International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 21 Issue 2 – APRIL 2016.

SECURITY AND PRIVACY OF CLOUD DATA USING HEALTH CARE SYSTEM

Anlet Anusha, Sibi Varthan K, Sandeep K, Subramanian S, Siddharth Oza V

[#1]*Assistant Professor (O G), Computer Science Department, SRM University, Ramapuram, Chennai, India*
[*2*3*4*5]*Student, Computer Science Department, SRM University, Ramapuram, Chennai, India*

anletanusha@gmail.com
sibivarthan1@gmail.com
subramanian.sathyanarayanan@hotmail.com
sandeeparjun79@gmail.com

***Abstract*--Personal health records (PHRs), it gives the patients to store, manage, and shares their personal health information. The sick patients can track their disease, symptoms, treatment and maintains the connection with their care providers. The PHR is invalid for the people with less sickness in self-managing health that reduces costs. For treatment the PHRs improved the communication for patient care provider and it enables information available in traditional treatment, mainly emergency care. The biometrics technology is more efficient to provide tight security for health care data or e-health card data maintenance. This project implements a biometrics based e-health card monitoring system. The healthcare providers, insurers and employers are offers an increasing variety and amount of information flows through the PHR database.**

Keywords:
Advance Encryption Standards (AES), Personal Health Records, Cloud Data, Security and Privacy, Healthcare System, Encryption, Decryption, PHR.

I. INTRODUCTION

Cloud computing is derived from traditional distributed computing where the data storage service rely on a trusted third-party server. The PHR contains information about the patient’s medical records like medications, mental health, genetic orders, behavior, lifestyle, beliefs, and habits. The data can be shared with the patients to receive proper medical care, but the other data are kept private, since unauthorized usage could harm the patient. The PHR data contains high commercial value for black marketers, identity thieves, and corrupted organizations.

Thus the PHR system offer new opportunities for personal health care management and has serious privacy threats. The patients worried about the secondary data use, which provides confidence in the PHR system. To reverse this step, researchers must input both legal and technical challenges prevent unauthorized usage in PHR.The building and maintenance specialize the data centers or provides third-party services.

It is mainly focused on the central cloud computing system which is not sufficient for efficiently processing the increasing volume of personal health information in m-healthcare system. But it is not enough for assuring the data confidentiality of the patient’s PHI, The communication can lead the adversary to conclude that the patient is suffering from a specific disease with a high probability. But the problem is how to protect both the patients’ data privacy and identity in the m-healthcare cloud computing system under the malicious model which is left behind.

To overcome these problems, the proposed system presents an efficient biometric based authentication system for government primary health care system. This system provides strong security in the terms of authentication and data maintenance authorization. It avoids the data misuse and bribing by unauthorized person.

This system will avoid processing the large amount of paper based manual work. This data can be easily accessed by anywhere by utilization of proper authentications. By achieving the data confidentiality and identity privacy with higher efficiency, But they can only access the personal health information, not the patient’s identity. To achieve a scalable data or complete accessed control for PHRs, The Advance Encryption Standards (AES) Algorithm is used to encrypt each patient’s PHR file.

II. RELATED WORK

The Advance Encryption Standards (AES) is a block cipher that encrypts a 128-bit block (plaintext) to a 128-bit block (ciphertext), or decrypts a 128-bit block (ciphertext) to a 128-bit block (plaintext). It is a symmetric key encryption algorithm uses a cipher key whose length is 128 bits, 192 bits or 256 bits. The AES algorithm with a cipher key of length 128, 192, 256 bits is denoted AES-128, AES-192, AES-256, respectively. In this case the entire data block is processed in parallel during each round using substitutions and permutations.

The number of AES parameter depends on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128 bit key. Rijndael was designed to have the following characteristics are Resistance against all known attacks, Speed and code compactness on a wide range of platforms, Design Simplicity. AES operates on an input data block of 128 bits and its output is also a data block of128 bits.

The AES algorithm starts with a whitening step, implemented by XOR the input data block with the first 128 bits of the cipher key. These 128 bits are the whitening key. The algorithm continues with 10/12/14 rounds, each one using another round key. When counting this way, the rounds and the round keys are counted from 1 to 10/12/14. The whitening step is also referred to as “Round 0”,and the corresponding 128 bits of the whitening key are referred to as Round Key 0. In that case, the count of the AES rounds and the round keys starts from 0 to 10/12/14.AES uses a cipher key whose length is 128, 192 or 256 bits. This cipher key is expanded into 10, 12, or 14 round keys, respectively, using the “Key Expansion” algorithm, where the length of each round key is 128 bits. This Key Expansion Algorithm depends only on the cipher key. Since it is independent of the processed data, it can be executed prior to the encryption and decryption phase.

