© 2017 IJSRST | Volume 3 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Secure Jelastic Cloud by Attribute Based Encryption

Banoth Seetha Ramulu[1], H.Balaji[2]
[1]Associate Professor, Department of CSE,Vardhaman College of Engineering, Shamshabad, Hyderabad, Telangana, India
[2]Associate Professor, Department of CSE, Sreenidhi Institute of Science and Technology, Ghatkesar, Hyderabad, Telangana, India

ABSTRACT

Nowadays secure sharing of patient health records in Jelastic cloud provides the more benefits to the data owners and end users. We know that building a specialized data center's is very difficult task and maintenance cost also very high. Sharing the PHR Application in the third party server raises the security and privacy risks. In this paper we introduce ABE highly secure encryption algorithm for providing the security and good privacy policies to the PHR information, which is stored in the cloud server. Not only this, for providing the Scalability, Load balancing and for easy maintenance to the application, we are deploying the Personal health record's application into Jelastic cloud by the use of Servint server. Nginx is the Load balancer to provide the load balance to our PHR application. Jelastic cloud is successfully providing the both Horizontal and Vertical Scaling to our PHR Application.

Keywords: Jelastic Cloud, ABE (Attribute Based Encryption), Nginx, Servint, Load balance, Scalability.

I. INTRODUCTION

Nowadays sharing of patient health records in third-party server raises the security problems and also privacy concerns regarding the PHR information. This PHR application will help's the user to create their own personal health records and they can delete the PHR in the cloud easily.

Not only this, they can modify the information easily using this application, and he can share their PHR to several users like friends, doctors and family members under certain access policies. We know that creating the own Data centres gives the expensive cost. That's the reason we are going to use the third party servers for deploying our application in the cloud environment.

Before deploying our PHR application into third-party server we need to consider some of the security and privacy policies, which is useful to our application. Yes, Jelastic Cloud is exactly providing the high security, scalability and easy maintenance to the PHR application in the cloud. Jelastic Cloud providing the Load balancer to our application by using Nginx, it can easily scale horizontally and vertically in both ways whenever user load is high. We can scale the application up to 12 cloudlets primarily in the Jelastic Cloud. To provide the security to our PHR information, we use the Attribute-based encryption algorithm.

By using this algorithm we can encrypt the patient health information before storing into the third-party server (Servint). Cloud provider or third party persons cannot access the data, even if they are able to view the PHR data, its only appearance in the form of encrypted data. For decrypting the information we need the key, only authorized persons having the key and they can easily access the PHR data based on the attributes (friends, family members and doctors) given

by the user while uploading their personal health records.

II. RELATED WORK

In [1], Kabilan N proposed the concept of using advanced encryption standard [AES] for sharing the personal health records securely in untrusted servers, like third party servers. In this paper Kabilan N is mainly focused on security for PHR information. Advanced encryption standard algorithm is useful for handling the multiple authorities to provide security to PHR information from untrusted users. But in this model key maintenance and distribution is very difficult task. Comparing between Advanced encryption and Attribute based encryption algorithms, Attribute based algorithm gives more performance and reliability.

In [3], Hons Lohr, Ahmad –Raza sudeghi and Marcel winandy propose a concept "Securing the eHealth Cloud". In this paper, they mainly focused on standards and solutions regarding to ensure privacy and security with respective to E- health system. We know it's very critical issue to provide security to E-Health system. In this paper they introduced the concept of security architecture for fulfilling the security gaps in Ehealth system, and also they given challenges related to security and privacy.

Identity based encryption [IBE] [4], is proposed by Alexandra Boldyreva for providing the security to the Information or data stored in third party servers. We know that Identity based encryption algorithm is one type of public key encryption algorithm. IBE algorithm is good for improving the key update efficiency. But this solution is not works well, when the number of users increasing.

In [10] proposed a framework based on web services to provide trust management in cloud environments. The model also proposed for finding credible and untrusted feedbacks. In [11] prepared a model for invoking different types of web services from the cloud server for mobile application. In mobile application load balancing and the response time is better than standalone application. It is used windows workflow for service composition in cloud based mobile application.

By the proposed system we can save the battery life and the storage capacity to be increased. Sasko Ristov and Co [12] tested the web services capacity in terms of memory in both the ways of hosting web services on premises and hosting web services in cloud environment. In these they found some variations among two methods to find the efficient deployment of the service. Wang and Co [13] employed particle swarm optimization with skyline operator to increase the capacity of service composition in the cloud based mobile application.

