ISSN No. 0976-5697

Volume 5, No. 8, Nov-Dec 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Securing Health Care Records over Cloud using PSZ Method

K.Govinda
SCSE, VIT University,
Vellore, India

Asv.Aadhithya
SCSE, VIT University,
Vellore, India

Rahul Soren
SCSE, VIT University,
Vellore, India

Abstract: In medical organizations cloud computing presents a new way for improving the business flexibility and delivery of healthcare. The cloud computing built shared servers which is connected through internet with privacy, security, access and compliance. While transfer medical and personal information through secured perimeter many compliance issues are take place. Cloud computing can improve the performance of healthcare organization, So it require a more secure and computing platform to protect health information cloud computing can improve the performance of healthcare organization. This paper describe how PSZ cryptography technique can be used to protect health care data.

Keywords: Healthcare, Position, Substitution, Cloud, Security.

I. INTRODAUCTION

Enormous change is take place in Healthcare services. In some countries a percentage of GDP rising b double digits annually. The growing over medical care access and quality, governments and healthcare institutions are working to find creative new ways to address the need for improved care delivery models and payment reform. So cloud Computing can help to face some of these challenges like efficiencies and low cost. The flexible cloud based resources will helpful for the growth of new generation in healthcare services

In the delivery of healthcare service cloud computing has a great potential. It will improve the data management and access with less costly methods .The cloud has centralized storage which also help to speed the deployment of electronic health record (EHR) and other advance which is prioritized under recent legislation such as the Health Information Technology for Economic and Clinical Health Act (HITECH), the Meaningful Use rules of the American Recovery and Reinvestment Act, and the European Commission eHealth Action Plan (eHAP).

We can access the information from anywhere with authorized. The cloud supports the various devices with data sharing and collaboration. A small healthcare clinic is specialized in some service such as radiology, with the help of cloud based application we can be part of internal network which are provided by the wide range of the medical service. With help of this service we can the money of staff, providing great flexibility in hour and coverage particularly in rural area. With help of healthcare cloud we can reach the clinical expertise across the entire region.

In healthcare organization, cloud computing provides greater efficiency, on-demand self-service, and numerous advantage to medical related business. High availability cloud infrastructures scale according to need, and provide the compute power for any type of workload, whether in a clinic or hospital or at a remote accident site. This services is provided via self-service or authenticated device through broadband connection. It is more efficient than traditional data center, cost reduction, energy saving and access from anywhere in any device.

The cloud computing is particularly important in healthcare organization .While cloud computing promises significant benefits, legitimate security and compliance concerns have slowed cloud implementation within the healthcare domain, particularly due to multiple layers of statutory and regulatory requirements that govern the handling of protected health information.

II. LITERATURE REVIEW

Mandatory Access Control (MAC), Discretionary Access Control (DAC) are traditional access control modelsand ensure less cloud data privacy protection. In sophisticated scenarios Role Based Access Control (RBAC) [12] model lacks context information to satisfy. In a distributed healthcare cloud a robust data protection is achieved by applying a scheme that supports fine-grained data protection requirement across multiple domains but does not rely on heavy communication and computation overhead, we propose the CPRBAC model. Comparing with other access control systems [9][12][15], and to enrich our policy description for complicated usage requirements, our model introduces four new components: *Organizations (Or)*, *Conditions (Co)*, *Obligations (Ob)*, *Purposes (Pu)* concerning authorization delegation, cross-realm role assignment, privacy-aware and active auditing scheme.

Recent researches have shown that there are partially addressed issues on data protection regarding security and privacy issues. To guarantee correctness and integrity one of well discussed approaches is Data dispersal storage and secure retrieval scheme [3][4] which adopts some effective and flexible distributed algorithms to allocate users' data to diverse domains. This scheme efficiently decrease the risk

of malicious data modification attack and server colluding attacks, but when data quantity is huge or existing using complex algorithm and distributed management scheme leads to unnecessary computation and communication overhead. Another solution [1][7][14] is key distribution scheme based on public key infrastructure which applies cryptographic primitives, and discloses decryption keys only to users who have authorized keys. By distributing the decryption keys to the expected users satisfies secure dynamic resource sharing scheme in cloud scenario.

Introduction of complexity in key distribution and data encryption is one of critical issues. The above two solutions are able to guarantee a coarse-grained data protection in cloud. However, new scheme is required to support some sophisticated context scenarios to achieve a fine-grained data protection scheme, such as access condition, time constraint or data operation purpose etc. another representative approach with predefined policy to guarantee data protection centrally and encapsulates sensitive data can be achieved through Data binding technology [5][8][11].

