CRYPTOGRAPHIC PERSONAL HEALTH RECORD MAINTENANCE IN THE CLOUD

[1]NAVYASHREE S, [2]POORNACHANDRA S

[1]Student, Department of Master of Computer Applications, East West Institute of Technology, Bangalore, Karnataka, India

[2]Assoc. Professor, Department of Master of Computer Applications, East West Institute of Technology, Bangalore, Karnataka, India

Abstract— Patients can control their health information over the internet with personal health records (PHR). PHRs hold highly sensitive information. Unintentional disclosure of this information impedes an intimate component of a patient's private life and may have severe effects. Cloud computing is gaining traction, but it has also raised security issues that have also been critically examined in academics and practice. Collaboration of technologies such as PHRs and Clouds necessitates study on security and privacy issues due to potential inherent conflicts. Our research aims to look into privacy concerns that may arise when using such a cloud service. A real-world scenario with solid facts and questions backs up the outcomes.

***Index Terms*—Personal Health Records (PHR), Cloud**

1. INTRODUCTION

Cloud computing is becoming increasingly important in today's technology. Every company has its own cloud where they can post their websites. As a result, we must provide more security for cloud files because there is a significant risk of being hacked by some individuals. All details, particularly in the medical profession, should be maintained in a more secure and safe manner. In this project Personal Health Record, the standard cypher text-policy attribute-based secret writing (CP-ABE)[19] gives access to manage the policy for the personal health record. To make the records safer, we need to apply additional security to the cloud files. Furthermore, the outcome of the user privacy for the access policy exposes a big amount of data from legitimate knowledge users. As a result, the guard users have privacy. The access policies should be buried under most privacy policies, thus there will be two problems: Because these regulations do not provide a large attribute universe, their utility in the decoding cost for the user is limited. To circumvent this issue, we must develop the CP-ABE algorithm [3] using low-cost decoding in which the dimensions of public parameters and, as a result, the value of decoding square measure constant. Furthermore, we must ensure that the system operates effectively and that the algorithm's accuracy is excellent.

2 LITERATURE SURVEY

Dual System Encryption introduces a novel technique to certifying the security of Identity-Based Encryption (IBE) and related encryption protocols. In a Dual Scheme Encryption system, cypher texts and private keys can take one of two indistinguishable forms. They will be normal if a private key or cypher text is created utilizing the system's key generation or encryption mechanism. These keys and cypher texts will behave as anticipated in an IBE system [1]. A public-key encryption technique based on the cypher text-policy attribute-based encryption scheme [9] with keyword search is suggested, which can conserve system storage. In order to offer increased access control for users and to provide a formal security analysis of the adaptive vs. chosen keyword attack paradigm, a novel attribute-based multi-keyword search for shared multiword primitives is proposed. The suggested methodology provides full security in the standard model under static assumptions by applying the dual system encryption method, as proven by a cypher text-policy attribute-based encryption [2](CP-ABE) scheme with efficient decryption. There will be a larger need to encrypt data saved at third-party sites as more sensitive data is exchanged and stored on the Internet by third-party sites. One drawback of encrypting data is that it can only be communicated in coarse-grained fashion (giving another party your private key). As a novel cryptosystem enabling fine-grained sharing of encrypted data, we propose Key Policy Attribute-Based Encryption (KP-ABE) [3]. Private keys are coupled with access structures that control which cypher texts a user may decrypt, and cypher texts are labeled with sets of characteristics in the cryptosystem [10]. Try to demonstrate our design's suitability for audit-log data sharing and broadcast encryption [7]. Hierarchical

Identity-Based Encryption [4] is one of the features of the design, which allows for the delegation of private keys. (HIBE). The approach of Fuzzy Identity-Based Encryption (FIBE) is a new type of Identity-Based Encryption (IBE). An identity is considered as a set of descriptive features in Fuzzy IBE. A Fuzzy IBE scheme may be used to enable encryption using biometric sources as identities; a Fuzzy IBE scheme's deviation property is exactly what allows the use of bionic identities, which will always make a commotion when sampled. We also illustrate how Fuzzy-IBE should be used to describe a style of guidance as attribute-based authentication [5].

3 METHEDOLOGY

Even if the access policy is disguised in most of the previous methods, they confront two obvious problems:

1. The applicability of those strategies in PHR is severely restricted since they do not give a vast attribute world.

2. As a result, the access policy is in ciphertext the cost of secret writing is quite high. We normally construct a CP-ABE concept featuring low-cost secret writing to meet these difficulties.