Satish et al [14] prescribed Mobile Cloud Middleware between the mobile host and the cloud region to improvise the QoS aspects of the mobile host for providing the security and the integration of the needed services. Paper [15] described security framework to ensure authentication and confidentiality in the mobile cloud environment between the mobile host and clients. Mariam Kiran and Co [16] introduced Model based testing for composed web services in cloud brokerage applications. In [17] used computational offloading to enable the computationally concentrated mobile applications on SMDs. Henryk Krawczyk et al [18] explained mobile cloud computing applications and challenges with existing solutions. They introduced mobile offloading framework for improving the efficiency to adopt for many applications.

In [19] introduced phased scheduling in order to improve the performance of the mobile client in the cloud environment to extend the battery lifetime and the resource utilization is to be high. William Tarnaberg [20] proposed cost optimal management

approach for the future mobile cloud network. Then it shows improving of aggregate cost and utilization of resources then it proves the adaptable environment of the users

III. PROPOSED WORK

The proposed demonstrate for the most part focuses on giving Security, Privacy, Scalable, Load adjusting, and simple upkeep to the individual health records application in the cloud. Any approved client can safely impart their own records to Doctors, loved ones through this PHR application based on the attributes given by the client and access arrangements. By sending PHR application in Jelastic Cloud client can get to their PHR data from anyplace and whenever by simply utilizing PHR application. By utilizing this application every patient has full control over their own records.

As of late Microsoft Health vault additionally proposing a similar idea of sharing PHR in the cloud. In this paper, we propose an Attribute-based encryption (ABE) algorithm for encryption and unscrambling of patient health records. This algorithm is encoding the data previously putting away the PHR data to the cloud server. Furthermore, unscramble the data while recovering from the server based on the attribute and access strategy given by Data owner. The accompanying Diagram demonstrates the Architecture of the PHR in Cloud.

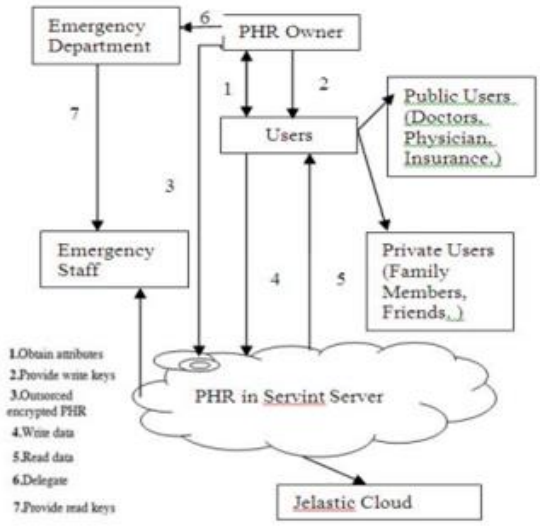

Fig. 1 Architecture of PHR in Jelastic Cloud

Source from :

Access policies are mainly categorized as two types' Personal user (Family members, friends and etc.) and Professional user (Doctors, Researchers and Pharmacists). The access policies are differ based on the users, some users may only have read option (like friends), and some users may have write option (like Doctors). This access policy is limited by Data owner.

Algorithm: Attribute based algorithm (ABE)

The following 6 steps are involved in the Attribute based algorithm.

a) Start.
b) **Setup:** (Pk, Mk), it will generate the Public key and master key.
c) **KeyGen**: (W, Mk) → (SKw)
Here W – User attributes
Mk – Master Key
SKw is generated by using W and Mk.
d) **Encrypt:** (M, Pk, T) → CT
Here T – Access policy
Encrypt the M by using the Pk and T
e) **Decrypt:** (CT, SKw) → M
Here decrypt the CT by using SKw..
f) End

We know that Attribute based encryption algorithm is one of the types of public key encryption. In this algorithm public key (pk) is combined with the set of attributes given by the data owner. The following fig.

