International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 1st Jun 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-06

Title: SECURE DATA ENCRYPTION AND ACCESS CONTROL IN HEALTHCARE USING ATTRIBUTE BASED SIGNCRYPTION

Volume 08, Issue 06, Pages: 110–115.

Paper Authors

MANJUNATH VARCHAGHALL, POOJA SG, POORNIMA G,MEGHANA M L, BHAVANA DORA M

RRCE, Bangalore

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

SECURE DATA ENCRYPTION AND ACCESS CONTROL IN HEALTHCARE USING ATTRIBUTE BASED SIGNCRYPTION

MANJUNATH VARCHAGHALL[1], POOJA SG[2], POORNIMA G[3], MEGHANA M L[4] AND BHAVANA DORA M[5]

Assistant Professor[1],Dept of CSE, Rajarajeswari College of Engineering,

UG Scholar[2,3,4,5], Dept of CSE, Rajarajeswari College of Engineering, Bengaluru-74.

Abstract- Personal health record (PHR) model isused to exchange the health record, and toaccess and store the information about patient’s health. This personal health records are used to store and accessed through cloud. As the data stored in the cloud will be exposed and accessed by the unauthorized organizations, this may lead to patient’s privacy risk hence the information is very sensitive and individual may lose their personal information. This paper proposes a system which provides secure data Encryption and Access control. This n-grained access control provides confidentiality and authenticity. In order to reconcile the conflict of high computation overhead and security issues the outsourcing schema is proposed in this paper. In this schema heavy computation is overhead and leaving only less computation to the individual or the user or the owner of the health record. A theoretical analysis and securing properties which gives the security, confidentiality and verifiability has been proved in thismodel.

1.INTRODUCTION

With the assistance Cloud computing technology several firms and Organization store the data within the public cloud that could be virtual surroundings to store the info. Cloud could also be restricted to single organization or to the multiple organizations or the mix of each. Since cloud is employed to store knowledge the organization or the user no ought to maintain the native storage. they will store {the knowledgethe infor the information} within the cloud like pay-per-use data that's the number is acquired the specific amount of area within the cloud. Taking the private Health Record because the example the many PHR users outsourced to the cloud server to fancy the advantages of the cloud. the info that is that the patient health record is keep within the cloud and it's accessed by the cloud itself instead of the PHR service supplier. Since this cloud aided PHR model has a lot of advantage and adaptability compare to the info that is keep within the native storage. Since storing knowledge in cloud has some disadvantage just like the knowledge are often accessed by the unauthorized persons and knowledge are often changed and original content could also be lost with this sort of activity. Since during this system we tend to area unit exploitation Patient health record knowledge that is incredibly sensitive form of knowledge it ought to lean a lot of security. wherever there could also be a lot of probability of PHR knowledge could also be accessed by licensed person and knowledge are often changed. On alternative hand PHR knowledge collected from the patient could also be contaminated with the malicious opponent delivers the false knowledge to the PHR service suppliers. Since to beat from this model the Attribute based mostly secure encoding is employed and it's voiceless the eye of the numerous researchers. It realizes the fine- grained access management and converts one to 1 communication to one-many communication mode. Moreover, this technique will give the high security to the info that is keep within the cloud. during this system to confirm the high security the 2 form of Attribute based mostly Encryption(ABE) area unit used specifically, Key policy ABE and Ciphertext based mostly ABE severally The Key policy ABE is employed to annotate the ciphertext and access policy area unit related to the user's personal key. In ciphertext based mostly ABE every ciphertext is related to the access policy and attribute set is go with every personal key. The ciphertext is decrypted only the attribute set is happy. Similarly, to sign the message while not revealing the identity of the user the special methodology ids used that's Attribute-Based Signature (ABS). In ABS a signer UN agency possess the set of attributes from the authority will sign a message with a predict that it satisfies the message. Since our main aim during this system is to realize the High security of the PHR knowledge keep within the cloud. so as to realize the confidentiality and genuineness at the same time a special methodology is employed during this paper that's Attribute-Based Signcryption (ABSC). This ABSC is employed to supply the protection to the cloud aided PHR with its characteristics. Since all the schemes that uses the ABSC has high Computation value. Therefore, the plain text is signcrypted and uploaded to the cloud server during this PHR system. However, the frequency of decipherment operation is bigger than the signcryption operation. The PHR system uses the Key problems so as to enhance the potency of decipherment. although the ABSC provides the high security it uses a lot of linear pairing technique that results in the high computation value for the system.