III. TECHNIQUES

The Techniques used in Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive data. It has been adopted by the United States government as anAdvanced Encryption Standard, a standard algorithm used to encrypt and decrypt sensitive information. AES is a symmetric block cipher with a block size of 128 bits. It allows for three different key lengths which can be 128 bits, 192 bits, or 256 bits; referred to as AES-128, AES-192, and AES-256, respectively.

The number of rounds in the encryption process for AES-128 is 10, for AES-192 it is 12, and for AES-256 it is 14.A performance reveals, going from 128 bits key to 192 bits key causes increase in power and time consumption by 8% and 256 bits key causes an increase of 16%. So we propose use of industry-standard high AES symmetric encryption algorithm with key length of 128-bits for this purpose.

IV. ARCHITECTURE

The PHR selects theattributes from the PHR file to give the access rights to the users. The owner provides access keys toattribute authorities in case of public domain and to the users in personal domain. Here, the PHR file is encrypted symmetrically with advanced encryption standard (AES) and the symmetric data key is again encrypted according to an access policy over a set of attributes, which specifies the owner is willing to share their data and the data owner stores the encrypted data along with encrypted license on the trusted third party (cloud server).

The users request the data from the cloud server using the access keys. These users can access the data from the cloud server after all the key verifications and access policy verifications are satisfied. The emergency staff can also access the data using the keys in emergency situations. The PHR owners assign the access keys to the emergency departmentfor the glass break scenario. The access keys are provided to the emergency staff from the emergency department in case of emergency.

Theseaccess keys assigned to emergency department is taken back by the owner after the glass break scenario, and again assigns new key to the emergency department. The revocation of access keys, access policy rights from the cloud server can also be done by the PHR owners when they required.

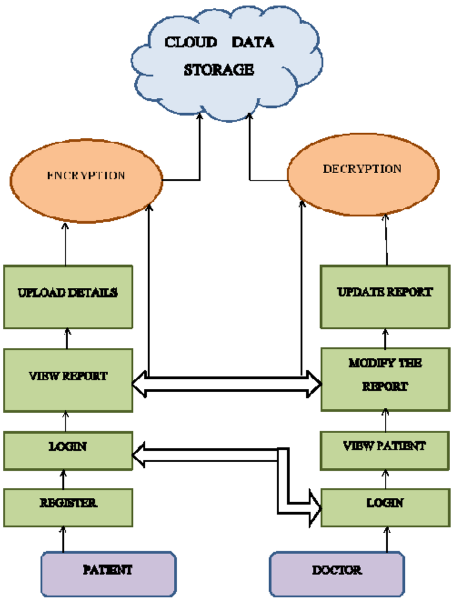

Figure 1: Overall Architecture

The cloud based Primary Health Care system consists of the healthcare providers, pharmaceutical companies, IT solutions and the patients. The healthcare process involves massive healthcare data which exists in different forms on disparate data sources, in different formats where patient information is entered into Personal health record(PHR) system.

V. COMPARISON

The AES Algorithm is more suitable than ABE, which is considered to be more expensive. So the data is not directly encrypted. Generally symmetric key is used for encrypting bulk of the data and asymmetrickey like ABE is suitable for encrypting short key value. First data is encrypted using AES with 128 bits keys and the AES keys are again encrypted or decrypted using ABE and are sent together with ciphertext.
During that clock cycle (*only* during the clock cycle), The128 bit data can be read back from TEXT_OUT. This data will be the encrypted data.

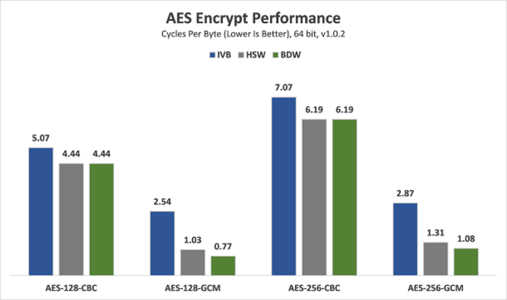

Figure 2: AES Encrypt Performance

There are two equivalent ways to perform AES decryption, one is called the “Inverse Cipher” and the other is called the “Equivalent Inverse Cipher”. They differ in the internal order of the sequence of the transformations, and also in the way that the decryption round keys are defined.

