International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 03
March 2017

Assured Distribute Data in Cloud Computing using Control Security Model

A. Venkateswarlu[1], S. Jalaiah [2]

[1]PG Scholar, Dept of CSE, Dr.Samuel George Institute of Engineering & Technology, Markapur, Prakasam Dist, AP.

[2] Assistant Professor, Dept of CSE, Dr.Samuel George Institute of Engineering & Technology, Markapur, Prakasam Dist,AP.

Abstract: *These PHR contains sensitive data is protected from unauthorized parties. But the service providers are uses many security and privacy risks for PHR. Recent years have witnessed a widespread availability of electronic healthcare data record (EHR) systems. The process of treatment in medical centers such hospitals, clinics, or other institutions. We present a new type of attribute-based encryption that is multi-authority attribute-based encryption (MA-ABE) scheme which is used to enforce patient access control policies. In MA-ABE the data is encrypted according to an access policy over a set of attributes. A high degree of patient's privacy is guaranteed. Extensive security and result analysis shows that the proposed scheme is highly efficient. Role of one user is encrypted to another user such that scalability, access control and efficient user revocation is achieved and also it proves the security of HASBE based on security of the Cipher text-Policy Attribute-Based Encryption (CP-ABE) scheme and analyse its performance and computational complexity.a novel Context-aware Access Control Security Model (CARE) is proposed to capture the scenario of data interoperability and support the security fundamentals of healthcare systems along with the capability of providing fine-grained access control. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE.*

Index Terms: Cloud Computing Hybrid cryptography, Privacy; Security regulations; Interoperability, Fine-Grained Access Control, MA-ABE,

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 03
March 2017

1. INTRODUCTION

Today healthcare delivery has exponentially extended from acute institutional care to outpatient care and home healthcare. A healthcare service is availed at a distance due to the advances in communication and information technology [1]. These are a number of initiatives for adoption of electronic health records (EHRs) many governments and world as well as from the private sector for adoption of personal health records (PHR). While EHR systems function to serve the information uses of health care professionals, PHR model health data entered by individuals and provide data related to the care of those individuals [2]. Although of many benefits provided by healthcare systems, nevertheless, there are vulnerable to a wide range of security of their portability and design [3]. Specifically emerged every level of the system, for instance At transmission level [4], and At storage level [5]. These threats were described. In addition to the aforementioned threats, some patients insufficient using healthcare systems applications. So, it is necessary to ensure patients feel fully confident to use the system and have their own security control.We conduct new survey study to analyze the healthcare system's security and destitute threats. We propose a novel security model that captures the model of data interoperability and supports the security fundamental of EHR within the capability of providing fine-grained access control [6]. The patient is decide with total information should be shared. For the fine-grained access of information, Introduces an architecture in which upon request from a person a virtual proxy server will be created for the purpose of accessing the data. Only the person who has the decryption key can enter in to the virtual proxy server [7].