2 shows the work flow of Attribute based encryption (ABE) diagrammatical representation

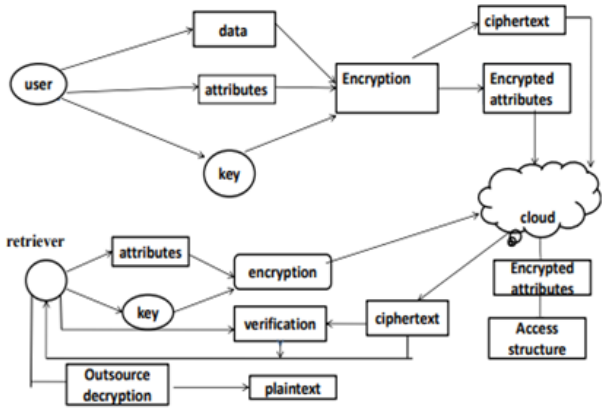

Fig. 2 Work flow of ABE

In the above, we can see the work stream of the ABE algorithm and client activities. Data owner chooses the information record or data and attributes. By utilizing the conjunction, disjunction and (p k) edge entryways get to strategies are characterized on the attributes. Based on data and attributes, it will encode the data.

Both the figure message and encoded attributes are put away in cloud server Data retriever needs to give the legitimate key. A client will have the capacity to unscramble the required document; if and just if his attributes are happy with the entrance arrangement characterizes by the data owner. On the off chance that it is substantial and matches with the attributes client will get the required data generally, the client won't get the required record.

IV. IMPLEMENTATION WORK

We have developed the web application for storing the PHR information in cloud by using the following software requirements are y Netbeans IDE, Tomcat Server y Jelastic Cloud, nginx y Servint (SQL Database) y Java (Servlets), xml, SQL,CSS (coding languages) In this application we have consider the mainly five modules.

Registration:

In this module generally several users will register for sharing and accessing the PHR information. Users will be data owners or data retrievers. Users are mainly divides into two categories like personal user and professional user[24].

Upload Files:

In this module user will upload their PHR files with secure keys. The data owner will upload the Encrypted PHR file into cloud server by using ABE algorithm. We know that each PHR owner file is encrypted and uploaded into cloud server under some access policies.

ABE Algorithm:

In this Module ABE algorithm is used to apply on PHR file for providing security and sharing the file in the third party server. Attribute based encryption algorithm is good for data access control over the outsourced data. Each PHR file is encrypted by using the CP- ABE algorithm before it outsourced, and it provides the direct revocation[23].

Key distribution:

In Key distribution first we have to define the common attributes with respect to the every PSD. In this module we have to define the attributes for Emergency situation like Break glass access. Here are some examples for attributes User profile, allergies, medical report and etc. public or master key is generated with respect to the each data owner PHR client application. Keys are distributed with respective user profile throw the mails.

Deployment and Maintenance in Jelastic Cloud:

We are using Jelastic cloud for deploying our PHR application in Cloud. Jelastic Cloud providing the Scalability, Load balancing and easy maintenance to our application. The above screenshot shows the creation of environment and deployment of PHR application in Servint Server[25].

V. CONCLUSION

In this paper, we created secure sharing of PHR data in the Jelastic Cloud by utilizing Attribute-based algorithm. Data owners can share their own health records to any client (like Doctors, relatives) by utilizing this application in the cloud. We demonstrate that this Attribute based algorithm is giving the security to the PHR document by encoding the PHR record before outsourced to the cloud. Just approved clients' entrance the PHR document or data based on a few attributes and access strategies. By utilizing ABE algorithm, it expands the data secrecy. And furthermore, it lessens the many-sided quality of key administration. Whenever and from anyplace client can share and view the PHR data by utilizing this application. The reason is, the application conveyed in Jelastic Cloud. Jelastic Cloud gives the Scalability, Load adjusting and simple upkeep to our PHR application. It decreases the Maintenance cost. We demonstrate that Compared to the past works our algorithm and PHR application is working effectively in a cloud situation with the immense highlights.

VI. REFERENCES

[1]. Kabilan N, "Scalable and secure sharing of Health record maintenance using advanced encryption standard", SR Research paper vol. 1, no. 4 may, 2014.

[2]. Ming Li, Shucheng yu, Yao Zheng, Kui Ren and Wenjing Lou, "Scalable and secure sharing of personal health records in cloud using Attribute based encryption algorithm ", IEEE Transanction on Parallel and Distributed systems vol. 3, no.7, july 2014.

[3]. Hans Lohr, Ahmad-Raza sadeghi and marcel winandy, "Securing the E-Health System in Cloud", in first ACM IHIS, 10, 2010, pp.220-229.

[4]. A.Boldyerva, Goyal V and Kumar V, "Identity based encryption with efficient Revocation", in ACM, CSS, 2008, pp. 417-426.