A. CONTRIBUTIONS

To overcome this, we have a tendency to gift a replacement Ciphertext Policy Attribute primarily based Signcryption with Outsourced secret writing (CP-OABC) within the cloud aided PHR. this can be the primary paper to use the CP-OABC theme to secure the outsourcing of ABSC theme. the most philosophy is behind the verifiable outsourcing of secret writing. the most contribution of the designcryption method is outsourced to the untrusted cloud server. To run the PHR user aspect the constant computation is needed. The associated user will verify the result came from untrusted cloud servers. By victimization this theme, the high security is provided to the cloud aidedPHR

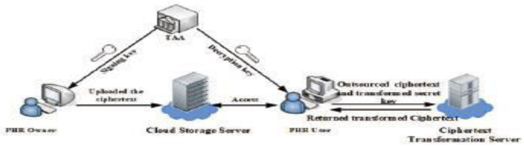
TAA
Signing key
Decryption key
Uploaded the ciphertext
Access
Outsourced ciphertext and transformed secret key
Returned transformed Ciphertext
PHR Owner
Cloud Storage Server
PHR User
Ciphertext Transformation Server

FIGURE 1. Architecture of CP-OABSC scheme.

Consider the figure that shows the design of the CP-OABSC theme wherever this technique consists of 3 variety of user Admin, information Owner shopper. Basically, this technique wants 2 servers in cloud, one can act as a Cloud Application Server wherever the PHR signcryption computer code is running. Another one is Cloud Storage Server wherever the encrypted information files area unit hold on. User has got to access the PHR signcryption application that is running in cloud application server with correct computer address on applications program. every user has their distinctive user id and positive identification to enter into their session. Once the user enters into their session, all the relevant functions they'll use. At a time, any variety of users will ready to access the PHR signcryption application, it's the potential to handle quite one user at a time.

2.RELATED WORK

Jun Huang, et al [1], explains that their system investigates the co-relations between different service providers. Based on results the proposed one is generic economic model and feasible. Dmitry Kogan, et al [2], in this paper offline Time-based One-Time Password (TOTP) schemes are explained which includes no server secrets. By developing near optimal algorithm for generating the necessary elements in a hash chain quickly with minimum memory requirements on the client side. But this requires some setup time to generate TOTP. Jun Haung, et al [3], clone detection approach which is termed as double track detection is used in this paper. This gives radio frequency identification for enabled supply chains. Supply chains are insufficient when dynamic change is taken into consideration. Hence this system is limited. Xiaokui Shu, et al [4], they used a set of sensitive data digests in data leakage detection. Using those sets, the data owner is able to assign the detection process to a biased provider without disclosing the sensitive data to him. Gilad Katz, et al [5], two phases, Training and Detection are used in this model. Documents can be generated and represented in a graphical way in Training phase. The key terms in this representation are considered to be confidential. The tested documents are assigned to various clusters and contents are matched with respective graph of each cluster during detection phase. Detection phase is an attempt to know the document's confidentiality. Al Neyadi, et al [6], in their first phase analysis they, have used an N-gram classification tool, eliminates which is not-English text. This N-gram classification prevents data leakage on the basis of separating possible and impossible personal health information container... Sultan Alneyadi et al [7], The approach used in this paper is based on well-known information retrieval function. Term Frequency-Inverse Document Frequency (TF-TDK) is used for document classification. Using Singular Value Decomposition (SVD) Matrix classification results are visualized.