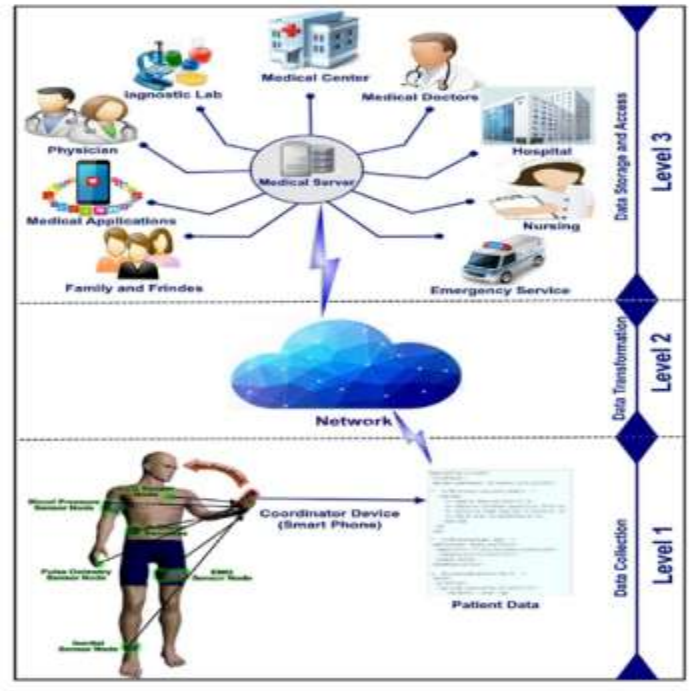

Fig. 1. The architecture of Healthcare Monitoring System

2. RELATED WORK

User secret keys is defined to reflect their access structures so that a user is able to decrypt a cipher text if and only if the data file attributes satisfy his access structure. Such a design also brings in the efficiency benefit as compared to existing works to complexity of encryption is just related the number of attributes associated to the data file and data file creation/deletion and new user grant operations just affect current file/user without new system-wide data file update keying [8].Multi- Authority Attribute-Based Encryption (MA-ABE): MA-ABE method accesses any polynomial number of independent authorities to change attributes and distribute secret keys. An encrypted choose, for each authority [9]. Cipher-text Policy Attribute-Based Encryption (CP-ABE): Using this algorithm [10], encrypted data is confidential and secure the server is un trusted also this prevents collusion attack. Key Policy Attribute-Based Encryption (KP-ABE):In this algorithm[11],the primitive take the senders to encrypt messages under a set of attributes and private keys is associated with access policies that is access structure in this context that specify the cipher text the key holder will be allowed to decrypt.

3. CARE SECURITY MODEL

The Context-aware Access Control Security Model (CARE) system is used on the scenario of data interoperability and supports the security fundamentals of healthcare systems many capability of providing finegrained access control. Specifically the CARE model could is located on the healthcare server which serves as an access point for users' requestsdepicts the architecture of CARE [12].

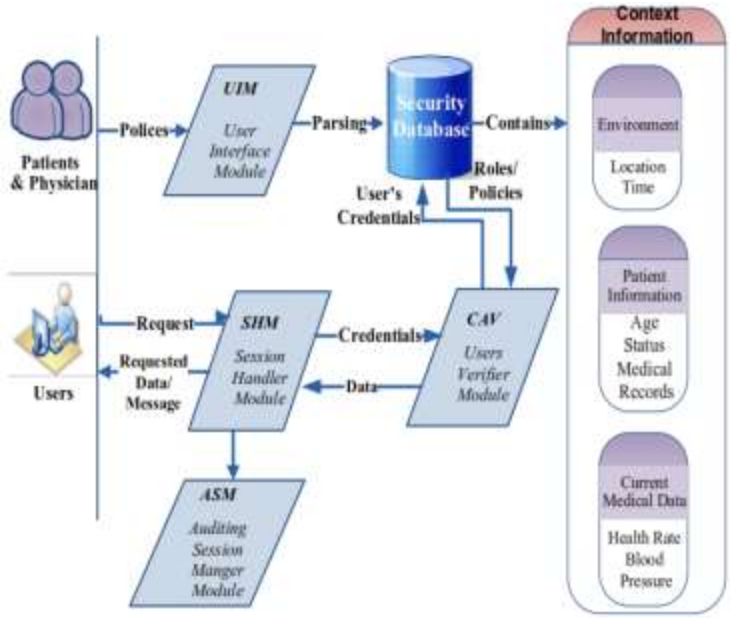

Fig. 2. CARE Model Architecture

In particular, when the patient's life is in danger the security settings are adapted by removing the uses for user authentication to

access the data [13].

4. ALGORITHM

Multi-Authority Attribute-Based Encryption (MA-ABE) [8] [9] is a type of attribute-based encryption model is used to enforce access policies cryptographically. In MA-ABE the data owner encrypts the data according to an access control policy is defined over a set of attributes [15], and the receiving end can decrypt the encrypted data only if his secret key associated with a set of attributes satisfies P. For example, suppose Alice encrypts her data according to an access policy P= (al AND a2) OR a3. Bob can decrypt the encrypted data only if his secret key is associated with a set of attributes that satisfy the access policy. To satisfy P, Bob must have a secret key associated with at least one from the following attribute sets: (ab a2), (a3) or (al, a2, a3)' In general, MA-ABE scheme consists of four algorithms [14]:

1. Setup algorithm (MK, PK) Setup (1 k): is run by the trusted authority The setup algorithm takes as input a security parameter k and outputs a master secret key MK and a master public key PK.

2. Key Generation algorithm (SK) Key Gen (MK, ffi): is used the trusted authority, and takes as input a set of attributes wand MK. The algorithm outputs a user secret key SK associated with the attribute set w.

3. Encrypt algorithm (CT) Encrypt (m, PK, P): is run by the encrypted master public key PK and an access control policy P, the output of the algorithm is a cipher-text CT encrypted under the access control policy P.

