International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 07 | July - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Efficient CP-ABE scheme for Privacy of PHR Based on OBDD Access Structure

Amol G Shendre
Dept. of Computer Sci. & Engg
Priyadarshini Bhagwati College of Engineering
Nagpur, India

Archana A. Nikose
Dept of Comp. Sci & Engg.
Priyadarshini Bhagwati College of Engineering
Nagpur, India

Abstract **— We have implement efficient CP-ABE scheme for Privacy of PHR Based on OBDD Access Structure with the advancement of information and communication technology (ICT), the medical sector is undergoing a massive transformation. Health records are being digitized, stored remotely in the cloud and shared with different stakeholders. However, the use of the cloud for personal health record (PHR) storage presents data security and privacy challenges. Ciphertext-policy attribute-based encryption (CP-ABE) is being widely studied for ne-grained access control of PHRs in the cloud. Expressiveness, efficient and attribute access, among others, are some key requirements of a cloud based health systems. it is based on the expressive and non-restrictive ordered binary decision diagram (OBDD) access structure, and it securely outsources the computationally demanding attribute operations of both encryption and decryption processes without requiring a dummy attribute. Security analysis shows that the CESCR scheme is secure in the selective model. Simulation and performance comparisons with related schemes also demonstrate that the CESCR scheme is expressive and efficient**

I. INTRODUCTION

The rapid development of information and communication technologies, in particular, the internet of things (IoT), wireless technologies and cloud computing in recent years have paved the way for interconnection of medical resources enabling improved delivery of healthcare services for patients. Digitized or electronic health records (EHR) (sometimes referred to as PHR) can now be collected from patients and sent to the cloud for analysis, diagnosis and sharing with different healthcare stakeholders. There are two variants of ABE, Ciphertext-policy attribute-based encryption (CP-ABE) .In CP-ABE, the Ciphertext is labeled with an access policy allowing the data owner to specify which users have access to his/her data while the user's key is associated with a set of attributes.

As fascinating as it may be, there are still several concerns that need to be addressed for its total acceptance. In particular, the use of third party servers for data storage presents privacy and security issues which are increasingly

Becoming the biggest concern in collaborative health systems. Adoption of the traditional access control techniques can be used to address the data privacy and security concern in collaborative health. However, these techniques only allow coarse-grained access policies which are not ideal for scalable environments.

II. PROPOSED SCHEME

In this study, I focused on addressing the privacy issues of PHR in cloud based health systems. We proposed and constructed an expressive, efficient and access control for ne-grained access to health data based on OBDD access structure. In our construction, we leveraged attribute roups and assigned version numbers to Ciphertext and user keys to achieve attribute/user access while preventing collusion between revoked and non-revoked users. Their proposed system utilizes the smart home environment to gather health information which is then sent to the cloud for analysis.

CPABE schemes are alternatively classified into "bounded" and "unbounded" schemes. In "bounded" schemes, the total number of attributes in the attribute space is fixed during setup and is polynomially bounded in the security parameter. The bounding of the size of the attribute universe can have

undesirable effects on systems deploying ABE schemes. A smaller bound might result in the system exhaustion and a need for complete rebuilding when expansion is required. For example, consider the scenario in which the patient suffering from the heart disease is being treated by a doctor in hospital H-A. In a smaller bound ABE scheme deployment, the attribute universe leveraged for encryption and user key generation can be set as {hospital, department, and profession}. However, at a later time, if the patient requires her data to be accessed only by experienced doctors, a new attribute "experience" might be introduced. In this bounded setting, to generate parameters associated with the "experience" attribute, the system will have to be completely rebuilt and additional expenses are incurred to re-encrypt all the ciphertexts. On the other hand, a larger bound might result in inefficient use of system resources as some parameters might be redundantly stored.

I have developed this system to perform this operations on programmatically to applying the instructions for converting the PHR file text on ciphertext using follow the procedure of CPABC to collect the attributes from user with the selected policy . Input attributes used for developed the salt to used for converted the ciphertext. The next procedures to reduced the ciphertext I have again convert this cipher text into binary form to implement the OBDD scheme.

