Attribute based Encrypted and Secured Cloud based Personal Health Record System

REDDY VEERAMOHANA RAO[1*], JETTI KUMAR RAJA [2], CHOLLA RAVINDRA RAMAN[3], PUJALA NANDA KISHORE [4]

[1,2,3,4] Department of CSE, Bapatla Engineering College, Bapatla, Guntur, Andhra Pradesh, India.
Corresponding Author Email: veeramohan.it65@gmail.com

ABSTRACT
As cloud computing has become an incredibly important task in real life, security of privacy in many areas, in especially in the context of Personal Health Record (PHR), has indeed been given growing attention. The traditional encryption based on ciphertext policy (CP-ABE) allows you to control the scrambled PHR information policy in a fine-grained manner, however the accessing policy is also sent with the cipher text. The entry policy, however, cannot activate the anonymity of users, as it includes an excessively large number of confidential information from valid users of software. It is now important to ensure the privacy of users through hiding access strategies. The overwhelming majority of previous plans however have to deal with two problems: (1) certain plans do not accept a wide universe of the attributes, hence their common sense in PHR is considerably reduced and (2) the decryption costs are very high because the entry scheme is set up in cypher text. Their utility is thus drastically limited. To resolve these problems, we create a CP-ABE plot with proficient decryption, where both the scale of available parameters and the cost of decryption are steady. In addition, by using the dual system encoding technique, we demonstrate that the proposed conspire achieves full safety in the standard model.

Keywords:
Cloud Computing, Personal Health Record (PHR), Hidden Policy, Fast Decryption Attribute-Based Encryption.

1. INTRODUCTION

Cloud infrastructure provides a quick and proficient solution as a late-growing advancement for the exchange of information properties and mountains of data connectivity through the network. For example , the patient doesn't need to transmit different paper versions of the test structures within the personal system of a health record system to determine how the patient is traditionally done, but only through the transfer of his or her own health record to the PHR system can store the health record and share it. A patient is fully controlled and can access these health information, such as companions, family or health care providers, by his own PHR records. In order to ensure precise access protection for PHR, data owners urgently need a kind of encryption that makes for a detailed control of access.

Hidden Ciphertext policy encryption attribute conspirator offers a good way of resolving the issue, where privacy protection is accomplished by hiding access control policies. However, in previous systems[2],[3],[7], access control policies are often sent unequivocally along with the chip text, making it easy to open up privacy, as specific access structure attributes convey legitimate user identity data urgently. PHR can include such sensitive characteristics such as cardiologists, focal clinics and so on in the access policy specified by a patient[8]. Therefore, regardless of whether an unsubscribed client can efficiently decipher, he can also grasp a simple content layout from the Access Policy that the encrypter has a certain disorder. HC-ABE was presented in [16] where the cyphertext entry mechanism was implanted into the ciphertext and was not legally submitted. In addition, in [17][19], some secret proposals for the CP-ABE were suggested gradually. In these plans, access mechanisms should be found only in positive, negative and special situations over AND doors or AND exits.

This leads to two pitfalls. Initially, the scale of public parameters increases concurrently with the number of attributes and, in comparison, the decryption costs are greatly increased. The above downsides present some low-overhead plans in [13], [14] and the standard strategy earned by these plans is to present a decryption test with the inclusion of any excess components in the ciphertext before the decryption. While the above plans increase decryption efficiency, ciphertext length is now completely increased and this will inevitably be a further bottleneck. Furthermore, the Diffie-Hellman decisional test (DDH-test) designs are unbelievably indefensible [9],[20].

A mountain amount of intelligent medical devices is recently designed with the rapid development of online and cloud computing. Be it as it might, access management techniques are frequently delivered alongside chip text in the past instrument-based cryptographic attribute, making it easy to identify confidential user data in the device. In PHR, specific characteristics communicate considerably more important details within the access procedure, for example: the beat recurrence of patients and their family history of genetic disorders as a result of patient's testing facilities examination data, etc.