In past years, as a growing technology, Cloud computing allows us a speedy and cost-effective solution thanks to exchange informational resources and For instance, a large number of people use the internet to gather information with in the health-recording system for individuals, It is not necessary for a patient to carry a large amount of paper varieties of the assessment forms to evaluate in the usual manner, Yet, he or she will only be able to save, obtain, and transfer the health history if he or she uploads his or her own individual medical record to the PHR system. The patient is in charge of almost everything to his or her own individual medical file and approves United Nations agency[15] will access these health knowledge, friends, family, or care providers, for instances. In order to gain easy accessibility.

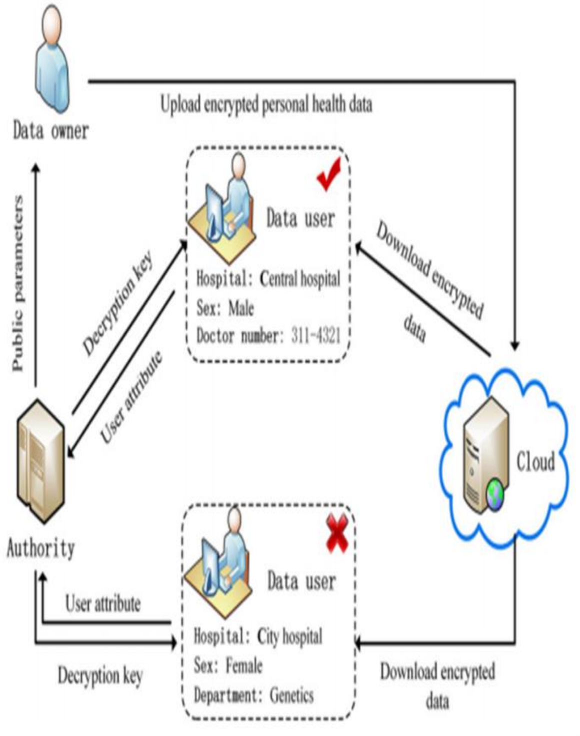

Fig. 1: Architecture diagram for secured personal health record

Management of this in [13], knowledge house owner urgently need a sort of cryptography them which will notice quite well authorization. Policy attribute-based encryptions with hidden ciphertext system gives sincere appreciation for resolving the issue Anywhere it offers data protection by obfuscating authentication and authorization policies. The access control policy in the preceding mechanism, on the other hand, was not enforced is frequently sent in combination with ciphertext, that makes it simple to betray the user's privacy because certain features in the proposed architecture provide vital information about genuine clients' identities. a patient's level connect strategy a patient's authorization might include some sensitive information such as a heart specialist, a centralized clinic, and so on. As a result, an unapproved individual

Despite the fact that he or she is unable to rephrase successfully, he/she can also the public key may be inferred in clear text form, something that the cipher or is afflicted with a disease. In [16], the fundamental Hidden Ciphertext-policy attribute-based cryptography (HCP-ABE) was established, in which the into above was integrated in the cyphertext rather than being communicated openly. Following that, various further concealed CP-ABE techniques were proposed in a series of papers.

The respond in these schemes, however, Supports just AND gates or AND gates on optimistic, negligible, and random entries. As a result, there are two disadvantages. First, as the number of characteristics grows, the size of adequate remedy grows linearly and second, the decryptions worth is substantially increased. Some minimal systems have better than negatives as a result of the larger than downsides incorporated in[21], as well as the standard technique The approach taken by such techniques is to use decryption The approach taken by such techniques is to use decryption.

Data house owners desperately want a form of encoding theme that may be aware of fine-grained data access. Concept of governance essential element encoding for hidden ciphertext expresses sincere appreciation in order to resolve the issue, in which it accomplishes confidentiality by concealing user access guidelines. The magnitude of right to be provided and, as a result, the cost of decoding remains fixed. Authority solely can have rights to get key for read information owner files[18], generate clinical report for information owner and think about information owner (patient details) and access information owner files. Data owner can't cipher the file simply, can generate the encoding key, then solely information owner cipher their files. Other user's (except doctors) cannot access the info owner files and conjointly generate report.

Here we tend to are implementing advanced encoding technique and every one the small print of the patient is saved within the centralized server.

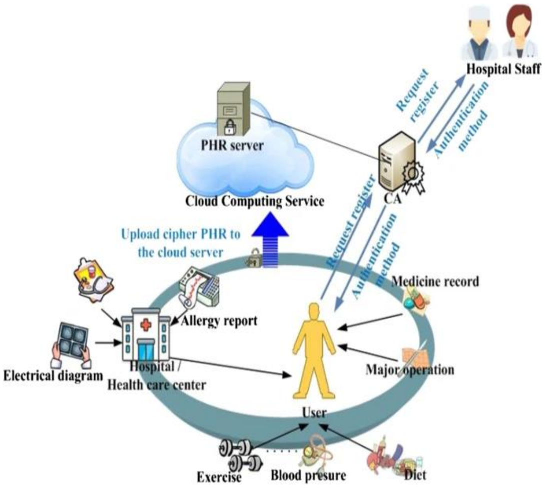

Fig. 2: The architecture of the PHR system in a potentially computerized environment

Here we tend to are mistreatment "Homomorphic encoding Algorithm(for encryption & decryption)."