However, due to its centralized nature it is difficult to protect sensitive data against malicious modification or intrusive attacks. To address the above schemes' weaknesses, we propose a novel data protection model which can be applied in distributed health cloud scenario with low computational overhead but solid data protection scheme and is based on Cloud-based Privacy-aware Role Based Access Control (CPRBAC) model and Active Auditing Scheme (AAS). CPRBAC extends traditional Role Based Access Control (RBAC) model and can achieve more sophisticated data protection scenarios including authorization delegation, resource sharing across different cloud servers, and context-based access control restricts consuming cloud service based on authorized token. In contrast to some public auditing schemes in [10][13], we rely on an AAS which has ability to automatically take actions based on a run-time scheme rather than on a probabilistic sampling technique periodically fetch the statue of data and provide an active ongoing monitoring.

Our previous work [6] proposed Mobile Cloud for Assistive Healthcare (MoCAsH) as architecture for assistive healthcare which embraces important concepts of mobile sensing, active sensor records, and collaborative cloud services by deploying intelligent mobile agents, context-aware middleware, collaborative protocol for efficient resource sharing and planning in cloud. This paper addresses security and extends MoCAsH and privacy concerns in healthcare cloud by deploying a novel CPRBAC model for controllability, traceability of data and authorized access to cloud resources. Furthermore, the work proposes and develops an AAS that is capable of tracing, tracking, and triggering an alert on any operation, data or policy violations in healthcare cloud environment.

The author Ming Li,et.l mostly related to works in attribute based encryption and enforced access control for outsourced data. The traditional public key encryption (PKE)-based schemes [8], [10] are used to realise fine-grained access control which either incur high key management overhead, or require encrypting multiple copies of a file using different users' keys. One-to-many encryption methods such as ABE can be used to improve upon the scalability of the above solutions. In Goyal et al.'s seminal paper on ABE [11], data are encrypted under a set of attributes so that multiple users who possess proper keys can decrypt. This makes encryption and key management more efficient [12]. Preventing against user collusion is a fundamental property of ABE. In addition, the encryptor is not required to know the ACL.

A number of works used ABE to realize fine-grained access control for outsourced data [13], [14], [9], [15]. Especially, to secure electronic healthcare records (EHRs). Recently, an attribute-based infrastructure for EHR systems is proposed by Narayan et al., where a broadcast variant of CP-ABE [16] is used to encrypt the HER files of each patient and allows direct revocation. However, the cipher text length grows linearly with the number of unrevoked users. In [17], delegation of access rights is proposed by variant of ABE for encrypted EHRs. Ibraimi et al. [18] applied cipher text policy ABE (CP-ABE) [19] to manage the sharing of PHRs, and introduced the concept of social/professional domains. In [20], Akinyele et al.

Investigated to generate self-protecting EMRs which can either be stored on cloud servers or cellphones using ABE, so that EMR could be accessed when the health provider is offline. However, the above work have several common drawbacks. First, they usually assume the use of a single trusted authority (TA) in the system. This not only suffers from the key escrow problem since the TA can access all the encrypted files and may create a load bottleneck, opening the door for potential privacy exposure.

In addition, to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys is not practical. In fact, to become suitable authorities to define and certify different sets of attributes belonging to their (sub) domains (i.e., divide and rule), different organizations usually form their own (sub) domains. For example, a professional association would be responsible for certifying medical specialties, while job ranks of its staffs would be certified by a regional health provider. Second, there still lacks an efficient mechanism for ABE with the support for dynamic policy updates/changes and on-demand user revocation, which are essential parts of secure PHR sharing. Finally, most of the existing works have different attribute definitions, key management requirements, and scalability issues, do not differentiate between the personal and public domains (PUDs). Our idea of conceptually dividing the system into two types of domains is similar with that in [18]; however, to govern the whole professional domain, a key difference is in [18] a single TA is still assumed.

III. PROPOSED METHOD

Here we are going to introduce our algorithm and its working. PSZ algorithm have three level of encryption such as Position, Substitution, and Zigzag. Comparing to other algorithm time taken by PSZ is less even more data. Based on the length of the text, single key is generated and the private key is taken as secrete. Position and Substitution method will use the key level which are taken from the user. Three level of encryption are shown below.

A. Position Method:

In this method word may be alphabet, number or special character which are given by the user.

a. Get the key level and Source file and check whether key is valid or not.

b. From database take the valid string of alphabets.
c. On basis of accessed string, the string is encrypted.
d. With help of length of the file key has been generated from the user.

B. Substitute Method:

In this method a lot of complexity is added to avoid the break of code. Actually in this method the character has been replaced which are provided by the user.

a. From the position method you will receive the encrypted text and key level.
b. The encrypted file divided into block of arrays.
c. Replace the character which are provided from the user.
d. The replaced character must be stored in the form of array.