3. METHODOLOGY

Cloud computing is the availability of resources for data storage and computing power and is an expression used to describe a variety of computing concepts.

It also referred to as network-based services.The Personal Health Record is a record of the patient data which is stored in cloud. The personal health information of the patient may be accessed and modified by the unauthorized persons. Because of this, the patient may lose the physical control over data.To avoid this kind of unauthorized data access to the personal health, this paper uses, Cipher text-policy Attribute based Signcryption(ABE) scheme.Symmetric key is encapsulated using the ABE and Symmetric Encryption algorithm is used to encrypt the PHR data. In this system files can be accessed only bythe authorized user.The system uses the three different end users, they are mainly, Admin, Data Owner, and Data Consumer as mentioned earlier in this paper. The system also includes two servers in the cloud for encryption of files and for storage of the files. The servers used are The Cloud Application server and the Cloud Storage Server. PHR Signcryption software will be running in the Cloud Application server, which is meant for encrypting the file which as to be uploaded by the Data Owner. And Encrypted data file from the Cloud Application server is stored in the Cloud storage server for further accessing or downloading the file from the cloud by the Users.

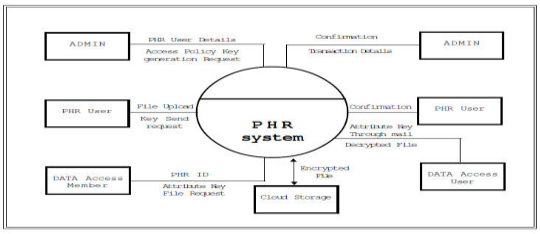

FIGURE 2. Architectureof the PHR System.

The PHR SystemArchitecture describes who are the end users and what are theircontribution or work in FIGURE 2.

a) Admin: Admin who is also called as Super User, has the authority to create the PHR Data Owners and able to maintain the cloud server's configuration. Admin has the ability to add orremove any number of Data Owners, and can edit the Data Owners details. Initially the Admin has to login to perform all these functions.

b) Data Owner: Data Owner can also be called as PHR user, who is created by the Admin. PHR user is the person who upload the file into the cloud. Once the data owner is logged in, he can able to upload the files which he selects from the system. While uploading the file into the cloud the Cloud Application server encrypts the file using the Data Owner encryption key. Anencryption key of the Data Owner is generated using RSA algorithm. And stores the encrypted file into Cloud Storage server for further access by the Data Users.

PHR Data Owner one who creates the Data User who can access the data files (PHR) uploaded in the cloud by the Data Owner. Data user can access the file once it is decrypted using the Attribute Base Decryption key sent by the data owner. The decryption key contains the PHR data owner's decryption key along with data users' attributes.

c) Data User: Data User who is known as the data access user. Each and every data user will be having two attributes, one is Domain and the other is Designation. Authorized data user will be receiving the access key i.e. Attribute based decryption key through email from data owners. Whenever the data users want to download the file from the cloud, he wants to select the file from the list which is accessible to the user. when the user selects the file, the system asks the access key and when it gets the access key from the user end, the attribute set will be separated from the key and check for the accessibility. And if the user has rights to access the file,then he can download the encrypted file by decrypting it and downloaded to the respective user's local system.

4.IMPLEMENTATION

Implementation is the process of implementation or practice of the method or design or idea or model or system. The paper proceeds final shape during the implementation phase. The implementation phase involves the actual construction. In other words, implementation mentions ultimate installation of packages (code) in its physical environs, towards satisfying customer necessities as well as system. Formerly accepted onward plus broadcasting system, user essential recognize that server package must run on server, client program should run in the client end and back-up client program should run in the back-up client. The user must have conscious that server-object is not in succession on server then genuine progression does-not apprehended.