As , I explained before OBDD scheme perform operation to replace the common node with single node, the same procedure , I have set this binary code in linked list tree array and as follow the OBDD algorithm checked the each and every node in array. In this operation I have checked the each and every array cell having parent node and their child node and having bit node. Similarly, matching the other cell node data with each other if any cell node having the same value in the tree array than I have delete one of the cell and maintain only one node in the array tree.

To follow the OBDD procedure on each level of tree array we get the filtered the fine grained binary value. Now I again reverse the binary string into the character ciphertext and stored into the file and download from the application. The above operation performs large ciphertext effectively reduced the ciphertext which is more less in the size to share with any desirable medium and safe and secure from break or corrupt the encryption.

III. RELATED WORK

KENNEDY EDEMACU, BEAKCHEOL JANG , AND JONG WOOK KIM , (Member, IEEE) This work was supported in part by the National Research Foundation of Korea through the Basic Science Research Program, Ministry of Education, under Grant NRF-2017R1D1A1B03028097 and in part by Institute of Information and Communications Technology Planning and Evaluation (IITP) grant funded by the Korea government (MSIT) (A Research on Safe and Convenient Big Data Processing Methods) under Grant 2018-0-00269. With the advancement of information and communication technology (ICT), the medical sector is undergoing a massive transformation. Health records are being digitized, stored remotely in the cloud and shared with different stakeholders.

A. Sahai and B.Waters, ``Fuzzy identity-based encryption We introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity. Identity-Based Encryption (IBE) allows for a sender to encrypt a message to an identity without access to a public key certificate.

John Bethencourt, Amit Sahai, Brent Waters In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques

In addition, we provide an implementation of our system and give performance measurements. We use the attribute group approach to achieve the attribute/user revocation in our work. Additionally, the ciphertexts and private keys are assigned version numbers to prevent the revoked group members from colluding with non-revoked members. Security and efficiency analysis show that our proposed scheme is secure, expressive and efficient. In this study, we focused on addressing the privacy issues of PHR in cloud based health systems. We proposed and constructed an expressive, efficient and revocable access control for ne-grained access to health data based on OBDD access structure. In our construction, we leveraged attribute roups and assigned version numbers to Ciphertext and user keys to achieve attribute/user access while preventing collusion between revoked and non-revoked users. Their proposed system utilizes the smart home environment to gather health information which is then sent to the cloud for analysis. Apart from the mentioned issues, expressiveness is another important issue to consider in attribute-based access control schemes. Several existing schemes support restrictive and monotonic access structures which are less expressive. A more

expressive and non-restrictive access structure is the OBDD access structure and it can represent any non-monotonic Boolean formula. In this study, we address the security and privacy concerns in collaborative health by proposing CESCR scheme. In CESCR, we simultaneously address the issues of attribute/user revocation, user collusion, unboundedness, expressiveness and efficiency. We provide a comprehensive security analysis, and simulation and performance evaluation for the CESCR scheme. The security analysis and the simulation and performance evaluation results show that CESCR is secure and efficient for sharing of health data in collaborative health systems.

In this study, we focused on addressing the privacy issues of PHR in cloud based health systems. We proposed and constructed an expressive, efficient and revocable access control for ne-grained access to health data based on OBDD access structure. In our construction, we leveraged attribute roups and assigned version numbers to Ciphertext and user keys to achieve attribute/user access while preventing collusion between revoked and non-revoked users. Their proposed system utilizes the smart home environment to gather health information which is then sent to the cloud for analysis.

III PROPOSED METHODOLOGY

In this study, I have focused on addressing the privacy issues of PHR in cloud based health systems. We proposed and constructed an expressive, efficient and revocable access control for ne-grained access to health data based on OBDD access structure. In our construction, we leveraged attribute roups and assigned version numbers to Ciphertext and user keys to achieve attribute/user access while preventing collusion between revoked and non-revoked users. Their proposed system utilizes the smart home environment to gather health information which is then sent to the cloud for analysis.