4. Decrypt algorithm (m) Decrypt (CT, SK): is run by the decryptor. The input of the algorithm is a cipher-text CT to be decrypted and a user secret key SK. an error message if the attribute set of the secret key does not satisfies he access policy P under which the message was encrypted.

A. .MD5 ALGORITHM:

MD5 is cryptographic hash function in which produces 128bit hash value. The message digest algorithm is used for digital signature application, where a large file must be "compressed". For securing the password and using MD5 algorithm. MD5 algorithm is one way encryption technique. Five step to compute message [16]:

Step1: Append padding bits: Message is pad so its length is 448 mod 512.

Step2: Append Length Append a 64-bit length value to message Generate a message with 512 bits in length.

Step3: Initialize MD buffer Initialize a 4-word (128-bit) MD buffer (A, B, C, D)

Word A: 01 23 45 67 Word B: 89 AB CD EF Word C: FE DC BA 98 Word D: 76 54 32 10

Step4: Process Message in 16-word block Process message in 16-word (512-bit) blocks.

Step5: Output.

B. HYBRID CRYPTOGRAPHY

In cryptography public-key cryptosystems is modify the sender and receiver to share a common secret in order to communicate securely they often rely on complicated mathematical computations and use generally efficient inefficient than comparable symmetric-key cryptosystem [17].A hybrid cryptosystem is constructed using any two separate cryptosystems: 1. A key encapsulation scheme, which is a public-key cryptosystem

2. A data encapsulation scheme, which is a symmetric-key cryptosystem.

The hybrid cryptosystem is itself public-key system public and private keys are the same as in the key encapsulation scheme. A simple and security to build an encryption model is unrestricted message is to build a hybrid encryption scheme. Loosely speaking such a scheme uses public-key encryption techniques to encrypt a key K that is then used to encrypt the total message using symmetric key encryption schema [18]

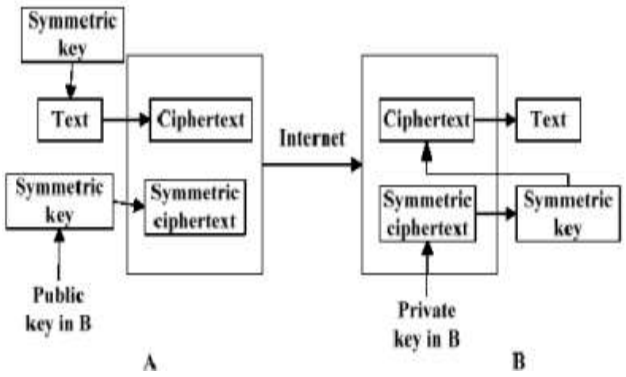

Figure 3. Hybrid Cryptosystem

C.SECURITY ATTACKS IN HEALTHCARE SYSTEM

Healthcare systems are vulnerable to penetration small attacks from users for profit. This damages the effectiveness performance of healthcare model. Specifically, insulin pump sensors, hospital networks, or the personal health data is hacked or stolen by small users [19]. Attacks at data collection level These attacks is many threats to data collection level such as altering information dropping some important data resending data messages. Jamming Attack refers to interference attacker's radio signal with frequencies of the BAN (Body Area Networks). Resulting in isolating and preventing network node within the range of the attacker signals for giving or receiving any message many the affected nodes and other sender nodes [20].

The modular design makes the system configuration very effective and simplifies the composition of policies to deploy safer and more secure medical sensor networks the critical or emergency case raised, the medical stuff is override the restrictions to access sensitive data that was restricted in normal condition. One of the limitations of this model is that there is no detection mechanism for unauthorized access when critical situations occur

5. RESULT

After establishing the session, the Users Verifier Module (CAV) verifies the requester credentials and then determines if the user access the requested data or not. This is done by contacting the security database and retrieving the applicable model and requester's assigned roles. CAV also classifies the request's cases as critical, emergency, or normal depending on the context-aware data and then adjusts the final access decision.