Implementation Overview

Adding sensitive keywords and weight age

Admin going to add sensitive keywords with weightage.Those sensitive keyword are converted into fingerprinthash code by using MD5 algorithm.

Intranet Mail System.

With the help of this module user can able to send a mail to other users in the system and he can able attach the files to the mails.

Detecting Sensitive Data in the text file

This module is used to verify whether the attached files has sensitive message or not. If the attached file contains the sensitive message and user by mistake send to otherswitchwill create the data leakage problem. To overcome this from the attached files keywords are extracted and compared with the sensitive keywords.

Giving Sensitive Data Alert message to the user

There is a sensitive keyword scoring mechanism by which score will be calculated and compared with sensitive words in database using hashing technique and ifthe score crosses the threshold level, it warns the user.

Natural language processing

The field that deals with human and computer interaction with each other is known as language processing or natural language processing. This can be found at the intersection of computer science, engineering and linguistics. Natural language processing is a manner using which the computers will analyze, understand and make a decision in an intelligent way. Developers can organize and information can be structured to perform specific tasks like analysis of sentiment, recognition of speech, segment of topics etc., Natural language processing is said to be a tough downside in the field of applied science. Understanding the human language is not only to grasp the words pronounced, but also the ideas and meaning of the connected words in the sentence must be recognized.

5.CONCLUSION

This paper proposed a system to overcome the problem of designcryption mechanism at PHR user side, and also implemented CP-ABSC scheme, which is efficient and secure. This CP-ABSC is verifiable outsourced designcryption scheme. Hence, both bandwidth and local computation time can be reduced significantly. Due to this the proposed PHR system is efficient. The outcome has shown this system is secure and also practicable.

6.REFERENCES

*[1]*Jun Huang , Senior Member, IEEE, Jinyun Zou, and Cong-Cong Xing," Competitions Among Service Providers in Cloud Computing: A New Economic Model "[2018].

[2]Dmitry Kogan , Nathan Manohar , Dan Boneh [5]," T/Key: Second-Factor Authentication From Secure Hash Chain"[2017].

[3]JunHuang,XiangLi,Cong-congXing,WeiWang,Kun Hua and Song Guo,"DTD:A Novel Double-Track Approach to Clone Detection for RFID-Enabled Supply Chains [2017].

[4]SultanAlneyadi, ElankayerSithirasenan, VallipuramMuthukkumarasamy," Detectin"g data semantic: A data leakage prevention approach"[2015].

[5]Gilad Katz , Yuval Elovici, Bracha Shapira "CoBAn: A context based model for data leakage prevention" [2014].

[6]AlNeyadi, Sultan, Sithirasenan, Elankayer, Muthukkumarasamy, Vallipuram," Word N-Gram Based Classification for Data Leakage Prevention "[2013].

[7]SultanAlneyadi,ElankayerSithirasenan, VallipuramMuthukkumarasamy, **"**Adaptable N-gram Classification Model for Data Leakage Prevention" [2013]

[8] A. Sahai and B. Waters, ''Fuzzy identity-based encryption,'' in Advances in Cryptology—EUROCRYPT, vol. 3494. Berlin, Germany: Springer, 2005, pp. 457–473.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ''Attribute-based encryption for fine-grained access control of encrypted data,'' in Proc. 13th ACM Conf. Comput. Commun. Secur., 2006, pp. 89–98.

[10] A. Lewko and B. Waters, ''Unbounded HIBE and attribute-based encryption,'' in Advances in Cryptology—EUROCRYPT, vol. 6632. Berlin, Germany: Springer, 2011, pp. 547–567.

[11] J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-policy attributebased encryption,'' in Proc. IEEE Symp. Secur. Privacy (SP), May 2007, pp. 321–334. signcryption with ciphertextpolicy and claim-predicate mechanism,'' in Proc. IEEE 7th Int. Conf. Comput. Intell. Secur. (CIS), Dec. 2011, pp. 905–909.