ABE schemes are alternatively classified into "bounded" and "unbounded" schemes. In "bounded" schemes, the total number of attributes in the attribute space is fixed during setup and is polynomially bounded in the security parameter. The bounding of the size of the attribute universe can have undesirable effects on systems deploying ABE schemes. A smaller bound might result in the system exhaustion and a need for complete rebuilding when expansion is required. For example, consider the previous scenario in which the patient suffering from the heart disease is being treated by a doctor in hospital H-A. In a smaller bound ABE scheme deployment, the attribute universe leveraged for encryption and user key generation can be set as {hospital, department, profession}. However, at a later time, if the patient requires her data to be accessed only by experienced doctors, a new attribute "experience" might be introduced. In this bounded setting, to generate parameters associated with the "experience" attribute, the system will have to be completely rebuilt and additional expenses are incurred to re-encrypt all the ciphertexts. On the other hand, a larger bound might result in inefficient use of system resources as some parameters might be redundantly stored. Meanwhile, in the "unbounded" schemes, the total number of attributes in the attribute space is not bounded during setup and can expand exponentially.

IV. PRELIMINARIES

In this section, we summarize the dentations of access structure, security complexity assumption, OBDD and bilinear maps which are adapted for use in our construction. A. ACCESS structurednation 1 (Access Structure): Access structures are for-mal representations of access policies. There are numerous access structures being used in ABE today such as; LSSS [7], AND-gates [12], threshold gates [2], [3], OBDD [8], etc.In relation to OBDD access structure (which is of interesting this work), an access structure is a rule R that satires a given set of attributes S, i.e., 1 is returned if S satisfies R (S = R). Otherwise 0 is returned.

B. BILINEAR MAPS

Definition 2 (Bilinear Maps): Let, G and GT be twoMultiplicative cyclic groups of prime order p, and g be theGenerator of G. A bilinear map e is dammed as e V G X G -> GT and should satisfy the following conditions.

1) Bilinearity, i.e., e(ga , gb) = e(g; g)ab for all a and b.

2) Non-degenerate, i.e., e(g; g) $\neq$ 1.

3)and is computationally feasible.

C. OBDD access structure

A Boolean function can be represented as a rooted, directed, acyclic graph, which consists of several (decision) nodes and two terminal nodes. The two terminal nodes are labeled 0 (FALSE) and 1 (TRUE). Each (decision) node {\display style u}u is labeled by a Boolean variable {\display style x_{i}}x_{i} and has two child nodes called low child and high child. The edge from node {\display style u}u to a low (or high) child represents an assignment of the value FALSE (or TRUE, respectively) to variable {\display style x_{i}}x_{i}. Such a BDD is called 'ordered' if different variables appear in the same order on all paths from the root. A BDD is said to be 'reduced' if the following two rules have been applied to its graph: Merge any isomorphic sub graphs. Eliminate any node whose two children are isomorphic.

In popular usage, the term BDD almost always refers to Ordered Binary Decision Diagram (OBDD in the literature, used

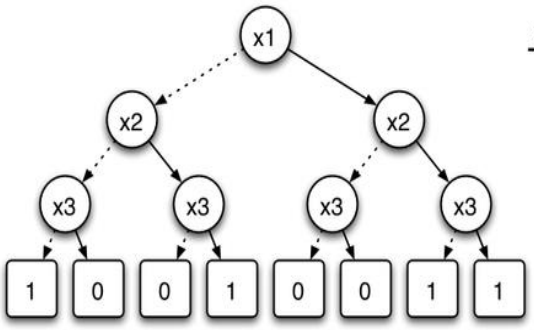
when the ordering and reduction aspects need to be emphasized). The advantage of an OBDD is that it is canonical (unique) for a particular function and variable order.[1] This property makes it useful in functional equivalence checking and other operations like functional technology mapping.

A path from the root node to the 1-terminal represents a (possibly partial) variable assignment for which the represented Boolean function is true. As the path descends to a low (or high) child from a node, then that node's variable is assigned to 0 (respectively 1).