Access structure: Every attribute throughout this paper has two parts, the name file of the attribute and its value for attribute. And there are multiple candidate projections for each attribute. Each decrytor just produces his own name file and recognition of an attribute. Furthermore, the estimates of the attributes defined by the encryptor in the Access Policy are hidden and not sent with the text. The ciphertext can be decrypted with only the access grid and specified β power. In addition, any access management scheme that is conveyed as a straight mystery sharing plan will be protected in the proposed plan.

Fast decryption: Of course, it is hard for a client to know that whether access policy relating to a ciphertext fulfils the access policy established by the encryptor. Therefore, a decryption has to render a bunch of estimates to select whether or not it is valid. We present an effective development of Hidden Ciphertext Policy Attributes-Based Encryption that supports fast decoding, in which the amount of bilinear combination evaluations are reduced to a consistent level of decryption.

Data verifiability: Typically two practical difficulties can be listed in many previous proposals. One is the scale of the rise of public parameters with the universe's scale directly. And the other is that the accepted client can not determine if the message he has sent is relevant or not because of the lack of an apparent link to the message. Nevertheless, the scale of public criteria in the suggested conspiracy is reasonable, so that the universe of attributes in this strategy will be infinite, and it also promotes the acceptance of unscrewed texts, which will boost the unwavering decryption. In addition, by using dual device encryption technologies, we demonstrate the complete security of the proposed plot in the regular model under static suspicion [1] [20] [21].

2. LITERATURE REVIEW

B. Waters, Here we are proposing another technique to illustrate encryption system reliability by using what we call dual system encryption. Our procedures are based upon the simple and conclusive Bilinear-Hellman and Linear decisional presumptions, and allow for a fully stable Identity Based Encryption and Hierarchical Identity Based Encryption (IBE) schemes. Our IBE framework has a variety of selection elements, each with ciphertexts, private keys and public parameters. Such results are the first HIBE system and the first IBE system with simple short parameters. Both ciphertexts and private keys can use one of two undefined structures in a dual system encryption method. In case of isolation from the key age or encryption measurement of the device, a private key or chiptext is common. This keys and ciphertexts will work in an IBE system as one hopes. Similarly, we describe seminal and ciphertext keys. A private semi-utilitarian key would have the option of decoding all ciphertexts frequently generated. In case of attempting to uncramble a semi-practical ciphertext with a semi-useful private key the decryption will be quick. In addition, only traditional private keys can be decrypted by semi-practical ciphertexts.

M. Qutaibah, S. Abdullatif, and C.T. Viet, However we struggle with the topic of fine-cutting cryptographic crude, which has a range of sound implementations such as pay TV, eHealth, Cloud Storage etc. Ciphertext regulation attribute-based cryption. In this sense we reinforce the past LSSS-based procedures by broadening the previous work of Hohenberger and Waters in PKC'13 and proposing a creation that achieves the size of the boolean access equation in the basis between its size and the quantity of its provisions. Furthermore, our creation supports fast decryption. Furthermore, we recommend two interesting expansions: the first is to minimize room, measurement and lightweight tools that use a cloud administrator to help. The second suggests the use to moderate the main power supply by various specialists.

B. Waters, We have an additional Ciphertext-Article Policy Encryption (CP-ABE) method in the standard model, which contains cement and non-intuitive cryptographic assumptions. Our responses allow any encrypter to signify access control over the device attributes of any access reception. Ciphertext format, encryption, and decryption timescales with the sophistication of the control recet directly in our most competent method. The key work undertaken in the past to attain these criteria has been an evidence in the non-exclusive selection model. Under our framework, we propose three innovations. The first scheme is clearly shown to be stable under the presumption that we call the decisory Parallel Bilinear Diffie-Hellman Exponent (PBDHE), a speculation of the BDHE scepticism. In line with the (more fragile) Bilinear Diffie Hellman Exponent and the Bilinear Diffie Hellman Provincial Topics, we are now making implementing agreements to achieve established protection individually.

J. Lai, R.H. Deng, and Y. Li, The principle of attribute-based encryption (ABE) has been implemented. ABE provides one to several encryption-based public key solutions and is known to be a versatile cryptographic crude for the development of multifunctional and fine grain access control systems. Two kinds of ABE plans[1] exist, ABE (KP-ABE) main policy plans and ABE (CP-ABE) ciphertext policy. This study is about our fear.