Fully homomorphic systems[20] are those in which the cypher text may be computed in any way that is reasonableIn today's world, completely homomorphic programs exist Since 2009, they've been improved to the point where they're useful for a few workloads. Craig aristocracy was the first to suggest that these may be possible in theory. He was ready to create a system and individuals that were homomorphic in two ways, allowing for complete homomorphy.

In this thesis, Gentry takes the example of a jewelry store owner to demonstrate why completely homomorphic networks should and can exist. Consider Alice as the proprietor of a jewelry business. She employs people to construct items made of raw resources such as gold and diamonds. However, she is concerned about the possibility of theft. As a result, she designs cases with sleeves attached. To assemble the goods, employees will insert their palms through into box. They can't get anything out of the carton, though, because Alice is the only one with the key. So, Alice's employees will perform procedures on the secure data (the jewelry) although never getting the opportunity to get that sensitive data off.

Associates are included in Gentry's scheme noise level in the environment crypto graphical method. Every sequent encoding introduces a lot of system noise Gentry's early style reflects this is impractical[18] (Despite the fact that it was subsequently enhanced). Noise isn't a viable option as a result of eventually the system has to be restarted as a result of the side noise makes the whole system abundant slower. this technique depends on ideal Lattice based mostly

Cryptography to alter abundant of the system's style.

4. RESULTS

This research was undertaken to establish the socioeconomic influence of these factors on the entity. The quantity of funds the company can spend on research and enhancement for the infrastructure is constrained. As a consequence, the system that was created was also within plan; this was made feasible due to the reality that the bulk of the procedures employed were open to the community.

This research was done to assess the technological effectiveness of the system, or technological requirements. There was a strong demand for all available technological resources, which might result in a high demand for technical resources. This may result in the client being subjected to unreasonable demands. To implement the system, only little or no changes were required.

The purpose of this research is to see how far the user accepts the system. This covers how the user is coached to use the technology effectively. The methods used to train the customer more about system and make him conversant in it are solely the amount of recognition and utilization is the responsibility of the person in charge. His self-confidence has to be strengthened in order for him to be able to provide useful criticism, which would be advisable as he is the most powerful owner of the account.

Doctor can able to register their account once they register their account they cannot able to login because the cloud server has to authorize the particular person to login. Once the Doctor can authorized by cloud server then the doctor can able to login into the system. The Doctor can able to upload the Patient record and Doctor is the authorized person to add the patient details and they can able to view their patients details and they can able to monitor those patients. The doctors can able to view their reports and they can able to view their details and if they want they can able to edit the details accordingly.

The cloud server has to login their account using their login credentials once they logged into the system the access all the activities of the hospital. The cloud server is the responsible person to activate the data user and doctors once they are activated by the cloud server then only they can able to login They are the authorized person to monitor all the patient details, Clinical report details, attacker details and result analysis of the particular system.

The data user has to register their account once they register their account they cannot able to login because the cloud server has to authorize the particular person to login. Once the Data User can authorized by cloud server then the data user can able to login into the system.

Once they logged in the data user can able to view their details and if they want to download the report they have to get the key from the attributor. The data user can able to Search files based on the keyword. If user enters the wrong keyword, our application suspects this user is the attacker. Because, The main goal of the project is secure against chosen-keyword attack. Based on the search file they can able to request the key from the attributor. Once they received the key from the attributor the data user can able to download the file.

6. FUTURE WORK

In this project, we are introducing advanced the advanced algorithm implementation for the encryption and decryption and the efficiency of the algorithm should high. In future we will try to reduce the execution speed and the make the system with uploading the data is the centralized server with distributed networks so the time delay will be reduce and efficiency of the projects became high.

In future we will try to automate the system by adding Machine Learning Technique so it will reduce the human efforts.

5. CONCLUSION

In this project, we have a tendency to introduce a replacement technique known as disclosing a hidden truth with the several parameters. It has the potential to significantly enhance the articulation of access structure. Consequently, every characteristic is classified into two components, Essentially, the title of the characteristic and its result. Ultimately, the foremost the suggested scheme has a clear benefit is that Values of integrity and confidentiality are concealed. It will in PHR, consumers' privacy is carefully protected. Within the framework of the proposal the quantity of public variables is always the same and also only two pairing actions are required for decoding, it’s also a lot more rational as a result of this. Eventually, we have a inclination to prove one's point that total the proposed theme's safety within the customary model underneath

By utilising the twin system cryptography approach, static preconceptions may be avoided. The planned theme solely achieves part concealment policy. It is a remarkable drawback that achieves totally concealment policy with quick cryptography that will have to wait till eventually.