Example:

The left figure below shows a binary decision tree (the reduction rules are not applied), and a truth table, each representing the function {\display style f(x1, x2, x3)}{\display style f(x1,x2,x3)}. In the tree on the left, the value of the function can be determined for a given variable assignment by following a path down the graph to a terminal. In the figures below, dotted lines represent edges to a low child, while solid lines represent edges to a high child. Therefore, to find {\display style f (0, 1,1)}{\display style f(0,1,1)}, begin at x1, traverse down the dotted line to x2 (since x1 has an assignment to 0), then down two solid lines (since x2 and x3 each have an assignment to one). This leads to the terminal 1, which is the value of {\display style f (0, 1, 1)}{\display style f(0,1,1)}.

Another notation for writing this Boolean function is {\display style {\bar {x}}_{1}{\bar {x}}_{2}{\bar {x}}_{3}+x_{1}x_{2}+x_{2}x_{3}}{\display style {\bar {x}}_{1}{\bar {x}}_{2}{\bar {x}}_{3}+x_{1}x_{2}+x_{2}x_{3}}.



x1	x2	x3	f
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Binary decision tree and truth table for the function {\display style f(x_{1},x_{2},x_{3})=(\neg x_{1}\wedge \neg x_{2}\wedge \neg x_{3})\vee (x_{1}\wedge x_{2})\vee (x_{2}\wedge x_{3})}{\display style f(x_{1},x_{2},x_{3})=(\neg x_{1}\wedge \neg x_{2}\wedge \neg x_{3})\vee (x_{1}\wedge x_{2})\vee (x_{2}\wedge x_{3})}, described in notation for Boolean operators.

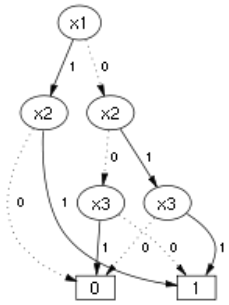


Fig.1 BDD for the function f

An OBDD can be represented even more compactly, using complemented edges.[2][3] Complemented edges are formed by annotating low edges as complemented or not. If an edge is complemented, then it refers to the negation of the Boolean function that corresponds to the node that the edge points to (the Boolean function represented by the BDD with root that node). High edges are not complemented, in order to ensure that the resulting OBDD representation is a canonical form. In this representation, OBDDs have a single leaf node, for reasons explained below.

Two advantages of using complemented edges when representing BDDs are: computing the negation of a BDD takes constant time space usage (i.e., required memory) is reduced

A reference to a BDD in this representation is a (possibly complemented) "edge" that points to the root of the BDD. This is in contrast to a reference to a BDD in the representation without use of complemented edges, which is the root node of the BDD. The reason why a reference in this representation needs to be an edge is that for each Boolean function, the function and its negation are represented by an edge to the root of a BDD, and a complemented edge to the root of the same BDD. This is why negation takes constant time. It also explains why a single leaf node suffices: FALSE is represented by a complemented edge that points to the leaf node, and TRUE is represented by an ordinary edge (i.e., not complemented) that points to the leaf node.

For example, assume that a Boolean function is represented with a BDD represented using complemented edges. To find the value of the Boolean function for a given assignment of (Boolean) values to the variables, we start at the reference edge, which points to the BDD's root, and follow the path that is defined by the given variable values (following a low edge if the variable that labels a node equals FALSE, and following the high edge if the variable that labels a node equals TRUE), until we reach the leaf node. While following this path, we count how many complemented edges we have traversed. If when we reach the leaf node we have crossed an odd number of complemented edges, then the value of the Boolean function for the given variable assignment is FALSE, otherwise (if we have crossed an even number of complemented edges), then the value of the Boolean function for the given variable assignment is TRUE.