A. Sahai and B. Waters, We introduce another form of IDE scheme we are called the Fuzzy ID-based Encryption method. We see an identification in Fuzzy IBE as a set of elucidating characteristics. A Fuzzy IBE scheme facilitates the encoding of a ciphertext embedded with an identity, a single person if and only if the characteristics "alien" and alien "are similar each other as determined by the metric for the" context package. The Fuzzy IBE scheme can be used to motivate encryption using biometric representations as characters; the error tolerance function of a Fuzzy IBE scheme is precise and enables the use of biometric identities that will inevitably be upset any time it is tested. We also demonstrate that Fuzzy-IBE can be used for a form of application we call "attribute-based encryption." Two developments on fuzzy IBE schemes are presented in this paper. Our innovations can be considered to encrypt the identity of a message under a couple of (fuzzy) attributes. Intrigue attacks are both blamelessly open-minded and secure. In addition, random prophets are not included in our fundamental creation. Under the Selective-ID protection paradigm, we reveal the safety of our systems.

J. Bethencourt, A. Sahai, and B. Waters, A customer may have the ability to view data in a few distributed structures where a customer forces a certain credential or quality structure. The key approach for retaining such structures now is to use a reliable server to store the data and monitor the connexion. In any case, the authentication of the data will be compromised whenever any system that extracts the data is compromised. In this post, we introduce a method for full access control on encoded data, which we call ciphertext-based encryption based on attributes. Through using our encoded knowledge, the capability of the server is untrusted and our techniques are protected against plot attacks. Former system attributes used for encryption attributes to display broken details and synchronised approaches with the keys of the customer; while in our system attribute the credentials of the customer are represented, and the set of encoding data determines who can decode. In this way, we are closer to conventional access management policies, such as roles-based access control (RBAC), through our strategies. In addition, we provide our framework with an installation and efficiency forecasts.

3. IMPLEMENTATION METHODOLOGY

Very first CP-ABE scheme was introduced in [7] in which ciphertexts were associated with the data proprietors' access system, the key being associated with user-related attribute sets. Consequently, in [15], [17] and [18], a lot of CPABE strategies have been suggested, but, these schemes are beneficial to AND entries. Waters suggested an access system based on a linear information sharing (LSSS) and a established safe scheme in the regular model to make the access structure increasingly descriptive [3]. To protect the privacy of users in addition, Yoneyama et al . [16] suggested the key CP-ABE scheme with a framework of secret entry. In their job, access control policies are not unequivocally conveyed alongside ciphertext, as no unapproved customer can get helpful access framework details. Different scientists have suggested separate strategies with a common presentation, called Anonymous Cryption-based attributes.

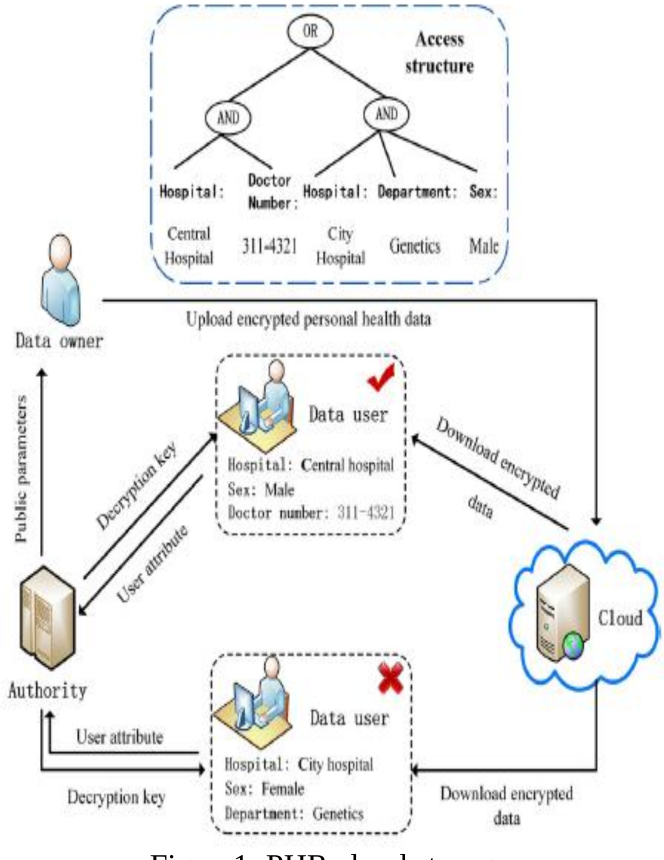

Figure1: PHR cloud storage.