[5]. Anthony Velte, Toby Velte and Roert Elsen peter, "Cloud computing-A practical approach", McGraw-Hill, Inc. New York, USA, 2010.

[6]. Brent Waters, "Ciphertext-Policy Attribute Based Encryption an Expensive, Efficient, and Provably Secure Realization", University of Texas at Austin.

[7]. S. Yu, C. Wang, K.Ren, "Achieving secure, scalable and finegrained data access control in Cloud Computing", in IEEE, INFOCOM, 10, 2010.

[8]. M.chase, E. Horvitz, J. Benaloh and Lauter K, "Patient controlled encryption: ensuring the privacy of electronic medical records", in CCSW'09, 2009, pp. 103-114.

[9]. "App deployment in Jelastic cloud", http://www.Jelastic.com by Servint.

[10]. Noor, Talal H, and Quan Z. Sheng, "Web service-based trust management in cloud environments", Advanced Web Services, Springer New York, 2014, pp.101-120.

[11]. Ramasamy, R. Kanesaraj, Fang-Fang Chua, and Su-Cheng Haw, "Web Service Composition Using Windows Workflow for Cloud-Based Mobile Application," Advanced Computer and Communication Engineering Technology, Springer International Publishing, 2015, pp. 975-985.

[12]. Ristov, Sasko, et al. "Compute and memory intensive web service performance in the cloud," ICT Innovations 2012, Springer Berlin Heidelberg, 2013, pp. 215-224.

[13]. Wang, Shangguang, et al. "Particle swarm optimization with skyline operator for fast cloud-based web service composition," Mobile Networks and Applications, vol.18, no.1, 2013, pp.116-121.

[14]. Srirama, Satish Narayana, "Mobile Web and Cloud Services," Advanced Web Services, Springer New York, 2014, pp. 501-525.

[15]. AlShahwan, Feda, Maha Faisal, and Godwin Ansa, "Security framework for RESTful mobile cloud computing Web services," Journal of Ambient Intelligence and Humanized Computing, 2015, pp. 1-11.

[16]. Kiran, Mariam, and Anthony JH Simons, "Model-Based Testing for Composite Web Services in Cloud Brokerage Scenarios," European Conference on Service-Oriented and Cloud Computing, Springer International Publishing, 2014.

[17]. Shiraz, Muhammad, et al, "Energy efficient computational offloading framework for mobile cloud computing," Journal of Grid Computing, vol. 13, no.1,2015, pp. 1-18.

[18]. Colombo-Mendoza, Luis Omar, et al, "MobiCloUP!: a PaaS for cloud services-based mobile applications," Automated Software Engineering, vol. 21, no.3, 2014, pp. 391-437.

[19]. Li, Chunlin and Layuan Li, "Phased scheduling for resourceconstrained mobile devices in mobile cloud computing," Wireless Personal Communications, vol.77, no.4, 2014, pp. 2817-2837.

[20]. Tarneberg, William, et al, "Dynamic application placement in the Mobile Cloud Network," Future Generation Computer Systems, 2016.

[21]. B.Sameena Begum, P.Ragha Vardhini," Augmented Privacy-Preserving Authentication Protocol by Trusted Third Party in Cloud." International Journal of Computer Engineering in Research Trends., vol.2, no.5, pp. 378-382, 2015.

[22]. P.FARZANA, A.HARSHAVARDHAN," Integrity Auditing for Outsourced Dynamic Cloud Data with Group User Revocation." International Journal of Computer Engineering in Research Trends., vol.2, no.11, pp. 877-881, 2015.

[23]. N. Meghasree, U.Veeresh and Dr.S.Prem Kumar," Multi Cloud Architecture to Provide Data Privacy and Integrity." International Journal of Computer Engineering in Research Trends., vol.2, no.9, pp. 558-564, 2015.

[24]. A.Shekinah prema sunaina," Decentralized Fine-grained Access Control scheme for Secure Cloud Storage data." International Journal of Computer Engineering in Research Trends., vol.2, no.7, pp. 421-424, 2015.

[25]. P. Rizwana khatoon and Dr.C.Mohammed Gulzar ," SecCloudPro:A Novel Secure Cloud Storage System for Auditing and Deduplication." International Journal of Computer Engineering in Research Trends., vol.3, no.5, pp. 210-215, 2016.