An example diagram of a OBDD in this representation is shown on the right, and represents the same Boolean expression as shown in diagrams above, i.e., {\displaystyle (\neg x_{1}\wedge \neg x_{2}\wedge \neg x_{3})\vee (x_{1}\wedge x_{2})\vee (x_{2}\wedge x_{3})}{\displaystyle (\neg x_{1}\wedge \neg x_{2}\wedge \neg x_{3})\vee (x_{1}\wedge x_{2})\vee (x_{2}\wedge x_{3})}. Low edges are dashed, high edges solid, and complemented edges are signified by a "-1" label. The node whose label starts with an @ symbol represents the reference to the BDD, i.e., the reference edge is the edge that starts from this node.

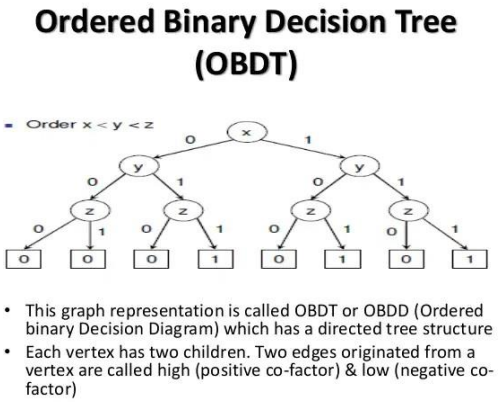
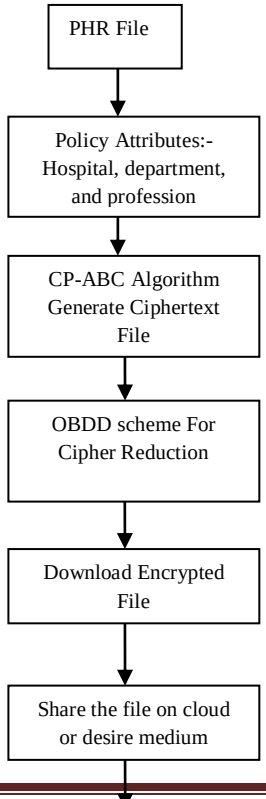
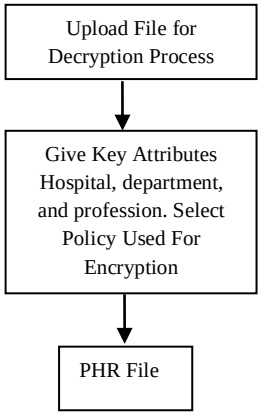


Fig.2 OBDD Access Structure

V SYSTEM ARCHITECTURE AND FLOW DIAGRAM





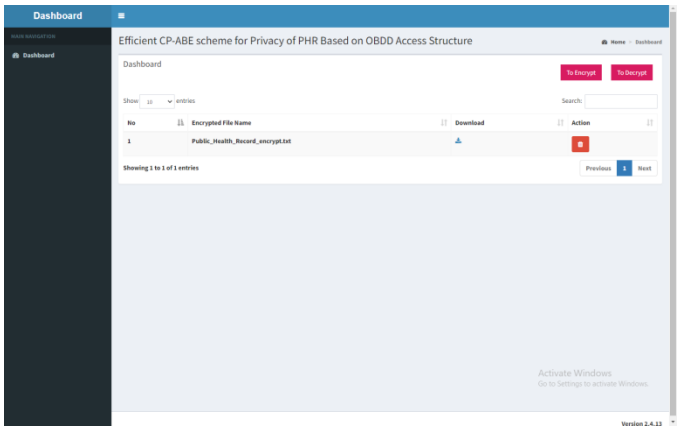
I have using sample physical health records to encrypt and decrypt using cp abc algorithm and reduced the generated cipher on applying OBDD access structure. In this module I have uploaded the PHR (physical health record) in text format file for encryption and then taking three attributes to use for generating the cipher. Similarly, I have given a three option for choose the policy to encrypt the file. Using input attributes and default salt cipher I have follow the cpabc algorithm to create the encrypted text than call the OBDD function to reduced the cipher text and stored the end result on another file. The encrypted file can directly download after the process or option present in the main dashboard. Now you can share this file on cloud server or mail to others or any available medium to desired user.