Within those systems, ciphertext instals the customer's structures that fulfil the access policy, and the customer can then decipher ciphertext efficiently. The developers subsequently introduced another incredibly effective enigmatic CP-ABE scheme, and it was supplied with security proof pursuant to Decisionary changing the Bilinear Diffie-Hellman Presumption (MBDH)[20]. In [9] and [14], numerous projects were introduced to further develop the unclear scheme of the CP-ABE. Scandalously, each of them has to face high decryption costs, which might contribute to their lack of profitability.

Algorithm: Hidden Ciphertext Policy ABE

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

Setup (1λ) → (PK, MSK): This is a distributed computation which provides information on a security parameter *λ* and gives PK and MASKS the public parameters.

KeyGen(PK, MSK, S) → SK: The estimation of the key age requires the public parameters PK, the main key MSK and the attributes S as information. It offers SK-related private key customers.

Encrypt (PK, M, (A, ρ, T)) → CT: An encryption computation takes the PK, M plaintext and T entry constructs (A, ρ, T) as information as the public parameters and returns a ciphertext CT, where T is an attribute of great value to and does not emit alongside CT ciphertext.

Decode (PK, SK, CT) → M: This uses Public Parameters PK, a hidden SK key, combined with attributes set S = (IS, LS), as a details and provides the message M or an extraordinary picture $\perp$ a client who has forgotten to unscrew the CT cyphertext.

Security Implementation

Secret key and Semi-functional ciphertext

Our protection confirmation uses the same technique as Lai[5], which is known as dual encryption. We describe two semi-functional constructs from the outset, Semi-functional SFC and Semi-funtional SFK keys. The ordinary private keys can be decoded by both traditional ciphertexts and semi-functional ciphertexts, but a semi-functional private key can not screw off a semi-functioning ciphertext. We clearly made it known that SFC and SFK cannot be used in the actual method and only used in our proofs.

4. 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]. 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 ciphertext is lighter than the ones suggested.