C. Zigzag Method:

From the replaced character which are stored in the form of array we are going to shuffle the data in array by Zigzag manner (Fig 1). With help of this algorithm we can minimize possible way of attacking

a. Take the array which has been given by substitute method.
b. Shuffle the data in array in zigzag manner (Fig 1).
c. The Shuffled data are combine together in a single encrypted file.
d. For decoding in future the private key has to be generate.

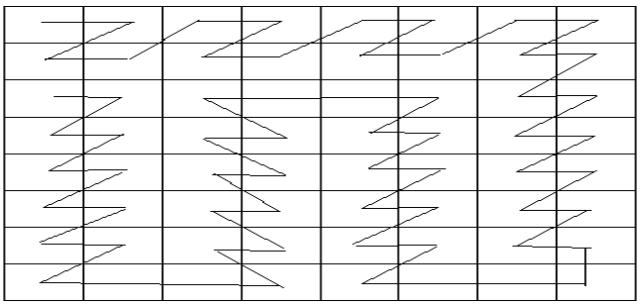
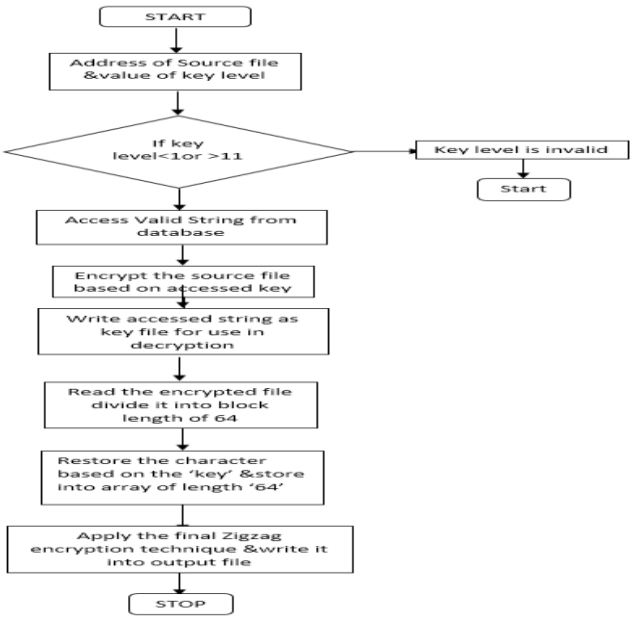


Figure 1 Zigzag method

IV. FLOWCHART



V. IMPLEMENTATION AND ANALYSIS

We have implemented the new algorithm with the following configuration. Intel(R) Pentium(R) @2.10Gh.z, 2.00GB RAM, windows 7 ultimate (64bit), Intel(R) HD graphics, DirectX 11, InsydeH2O Version 03.72.101.40

A. Time Complexity:

a) ***RSA:*** In this algorithm during encryption and decryption it will take more time [1]. For encryption it takes 1078(ms) and for decryption 875 ms

b) ***PSZ:*** While comparing to RSA algorithm PSZ will takes less time [1]. For encryption it takes 125 ms and for decryption 63ms

B. Confidentiality

a) ***RSA:*** This algorithm requires two key, public key for encryption and private key for decryption.

b) ***PSZ:*** Here key level is required for encryption and private key for authorized person to decode the encrypted file.