For the decryption process you need to again upload this encrypted file to the decryption module with the same attributed used for encryption. I have added the validation for correct attributes pattern and scheme selection.

The system checked the attribute and if given attribute satisfied the encryption attributed than encrypted file decrypted and directly downloaded with the system.

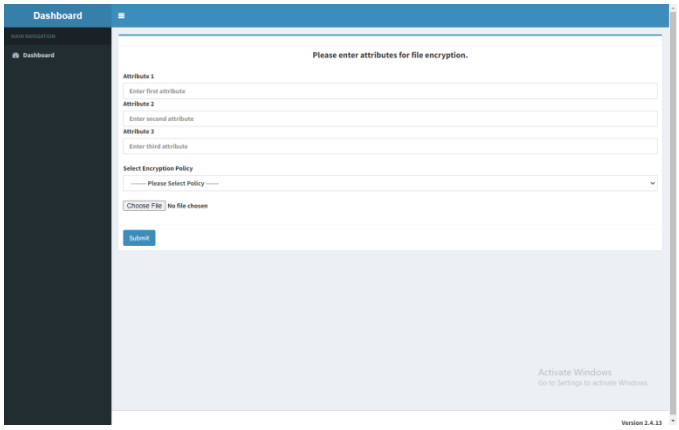
In this study, I focused on addressing the privacy issues of PHR in cloud based health systems. We proposed and constructed an expressive, efficient and revocable access control for ne-grained access to health data based on OBDD access structure. In our construction, we leveraged attribute roups and assigned version numbers to Ciphertext and user keys to achieve attribute/user access while preventing collusion between revoked and non-revoked users. Their proposed system utilizes the smart home environment to gather health information which is then sent to the cloud for analysis.

B. THE PROPOSED ACCESS CONTROL SCHEME In order to achieve expressiveness and efficiency with revocation, our proposed access control scheme possesses the following modules.



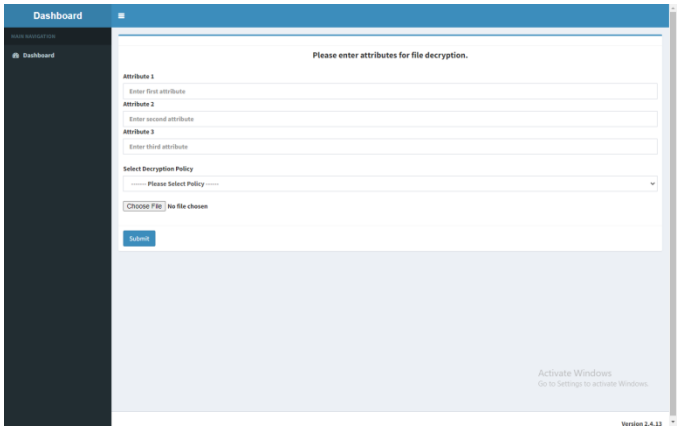
Main dashboard module to give two buttons on top right layout. Similarly the list of encrypted file to download for share to desired users.

Fig. 3 SYSTEM ARCHITECTURE



The below module is developed for encryption the files using CP-ABC algorithm taking three attributes and choose the required policy. On same process the upload file option available in below module taking PHR text file.

The below image is decryption process you need to again upload this encrypted file to the decryption module with the same attributed used for encryption. I have added the validation for correct attributes pattern and scheme selection. The system checked the attribute and if given attribute satisfied the encryption attributed than encrypted file decrypted and directly downloaded with the system.



Below image shown the encrypted cipher text in text file. This file are directly download and also avilabel in the decryption table .

