A Privacy Preserving System for Protecting Cloud Based Health Care Records Using Fine Grade Access Techniques

P.S.G. Aruna Sri¹, M. Anusha², K. Kiran Kumar³ and S. Sridevi⁴

¹Associate Professor, Department of ECM, Koneru Lakshmaiah Education Foundation. Vaddeswaram, Guntur, Andhra Pradesh, India
²Associate Professor, Department of CSE, Koneru Lakshmaiah Education Foundation. Vaddeswaram, Guntur, Andhra Pradesh, India
³Professor, Department of CSE, Koneru Lakshmaiah Education Foundation. Vaddeswaram, Guntur, Andhra Pradesh, India
⁴Assistant Professor, Department of ECM, Koneru Lakshmaiah Education Foundation. Vaddeswaram, Guntur, Andhra Pradesh, India

Email: arunasri_2012@kluniversity.in

Abstract. Protection of privacy has also received increasing attention in many fields, mainly in the sense of the Individual Health Record (IHR), as cloud computing has become an essential activity in the real world. Traditional encryption of the cypher text policy (CP-ABE) allows you to track the scrambled PHR information policy in a fine-grained fashion. Still, with the cypher text, the access policy is also sent. However, the entry policy does not allow users to be anonymous, as a considerable amount of sensitive information from legitimate users of the app is needed. It is now necessary to protect users’ privacy by hiding access methods. The vast majority of previous plans, however, have to address two problems: the first problem is that specific plans do not embrace a broad universe of attributes, so their common sense in PHR is dramatically reduced, and the second is that the decryption cost is very high because the entry mechanism is set up in the cypher paper. This dramatically reduces their usefulness as a result. To solve these issues, we are constructing a CP-ABE plot with sufficient decryption, where together the size of the available limits and the cost of decryption is endless. Also, using the dual system encoding technique, we show that the proposed conspiracies achieve optimum protection in the basic model.

1 Introduction

Cloud storage is a fast and effective solution as the recent trend towards knowledge sharing and a mountain of data access across the network. For example, the patient does not have to forward several paper copies of the test systems into the personal health record system to decide how the patient is treated traditionally. However, only by transfer of his or her health record to the PHR system can the health record be kept and shared. A patient is tracked absolutely [2],[3],[7], making it easy to open up privacy, as specific access structure characteristics transmit legitimate user identity data as a matter of urgency. In the access policy of the patient [8],[15], PHR should include such sensitive features as cardiologists, focal clinics and so on. Therefore, regardless of whether the unsubscribed client can decode efficiently, it can also be understood by the simple content layout in the Access Policy that the encrypter has a particular disorder. In[16], HC-ABE was implemented where the form of cypher text entry was integrated into the cypher text and was not legally submitted. In
addition, in [12][16][14], a number of secret plans for the CP-ABE were eventually proposed. In such scenarios, access mechanisms should be specified only in positive, negative and unique circumstances concerning AND doors or AND exits.

This leads to 2 pitfalls. Initially, at the same time as the number of attributes, the size of society parameters increases and, additionally, the cost of decryption increases considerably. Some low overhead plans are seen in the above downsides in[13],[14] and the standard technique obtained by these plans is to present a decryption test before decryption with the inclusion of any excess components in the cypher text. While the above methods speed up the decryption speed, the cypher’s text duration is now completely increased, and this will be another bottleneck eventually. The Diffie-Hellman Decision Test prototypes (DDH-Test) are, however, extremely indefensible [9][10][13].

To rapidly extend online and cloud computing, a mountain range of intelligent medical devices has recently been developed. Access control methods are also provided alongside chip text in the previous instrument-based cryptographic attribute, making it easy to recognise sensitive user data in the scheme. Basic features transmit even more important data in the access process in the case of PHR, such as: the recurrence of patients and their family history of genetic diseases due to the service ‘s patient surveillance, etc.

**Access Structure:** There are two sections for each attribute in this document, the attribute name file and the function value. And, there are several candidate predictions for each feature. Each descriptor generates its own recognition of name files and attributes. Besides, in the Access Policy, estimates of the attributes defined by the encrypter are secret and not text-based. Using only the access grid and the specified $\beta$ power, you can decrypt the cypher text. Besides, the proposed proposal would cover any access control scheme that is expressed as a straight-line mystery sharing arrangement.

**Quick decryption:** Of course, it is difficult for a client to know if a cypher text access policy is compliant with the encrypter's access policy. As a result, to determine whether or not it is precise, decryption must produce a bunch of equations. We are introducing a successful Secret Cipher text Policy Attributes-Based Encryption creation that facilitates easy decoding, reducing the number of bilinear combination tests to a consistent decoding level.