6. REFERENCES

[1] B. Waters, ―Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions,‖ in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science), vol. 5677, S. Halevi, Eds. Berlin, Germany: Springer, Aug. 2009, pp. 619–636.

[2] M. Qutaibah, S. Abdullatif, and C.T. Viet, ―A Ciphertext-Policy Attribute based Encryption Scheme With Optimized Ciphertext Size And Fast Decryption,‖ in Proc. 2017 ACM Asia Conf. Comput, Commun. Secur. (ASIA CCS), Apr. 2017, pp. 230–240.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ―Attribute-based encryption for finegrained access control of encrypted data,‖ in Proc. 13th ACM Conf. Comput, Commune. Secure. (CCS), Nov. 2006, pp. 89–98.

[4] J. Lai, R.H. Deng, and Y. Li, ―Expressive CP-ABE with partially hidden access structures,‖ in Proc. 7th ACM Sym. Infor., Comput, Commun. Secur., May. 2012, pp. 18–19.

[5] Sahai and B. Waters, ―Fuzzy identity-based encryption,‖ in Advances in Cryptology— EUROCRYPT (Lecture Notes in Computer Science), vol. 3494, R. Cramer, Eds. Berlin, Germany: Springer, May 2005, pp. 457–473.

[6] L. Ibraimi, M. Asim, M. Petkovic, ―Secure management of personal health records by applying attribute-based encryption‖, in: 2009 6th International Workshop on Wearable Micro and Nano Technologies for Personalized Health, pHealth, IEEE, pp. 71–74.

[7] M. Li, S. Yu, N. Cao, W. Lou, ―Authorized private keyword search over encrypted data in cloud computing‖, in: 2011 31st International Conference on Distributed Computing Systems, ICDCS, IEEE, pp. 383–392.

[8] Emura, K., Miyaji, A., Omote, K.: A dynamic attribute-based group signature scheme and its application in an anonymous survey for the collection of attribute statistics. Journal of Information Processing 17, 216–231.

[9] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, SP 2007, pp. 321–334.

[10] Attrapadung, N., Imai, H.: Conjunctive broadcast and attribute-based encryption. In: Shacham, H., Waters, B. (eds.) Pairing-Based Cryptography – Pairing 2009. LNCS, vol. 5671, pp. 248–26

[11] Boneh, D., & Franklin, M. (2001). Identity-based cryptosystems and signature schemes. Advances in Cryptology-Proceedings of Crypto, 2139, 213–229.

[12] Fan, C. I., Sun, W. Z., & Huang, V. S. (2010). Provably secure randomized blind signature scheme based on bilinear pairing. Computers & Mathematics with Applications, 60(2), 285–293.

[13] Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., & Sands, D. Z. (2006). Personal health records: Dentitions, benefits, and strategies for overcoming barriers to adoption. Journal of American Medical Informatics Association, 13(2), 121–126.

[14] AHIMA, J. (2007). The value of personal health records: A joint position statement for consumers of healthcare. Journal of the American Medical Informatics Association, 78(4), 22–24.

[15] Miller, R. H., & Sim, I. (2004). Physician's use of electronic medical records: Barriers and solutions. Health affairs, 32(2), 116–126.

[16] Kaelber, D. C., Jha, A. K., Johnston, D., Middleton, B., & Bates, D. W. (2008). A research agenda for personal health records (PHRs). Journal of the American Medical Informatics Association, 15(6), 729–736.

[17] Kim, M. I., & Johnson, K. B. (2002). Personal health records: Evaluation of functionality and utility. Journal of American Medical Informatics Association, 9(2), 171–180.

[18] Chen, L., Cheng, Z., & Smart, N. P. (2007). Identity-based key agreement protocols from pairings. International Journal of Information Security, 6, 213–241.

[19] Wu, S. Y., & Tseng, Y. M. (2010). An ID-based mutual authentication and key exchange protocol for low-power mobile devices. The Computer Journal, 53(7), 1062–1070.

[20] Joux, A. (2002). The weil and tate pairings as building blocks for public key cryptosystems. International Algorithmic Number Theory Symposium, pp. 20–32.

[21] Miller, R. H., & Sim, I. (2004). Physician's use of electronic medical records: Barriers and solutions. Health affairs, 32(2), 116–126.