File Size (KB)	Encryption Time (msec)	Decryption Time (msec)
800	12827	3516
500	9089	2869
150	3803	1639
100	2563	982

Fig No 4 Result Data

6. CONCLUSION

As suggested in paper, secure management of personal health records which is stored and shared from any un-trusted web server is managed. The MA-ABE scheme has shown to be a useful tool in a healthcare setting since the access policy is enforced by virtually associating the access control policy to the protected data.A novel context-aware access control security model that supports the security fundamentals of healthcare systems and providing fine-grained access control. The model consists of multiple modulesevery charge of taking a different type of task. This modular design aims at simple and efficient access control decision depending on the patient's situation and the requester assigned roles. Privacy and security to the medical data which is stored in the third party cloud storage. It prevents attackers and hackers by using new cryptographic techniques like hybrid

encryption and attribute based encryption. In future we propose document security and query privacy to increase the efficiency and also to reducing key management problem for enhancing privacy guarantee.

7. FUTURE WORK

Data needs more security. If the key that has to be encrypted is as same length as the message then using public key cryptography is of no use. Now days there are many cryptographic present for the efficient encryption and decryption. These are adopted for the better security for the data's that are stored in the cloud storage.

8. REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in SecureComm'10, Sept. 2010, pp. 89–106.

[2] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient Centric and FineGrained Data Access Control in Multi-Owner Settings,"Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.

[3] Om, S. and M. Talib, Wireless Ad-hoc Network under Black-hole Attack. International Journal of Digital Information and Wireless Communications (IJDIWC), 2011. 1(3): p. 591-596.

[4] Ramli, R., N. Zakaria, and P. Sumari, Privacy issues in pervasive healthcare monitoring system: A review. World Acad. Sci. Eng. Technol, 2010. 72: p. 741-747.

[5] Partala, J., et al. Security threats against the transmission chain of a medical health monitoring system. in e-Health Networking, Applications & Services (Healthcom), 2013 IEEE 15th International Conference on. 2013. IEEE.

[6] Niksaz, P. and M. Branch, Wireless Body Area Networks: Attacks and Countermeasures.

[7] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM " 10, 2010.

[8] Cong Wang, KuiRen, Shucheng Yu and Wenjing Lou "Achieving Secure, Scalable,

and Fine-grained Data Access Control in Cloud Computing", INFOCOM, 2010 Proceedings IEEE,march 2010.

[9] Melissa Chase "Multi-authority Attribute based Encryption," Computer Science Department Brown University Providence, RI 02912.

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

[11] Jin Sun,Yupu Hu and Leyou Zhang," A Key-Policy Attribute-Based Broadcast Encryption," The International Arab Journal of Information Technology, Vol. 10, No. 5, September 2013.

[12] Partala, J., et al. Security threats against the transmission chain of a medical health monitoring system. in e-Health Networking, Applications & Services (Healthcom), 2013 IEEE 15th International Conference on. 2013. IEEE.

[13] Niksaz, P. and M. Branch, Wireless Body Area Networks: Attacks and Countermeasures

[14] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.

[15] Y. Zheng, "Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption," master's thesis, Worcester Polytechnic Inst., 2011.

[16] J. Bethencourt, A. Sahai, and B. Waters,"Ciphertext-policy attribute-based encryption," in IEEE S& P '07, 2007, pp. 321– 334.

[17] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW " 09), pp. 103-114, 2009.

[18] G. Ateniese, K. Benson, and S. Hohenberger, "Key-Private Proxy Re-Encryption, "Proc. Topics in Cryptology (CT-RSA),pp. 279-294, 2009.

[19] Saleem, S., S. Ullah, and H.S. Yoo, On the Security Issues in Wireless Body Area Networks. JDCTA, 2009. 3(3): p. 178-184.

[20] CHELLI, K. Security Issues in Wireless Sensor Networks: Attacks and

Countermeasures. in Proceedings of the World Congress on Engineering. 2015.

Student details:

A.VENKATESWARLU currently pursuing his M.Tech.in computer science and engg in Dr.Samuel George institute of engg&technology,Markapurm,Andhra Pradesh, affiliated to JNTU, Kakinada. He has done his B.Tech. Degree from ABR Engg&Tech,Kanigiri affiliated to JNTU, Kakinada, Andhra Pradesh,India

Guide details:

S.Jalaiah received B.Tech (CSE) Degree from JNT University, Hyderabad in 2008 and M.Tech (CSE) Degree from JNTUK Kakinada in 2011. He has 6 years of teaching experience. He joined as Assistant Professor in Dr.Samuel George Institute of Engineering & Technology, Markapur, Prakasamdt, AP. Presently he is working as Assistant Professor in CSE department. He published international journal on Robustly Detecting and Eliminating the Conflicts in Firewall Policies. He attended Various National and International Workshops and Conferences on Computer networks.