**Data verifiability:** Two functional problems can historically be found in a list of previous proposals. One is the degree to which public parameters evolve directly on the scale of the universe. The other is that, due to the lack of an apparent reference to the argument, the authorised customer does not determine whether or not the message he has sent is necessary. The size of the public parameters, however, is logical in the proposed conspiracy, so that the universe of attributes in this technique will be infinite, and it also encourages the acceptance of undescribed documents that will allow unwavering decryption. Also, by using dual device encryption technologies, we demonstrate the complete security of the proposed plot in the standard model under static suspicion [1][10-12].

### 2. Literature Review

B. Waters, here is another method to use what we call dual encryption schemes to illustrate the usefulness of the encryption mechanism. The procedures based on Bilinear-Hellman and Linear decisions are simple and conclusive and allow Identity Based Encryption and Hierarchical Identity Based Encryption (IBE) systems to be fully stable. A number of selection elements with encrypted text, private keys and public parameters are included in our IBE process. These results are the first HIBE and the first IBE system with short, simple parameters. For both text cyphers and private keys, one of the two unrecognized structures may be used in dual device encryption. In case of isolation from the crucial era or calculation of device encryption, a private key or chip text is standard. These keys and the IBE device cypher text will act as planned. We define text keys in the same way in seminal and cypher. A private semi-utilitarian key would allow the deciphering of all the frequently produced encrypted texts. The decryption would be easy if a semi-practical cypher is
attempted with a semi-useful private key. In addition, only conventional private keys can be decrypted by semi-practical cypher documents.

*M. Qutaibah, S. Abdullatif, C.T. Viet, However, we are dealing with the problem of cryptographic crude fine-cutting, which has a range of sound applications, such as pay T.V., eHealth, cloud storage, etc. Ciphertext-based attribute control for encryption. In this sense, by broadening the previous work of Hohenberger and Waters in PKC’13 and proposing a development that achieves the size of the Boolean access equation on the basis of its size and the number of its provisions, we improve past LSSS-based procedures. Furthermore, our development supports fast decryption. In addition, two exciting expansions are recommended: the first is to use a cloud administrator to help minimize capacity, calculation, and lightweight resources. The second indicates that the use of various experts moderates the main power supply.*

*B. In the standard model, which needs cement and non-intuitive cryptographic assumptions, we have an additional Cipher Text-Article Policy Encryption (CP-ABE) method. Our responses allow any encrypter to imply access control over any access reception attributes of the device. Cipher text format, encryption and decryption timescales with the complexity of the control recipe, directly in our most proficient process. In the non-exclusive selection model, evidence has been the key work carried out in the past to reach these requirements. We are proposing three evolutions in our system. On the premise that we call the definitive Parallel Bilinear Diffie-Hellman Exponent (PBDHE), speculation of BDHE scepticism, the first scheme is clearly shown to be stable. We are now entering into implementation agreements to achieve specified protection individually, in line with the (more fragile) Bilinear Diffie Hellman Exponent and the Bilinear Diffie Hellman Provincial Topics.*

**J. Lai, R.H. Deng, Y. Li** ABE (attribute-based encryption) theory was used. ABE provides one-to-many encryption solutions for the public key and is considered to be a versatile cryptographic crude for multifunctional and fine-grain access control systems development. There are two forms of ABE plans[1], main policy plans for ABE (KP-ABE) and cypher text policies for ABE (CP-ABE). This study deals with our fears.

*A. Sahai, Yeah, and B. We are introducing another form of IDE framework called the Fuzzy ID-based method of encryption. In Fuzzy IBE, identity is seen as a set of elucidating characteristics. The Fuzzy IBE scheme allows a single person to encrypt an identity-enclosed ciphertext, if and only if the "alien" and "alien" features are identical to each other as specified by the metric of the context set. By using biometric representations as characters, the Fuzzy IBE scheme can be used to encourage encryption; the error tolerance function of the Fuzzy IBE scheme is accurate and enables the use of biometric identities that will inevitably be altered when tested. We also demonstrate that Fuzzy-IBE can be used for an "Attribute-based Encryption" style of application. This paper introduces two developments on fuzzy IBE schemes. Our innovations can be thought of as encrypting a message's identity under a few (fuzzy) attributes. Attacks on intrigue are both blameless, open-minded and stable. In addition, random prophets are not part of our primary development. Under the Selective-ID protection model, we show the safety of our systems.*