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

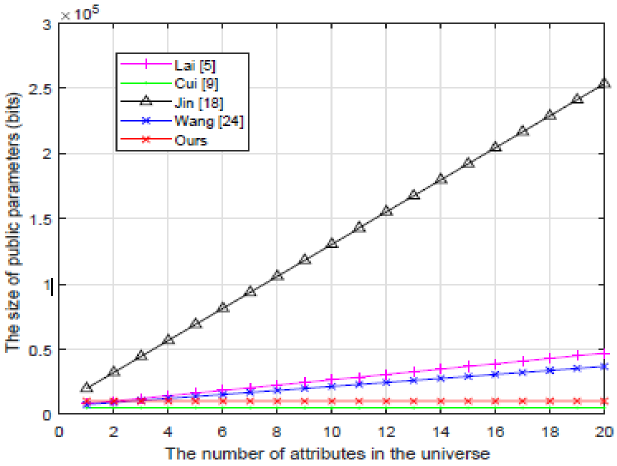

Figure2: Public parameter computing costs

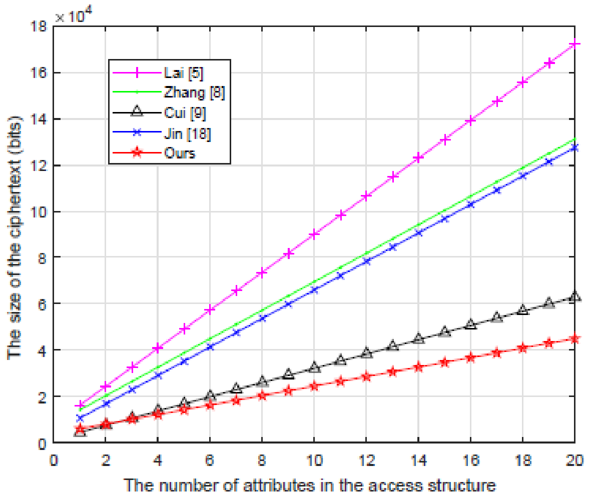

Figure3: The ciphertext storage costs

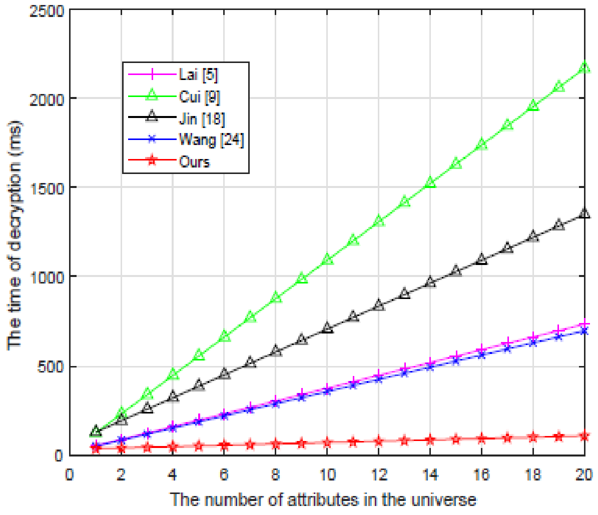

Figure4: Data consumers' overhead decryption

5. 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 attribute. The most obvious leeway in this context is that important 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 minimise 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 strategy which the proposed scheme does. The dilemma, with fast encryption that is left as a future job, is interesting, and completes a secret agenda.

REFERENCES:

1. Qinlong Huang, Wei Yue, Yue He and Yixian Yang, "Secure Identity-based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing", *IEEE*, July 2018.

2. Xu An Wang, Jianfeng, Fatos Xhafa, Mingwu Zhang and Xiaoshuang Luo, "Cost-effective secure E-health cloud system using identity based Cryptographic techniques", Future generation computer system, vol. 67, pp. 242-254, Feb 2017.

3. Xin Yao, Yaping Lin, Qin Liu and Junwei Zhang, "Privacy-preserving Search over Encrypted Personal Health Record in Multi-Source Cloud", *IEEE*, Jan 2018.

4. Shruthi ganesh, "Highly secured personal health record model", 2015 Online International Conference on Green Engineering and Technologies, 2015.

5. Cong wang, Bingsheng, Kui Janet and Chan wen Chen, "Privacy aware cloud-assisted healthcare Monitoring system via compressive sensing", IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, July 2014.
6. L. Azzopardi, M. Girolami, and K. van Risjbergen. Investigating the relationship between language model perplexity and iris precision-recall measures. In Proceedings of the 26th annual international ACM SIGIR conference on Research and development in information retrieval, pages 369-370. ACM, 2003.
7. S. Baccianella, A. Esuli, and F. Sebastiani. SentiWordNet 3.0: An enhanced lexical resource for sentiment analysis and opinion mining. In Proc. 7th Int. Conf. on Language Resources and Evaluation, 2010.
8. R. Baeza-Yates, B. Ribeiro-Neto, et al. Modern information retrieval, volume 463. ACM press New York, 1999.
9. D. Blei, A. Ng, and M. Jordan. Latent dirichlet allocation. the Journal of machine Learning research, 3:993-1022, 2003.
10. J. Blitzer, M. Dredze, and F. Pereira. Biographies, bollywood, boom-boxes and blenders: Domain adaptation for sentiment classification. In ACL, volume 7, pages 440-447, 2007.
11. S. Brody and N. Elhadad. An unsupervised aspect-sentiment model for online reviews. In Proc. Human Language Technologies: The 2010 Annual Conference of the North American Chapter of the Association for Computational Linguistics, pages 804-812, 2010.
12. G. Carenini, R. Ng, and E. Zwart. Extracting knowledge from evaluative text. In Proceedings of the 3rd international conference on Knowledge capture, pages 11-18. ACM, 2005.

G. Casella and R. L. Berger. Statistical inference. Duxbury Press, 1990.