calculating x. Thus, the techniques requires m rounds for all the users to calculate x, additional round to decrypt x, its giving round complexity as *O (m)*. The computation complexity is assessed with respect to the basic mathematical operations for encryption and decryption. The performances of security parameter results that the keys and size of cipher-text, execution times are shown. The keys is *2n lg q* approximately of choosing 50 KB and a cipher text generated by homomorphic encryption algorithm is 2n lg q approximately of 96 KB. The generation of keys runs in 250 ms, encryption takes 26 ms, whereas time taken for decryption is17-38 ms depending upon mathematical operation performed in homomorphic encryption. Following Fig 2 andFig 3 illustrates the performance and security of our proposed system.

CONCLUSION

Efficient retrieval and access control of EMR data sets from cloud storage is achieved by utilizing the EHABE scheme offers the facilities are as follows (i) provides more security by resisting the unauthorized patient's attack (ii) Efficient encryption by reducing the time complexity and computation complexity and (iii) finally, fastest retrieval of encrypted data by using hierarchical level access based on EHABE scheme. The EHABE encryption technique provides the significant processin accessing the EMR data sets securely. EHABE scheme is guaranteed encryption technique in providing the security and access control to EMR data sets in the cloud environment.

REFERENCES

1. Guojun Wang, Qin Liu, JieWub, MinyiGuo,"Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", Jul 1, 2011.
2. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, 2010; pp. 261-270 .
3. V. Goyal, O. Pandey, A. Sahai, and B.Waters"Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, 2006; pp. 89-98.
4. D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing", Proceedings of CRYPTO 2001, LNCS 2139, pages 213–229, Springer-Verlag, 2001.http:// crypto.stanford.edu/~dabo/papers/ibe.pdf.
5. J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute-based encryption," in *Proceedings of IEEE Symposium on Security and Privacy*, 2007; **334**: pp. 321.
6. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, 2010; pp. 261-270.
7. G.Wang, Q. Liu, and J.Wu, "Hierachicalattibute-based encryption for fine-grained access control in cloud storage services," in *Proc. ACM Conf.Computer and Communications Security (ACM CCS)*, Chicago, IL, 2010.
8. Maha TEBAA, Saïd EL HAJJI and Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", Proceedings of the World Congress on Engineering 2012; **1** WCE 2012, July 4 - 6, 2012, London, U.K.
9. L. Xiao, O. Bastani, and I.-L.Yen, "An efficient homomorphic encryption protocol for multi-user systems."
10. Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" *IEEE Transactions on Information Forensics andSecurity*, 2012; **7**(2).
11. Q. Liu, C. C. Tan, J. Wu, and Guojun Wang, Reliable re-encryption in unreliable clouds," in *Proceedings of the IEEE Global Telecommunications Conference*, 2011; pp. 1-5.
12. Q. Liu, G. Wang, and J. Wu, "Time-based proxy reencryption scheme for secure data sharing in a cloud environment," *Information Sciences.In Press*, 2012.
13. C. Gentry, "Fully homomorphic encryption using ideal lattices", in Proceedings of the 41st ACM Symposium on Theory of Computing STOC 2009, ACM, New York (2009), 169-178.
14. Youssef Gahi, MouhcineGuennoun and Khalil El-Khatib, "A Secure Database System using Homomorphic Encryption Schemes", *DBKDA 2011: The Third International Conference on*

Advances in Databases, Knowledge, and Data Applications, ISBN:978-1-61208-115-1.

15. R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, 1978; **21**(2): pp. 120–126.
16. C. A. Melchor and P. Gaborit, "A Fast Private Information Retrieval Protocol", ISIT 008, pp. 1848-1852, Toronto, Canada, July 6 - 11, 2008.
17. Y. Zheng, "Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption", PhD thesis, Worcester Polytechnic Institute, 2011.
18. S. M¨uller, S. Katzenbeisser, and C. Eckert, "Distributed attribute based encryption in Information Security and Cryptology", pp. 20–36, Springer, 2009.
19. HeenaKharcheand Deepak Singh Chouhan, " Building Trust In Cloud Using Public Key Infrastructure", *International Journal of Advanced Computer Science and Applications*, 2012; **3**(3).
20. D. Stehl_e, R. Steinfeld, K. Tanaka, and K. Xagawa, "E_cient public key encryption based on ideal lattices". In M. Matsui, editor, ASIACRYPT, volume 5912 of Lecture Notes in Computer Science, pages 617-635 Springer, 2009.
21. http://www.nccs.res.in/Libofml.html
22. S.SeenuIropia&R.Vijayalakshmi, "decentralized access control of data stored in cloud using key policy attribute based encryption", *International Journal of Inventions in Computer Science and Engineering"*, 2014; **1**(2).
23. A.Kanimozhi&S.Rinesh, "STORAGE OF SCALABLE DATA SHARING USING SECRET KEY CRYPTOGRAPHY", *Journal of Recent Research in Engineering and Technology (JRRET)*, 2015; **2**(3).