**J. Bethencourt, A. Sahai, B. Waters, Consumers** will be able to access data in a few distributed schemes where the consumer is required to provide a particular certificate or quality system. The key approach to maintaining such plans now is to use a secure server to store data and track the link. In any event, the authentication of the data will be compromised if any device which extracts the data is compromised. In this article, we are implementing a full access control scheme for encoding data, which we call text-based cypher encryption based on attributes. The resources of the server are untrusted using our encoded data and our tactics are protected from plot attacks. Former device attributes used for encryption attributes are used to show broken information and synchronised approaches to the customer's keys. In contrast, the customer's credential is expressed in our device attribute, and the encoding data set decides who decrypts. In this way, by our strategies, we are closer to traditional access management policies, such as role-based access control (RBAC). Moreover, for our system, we have an installation and performance forecast.
3. Implementation methodology

The first CP-ABE scheme[7] was implemented where the cipher text was associated with the access method of the data holder, and the key was correlated with the attribute sets relevant to the user. As a result, several CPABE ways were suggested in [15], [11-12] and [13-100], but these schemes are useful for AND entries. Waters told an access system based on linear information sharing (LSSS) and a secure system built on the standard model[3] to make the access structure progressively descriptive. Besides, Yoneyama et al.[16] suggested a key CP-ABE idea with a secret entry method to protect user privacy. Access control policies are not explicitly conveyed in their function alongside ciphertext since no unauthorised client can acquire valuable data about the access system. With a similar presentation called Anonymous Cryption-based attributes, different scientists have suggested different strategies.

Figure 1: PHR cloud storage.

Under these schemes, cipher text instals the customer's mechanisms that comply with the access policy, and the customer can then decipher the text efficiently. Subsequently, the developers implemented another extremely successful mysterious CP-ABE scheme and presented security evidence according to Decision Modifying the Bilinear Diffie-Hellman Assumption (MBDH)[12]. Numerous initiatives have been launched in [9] and [14][12] to refine the vague CP-ABE system further. Scandalously, each of them has to face high decryption costs that could lead to their lack of profitability.

Hidden Ciphertext Policy ABE

The following four equations provide a secret CP-ABE scheme.

\[ \text{Setup} (\lambda) \rightarrow \langle \text{P.K.}, \text{MSK} \rangle: \text{This is a distributed computation that provides } \lambda \text{ security parameter details and gives P.K. The Public Criteria and MASKS.} \]

\[ \text{KeyGen} (\text{P.K.}, \text{MSK}, S) \rightarrow \text{SK}: \text{Public parameters P.K., the main key MSK and the attributes S are needed as information to estimate the key age. It provides private key clients affiliated with S.K.} \]

\[ \text{Encrypt} (\text{P.K.}, M, (A, in, T)) \rightarrow \text{CT}: \text{An encryption calculation takes the constructs of the P.K., M plaintext and T entry (A, in, T) as information as the public parameters and returns a C.T. cipher text, where T is a high-value attribute to and does not emit alongside C.T. With cipher text.} \]

\[ \text{Decode} (P.K., SK, CT) \rightarrow M: \text{This uses P.K., a secret S.K. Public Parameters Key, combined with attributes set to } S = (I.S., L.S.), \text{ offers the message M or a specific image to a client who has forgotten to unscrew the C.T. Text by the cypher.} \]
4. **Implementation of Defense**

Hidden key and substitution cypher

The same technique as Lai[5], known as dual encryption, is used in our security confirmation. From the outset, substitutional cypher and substitutional cypher keys will be identified. Both traditional cypher text and semi-functional cypher text can decrypt standard private keys, but a semi-functional cypher text can not decode a semi-functional private key. We have made it clear that in the whole process, SFC and SFK can not be used and can only be used in our proofs.

5. **Performance Analysis**

In the field of protection and efficiency, we will undertake a couple of studies of our scheme with past work [5], [8], [9] [16]. Table 1 offers extensive connexion with a variety of essential highlights, including public keys height, private key, ciphertexts, overhead decryption, bunch order, and access policy articulation and status. In this case, we can see that the keys are the same size as numerous works in our method, but the size of the cypher text is lighter than the ones suggested.

Moreover, only the system suggested, and the study in [8] endorse massive advances in the cosmos. Besides, our device can achieve a steady pairing in the decryption process, contrasting and the above job, which can incredibly enhance decryption performance.