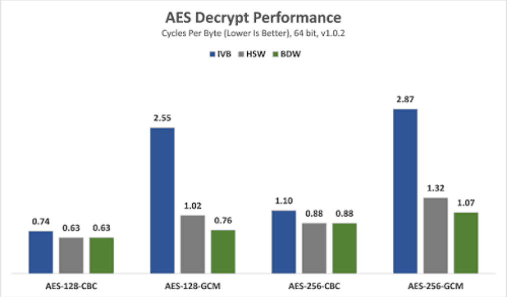

Figure 3: AES Decrypt Performance

AES makes use of 10, 12 and 14 rounds. The plain text is transformed into cipher text after repeated transformation rounds in AES. This makes the data secure on the cloud.

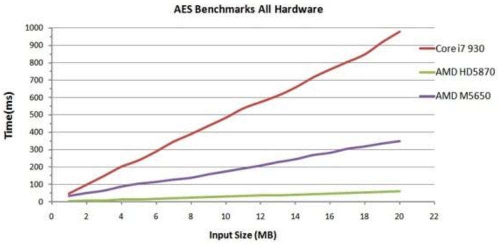

Figure 3: Comparative Strength of AES

To test whether the speed is sufficient for streaming the audio decryption, This system can easilybe used to decrypt encrypted data in external memory ahead of time, before playback. It is also possible for decryption.

VI. CONCLUSION

In this paper,This system uses double layer protection in which the PHRs are stored in the cloud.Considering the trustworthy cloud servers, we realize the patient-centric concept, patients shall have complete control of their own privacythrough encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we enhance the privacy guarantees compared with previousworks. It provides important performance and security benefits. AES is the leading standard for symmetric encryption used in a variety of applications.

VII. FUTURE WORK

The Cloud computing is likely to suffer from a number of known vulnerabilities, enabling attackers to either obtain computing services for free or steal information from cloud users. In the world of computing, security and privacy issues are a major concern Bysecuring the outsourced data and computation against mistrusted clouds is indeed costlier than the associated savings, with outsourcing mechanisms costlier than their non-outsourced locally run alternatives. It can be done to use the AES logic in streaming applications, Mobile applications using biometric algorithms and sensors similar to our original project goals.

It can be also used in the conjunction with a network interface in order to send secure information over the internet.In the first layer, the images and the text files areencrypted using Advanced Encryption Standard (AES). In the second layer, the encrypted files are divided into n files. These n files are then stored in the cloud. The original PHR can be decrypted only if the n files are merged. For splitting and merging the ciphertexts, a sequence key will be used.

REFERENCES

[1] Wright and D.F. Sittig, “Encryption Characteristics of Two USB-Based Personal Health Record Devices,” *J. Am. Medical Informatics Assoc.*, vol. 14, no. 4, pp.397-399, 2007

[2] J. Li, “Privacy Policies for Health Social Networking Sites,” *J. Am. Medical Informatics Assoc.*, vol. 20, no. 4, pp 704-707, 2013.

[3] K.D. Mandl et al., “Indivo: A Personally Controlled Health Record for Health Information Exchange and Communication,” *BMC Medical Informatics and Decision Making*, vol. 07, no. 25, pp. 1–10, 2007.

[4] J.M. Grossman, T. Zayas-Caban, and N. Kemper, “Information Gap: Can Health Insurer Personal Health Records Meet Patients’ and Physicians’ Needs,” *Health Affairs*, vol. 28, no. 2, pp. 377-389, 2009

[5] T. Rindfleisch, “Privacy, Information Technology, and Health Care,” *Comm. ACM*, vol. 40, no. 8, pp. 93-100, 1997.

[6] Li, M., Xiao, D., Peng, Z., and Nan, H., “A modified reversible data hiding in encrypted images using random diffusion and accurate prediction”, ETRI J., 2014, VOL.36, (2), pp. 325–328.

[7] https://netbeans.org/downloads/

[8] https://www.java.com/

[9] [10] Programming With Java: A Primer 4th Ed by E Balagurusamy |Author;-English-Tata McGraw Hill Education Private Limited-Paperback_Edition-4th : A Primer (English) 4th Edition.