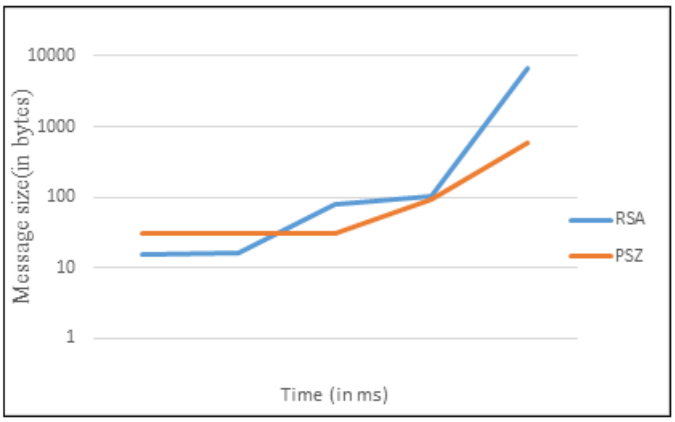


Figure 1. Encryption

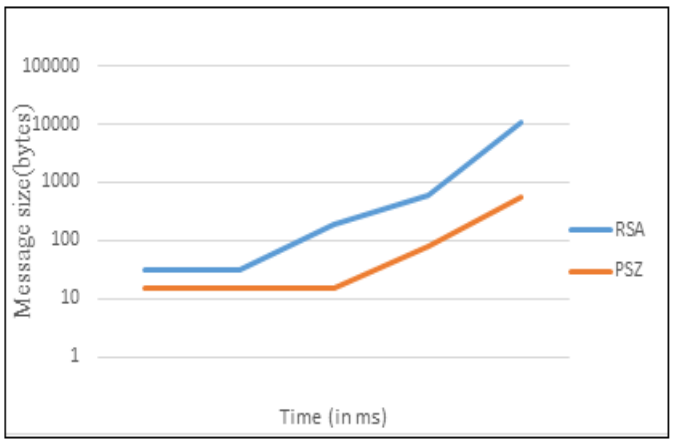


Figure 2. Decryption

VI. REFERENCES

[1] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models" Computer, vol. 29, pp. 38-47, 1996.

[2] N. Qun, E. Bertino, J. Lobo, and S. B. Calo, "Privacy-Aware Role-Based Access Control" Security & Privacy, IEEE, vol. 7, pp. 35-43, 2009.

[3] S. Liu, "Task-role-based access control model and its implementation" in Education Technology and Computer (ICETC), 2010 2nd International Conference, pp. V3-293-V3-296, 2010.

[4] Y. Shucheng, W. Cong, R. Kui, and L. Wenjing, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing" in INFOCOM, 2010 Proceedings IEEE, pp. 1-9, 2010.

[5] S. Wang, D. Agrawal, and A. El Abbadi, "A ComprehensiveFramework for Secure Query Processing on Relational Data in The Cloud"<http://www.cs.ucsb.edu/~sywang/docs/IDA-B+-tree.pdf >, 2010

[6] W. Cong, W. Qian, R. Kui, and L. Wenjing, "Ensuring data storagesecurity in Cloud Computing" in Quality of Service, 2009. IWQoS. 17th International Workshop on, pp. 1-9, 2009.

[7] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable secure file sharing on untrusted storage" in Proceedings of the Second USENIX Conference on File and Storage Technologies (FAST). USENIX, pp. 29–42, 2003.

[8] E. J. Goh, H. Shacham, N. Modadugu, and D. Boneh, "SiRiUS: Securing remote untrusted storage", < http://www.isoc.org/isoc/conference-s/ndss/03/proceedings/papers/9.pdf>, pp. 131–145, 2003.

[9] P. Angin, B. Bhargava, R. Ranchal, N. Singh, M. Linderman, L. Ben Othmane, and L. Lilien, "An Entity-Centric Approach for Privacy and Identity Management in Cloud Computing" in Reliable Distributed Systems, 2010 29th IEEE Symposium, pp. 177-183, 2010.

[10] D. B. Hoang and C. Lingfeng, "Mobile Cloud for Assistive Healthcare (MoCAsH)" in Services Computing Conference (APSCC), 2010 IEEE Asia-Pacific, pp. 325-332, 2010.

[11] A. Squicciarini, S. Sundareswaran, and L. Dan, "Preventing Information Leakage from Indexing in the Cloud" in Cloud Computing (CLOUD) 2010 IEEE 3rd International Conference, pp. 188-195, 2010.

[12] W. Cong, W. Qian, R. Kui, and L. Wenjing, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing" in INFOCOM, 2010 Proceedings IEEE, pp. 1-9, 2010.

[13] R. Ranchal, B. Bhargava, L. Othmane, L. Lilien, A. Kim, M. Kang, and M. Linderman, "Protection of Identity Information in Cloud Computing without Trusted Third Party" in Reliable Distributed Systems, 29th IEEE Symposium, pp. 368-372, 2010.

[14] W. Lifei, Z. Haojin, C. Zhenfu, J. Weiwei, and A. V. Vasilakos, "SecCloud: Bridging Secure Storage and Computation in Cloud" in Distributed Computing Systems Workshops (ICDCSW), 2010 IEEE 30th International Conference on, pp. 52-61, 2010.

[15] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.

[16] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes," 2009.

[17] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.

[18] S. Narayan, M. Gagne´, and R. Safavi-Naini, "Privacy Preserving EHR System Using Attribute-Based Infrastructure," Proc. ACM Cloud Computing Security Workshop (CCSW '10), pp. 47-52, 2010.

[19] X. Liang, R. Lu, X. Lin, and X.S. Shen, "Patient Self-Controllable Access Policy on Phi in Ehealthcare Systems," Proc. Advances in Health Informatics Conf. (AHIC 10), 2010.

[20] L. Ibraimi, M. Asim, and M. Petkovic, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption," technical report, Univ. of Twente, 2009.

[21] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy (SP '07), pp. 321-334, 2007.