![Figure2: Public parameter computing costs](image)
Figure 3: The ciphertext storage costs

Figure 4: Data consumers' overhead decryption

6. Conclusions

Throughout this article, we propose another technology called linear secret sharing which can enhance the access policy enormously. Furthermore, any attribute has two parts, in particular the name and meaning of the feature. The most apparent leeway in this context is that necessary evaluations of qualities may be covered. And in PHR it will provide consumers with strong protection. The scale of public parameters is comparable in the suggested scheme, and the cost of decryption is just 2 pairing jobs, which furthermore gradually minimize it to earth. Throughout the long run, we prove the complete protection of the method suggested by the use of the dual system encryption strategy in the regular model under static assumptions. It's just halfway hiding approach which the proposed scheme does. The dilemma, with quick encryption that is abandoned as a future job, is exciting and completes a secret agenda.
References

[1]. K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, “A cipher text-Policy Attribute-Based Encryption Scheme with Constant CiphertextLength,” in Infor. Secur.Prac., Experience—ISPEC (Lecture Notes in Computer Science), vol. 5451, F. Bao, H. Li, Eds. Berlin, Germany: Springer, Sep. 2009, pp.13–23.

[2]. Reddy P.R.S., Ravindranadh K. (2019), ‘An exploration on privacy concerned secured data sharing techniques in cloud’, International Journal of Innovative Technology and Exploring Engineering, 9(1), PP.1190-1198.

[3]. Pradeep Kumar V., Prakash K.B. (2019), ‘QoS aware resource provisioning in federated cloud and analysing maximum resource utilisation in agent based model’, International Journal of Innovative Technology and Exploring Engineering, 8(8), PP.2689-2697.

[4]. Prasad G.S., Praneetha D.L., Srivalli S., Sukes B.V. (2019), ‘Information security in cloud by using enhanced triple-DES encryption algorithm’, International Journal of Innovative Technology and Exploring Engineering, 8(5), PP.679-682.

[5]. Swami K.S., Sai Kiran P. (2018),’Identity based encryption (IBE) with outsourced abolishment in cloud computing’, Journal of Advanced Research in Dynamical and Control Systems, 10 (0), P.P. 762-770

[6]. Praveen S.P., Rao K.T., Janakiramaiah B. (2018),’Effective Allocation of Resources and Task Scheduling in Cloud Environment using Social Group Optimization’, Arabian Journal for Science and Engineering.43 (8), P.P. 4265-4272.

[7]. Rajeswari P., Viswanadha Raju S., Ashour A.S., Dey N. (2017),’Multi-fingerprint unimodel-based biometric authentication supporting cloud computing’,Studies in Computational Intelligence.660(),PP.469-485.

[8]. Vurukonda N., Trijan Kumar S., Rajasekhar Reddy J.V., Adithya A., Boddu S.B. (2018),’A secure attribute-Based encryption scheme in cloud computing’, International Journal of Engineering and Technology(UAE).7 (2), P.P. 90-92

[9]. K. V. Daya Sagar , P Sai Durga , G. Kavya , K Sri Sravya , K. Krishnaveni,”Mobile based home mechanization framework using IoT for smart cities”, International Journal of Engineering & Technology, 7 (2.7) (2018) 266-269.

[10]. K Sai Prasanthi , K.V.Day Sagar ,”Survey on secure protocols for data sharing through edge of cloud assisted internet of things”.International Journal of Engineering & Technology, 7 (2.7) (2018) 92-95.

[11]. K.V. Daya Sagar I, Ch Shyam Krishna, G. Lalith Kumar, P. Surya Teja, G. Charless Babu,”A Method for finding threatened web sites through crime data mining and sentiment analysis”.International Journal of Engineering & Technology.7 (2) (2018) 62-65.

[12]. A.Yasaswini, K.V. DayaSagar , K.SriVishnu,V.HariNandan, PVRD Prasadara Rao,”Automation of an IoT hub using artificial intelligence techniques”.International Journal of Engineering & Technology, 7 (2.7) (2018) 25-27.

[13]. K.V.Daya Sagar, M.Rupesh Chowdary,S.Mahesh,”Smart Crop Monitoring and Farming Using Internet of Things with Cloud”Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 02-Special Issue, 2018.

[14]. Rakeshshirsanth,Dr.K.V.Daya Sagar,”A Review of fine grained access control techniques”.International Journal of Engineering & Technology, 7 (2.7) (2018) 20-24.

[15]. K.V.DayaSagar,Dr.S.Narayana,Dr.K.RaghavaRao,G.Bhavya Deepika,M.SaiKiran Reddy.Developing Smart Kitchen Inventory tracking using Internet of Things,Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 02-Special Issue, 2018.