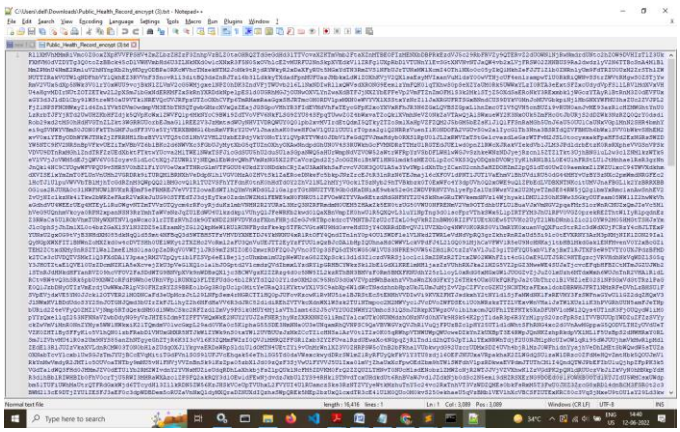


Table 2. Computation comparison of CP-ABE schemes.

*Multi, Expo and Pair represent the multiplication, exponentiation and pairing operations, respectively. DO is data owner and DU is data user.

VI CONCLUSIONS

In this study, we focused on CP-ABE scheme addressing the privacy issues of PHR in cloud based health systems. We proposed and constructed an expressive, efficient and access control for fine-grained access to health data based on OBDD access structure.

To solve computational burden on both the data owner and data users is linear with the number of attributes in the Ciphertext. To address these inadequacies, we propose CESCR, a CP-ABE for efficient and secure sharing of health data in collaborative health systems.

In this work, we focused on addressing data privacy and security concerns in collaborative health systems. We proposed the CESCR scheme, which is a CP-ABE scheme whose main ingredients are, immediate attribute/user access, unboundedness, expressiveness, efficiency, and collusion resistance. We adapted the attribute group approach to address the immediate attribute/user access issues and bind the keys to the user identities to prevent collusion between data users. OBDD access structure was used to achieve expressivessness. A novel technique that limits the attribute elements in the Ciphertext to only those associated with attribute group keys was proposed to achieve unboundedness and improved efficiency. The CESCR scheme further securely outsources the computationally demanding attribute operations in both encryption and decryption to the cloud without requiring a dummy attribute. We performed extensive security and performance analysis of the scheme in comparison with related CP-ABE schemes and the results show that the CESCR scheme is expressive, unbounded, secure, and efficient in comparison with the related CP-ABE schemes. The addition of traceability through the use of block chain technology and policy hiding are interesting future considerations.

VII REFERENCES

[1] A. Sahai and B.Waters, Fuzzy identity-based encryption," in Proc.Annu. Int. Conf. Theory Appl Cryptograph. Techno. 2005, pp. 457473

[2] J. Bettencourt, A. Sahai, and B.Waters, Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Secur. Privacy, Berkeley, CA, USA, May 2007, pp. 321334.

[3] V. Goyal, O. Pandey, A. Sahai, and B.Waters, ``Attribute-based encryption for ne-grained access control of encrypted data," in Proc. 13th ACMConf. Comput. Commun. Secur. (CCS), 2006, pp. 8998.

[4] 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 Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131143, Jan. 2013.

[5] Y. S. Rao, ``A secure and efcient ciphertext-policy attribute-based sign cryption for personal health records sharing in cloud computing," Future Gener. Comput. Syst., vol. 67, pp. 133151, Feb. 2017.

[6] A. Michalas and N. Weingarten, Health Share: Using attribute-base encryption for secure data sharing between multiple clouds," in Proc. IEEE 30th Int. Symp. Comput.-Based Med. Syst. (CBMS), Jun. 2017, pp. 811815.

[7] Y. Zhang, D. Zheng, and R. H. Deng, ``Security and privacy in smar health: Efcient policy-hiding attribute-based access control," IEEE Inter- net Things J., vol. 5, no. 3, pp. 21302145, Jun. 2018.

[8] L. Li, T. Gu, L. Chang, Z. Xu, Y. Liu, and J. Qian, A ciphertext-policy attribute-based encryption based on an ordered binary decision diagram IEEE Access, vol. 5, pp. 11371145, 2017.

[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 Med. Inform. Decis. Making, vol. 7, no. 1, p. 25, 2007.

[10] J. Hur and D. K. Noh, Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 12141221, Jul. 2011.

.