International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020

Security of Stored Data using AES Algorithm for Hospital Management System

Arnav Mehta, Gaurav Jain, Abirami G

Abstract: ***Securing data of patient in hospital is need of hour since hackers can misuse this data for doing some scam. There is increase in number of cyber attacks on healthcare organizations and the cybercriminals developing more sophisticated tools to attack healthcare industry, therefore security of healthcare has become more important. Many incidents have been reported, where patient comes to hospital routine blood check up, but pathologist hack old data of patient and generate a fake report by putting figure based on old data of last report and fool patient. There are scandals wherein certain organization hack the system of well reputed hospital to get private information about patient history and health record and misuse this information which lead to lot of agony and harassment to patient. Cyber attacks cause major disruption in healthcare services even in the best of time. Our project will ensure that that patient's data remain secure and does not goes into hand of wrong people. In this paper we have discussed method to store healthcare data in data in cloud and use AES encryption algorithm to encrypt data, so it does not go into wrong hand.***

Keywords: AES (Advance encryption Standard), Public Auditing, Integrity Check, Key-aggregation cryptosystem (KAC)

I. INTRODUCTION

Now a days people's immunity is deteriorating and lifestyle diseases cases are increasing, this along with greater health awareness, higher life expectancy, rising income level and increased role of government in healthcare investment had resulted in sharp growth of healthcare industry. Effective and efficient services for patients are very much important to healthcare organization compared to other organization, as failings can result in fatal consequences.

Healthcare data helps in improving patient treatment, preventing diseases, foresee epidemics and reduce cost with better quality of life, therefore huge amount of data is required to be stored, maintained and transmitted for delivery of efficient service and proper care; however there is lack of technical support with almost no security. Further the healthcare industry is more prone to data breaches. There is rise in data breaches on confidential healthcare data. Cyber criminals use data mining techniques to get sensitive information related to patient. These cyber criminals can use this information to blackmail patient for extorting money or can sell this information to pharmaceutical company to give them new clients to which they can sell their products to. Therefore, it is necessary for healthcare industry to protect its clinical as well as administrative data by implementing data security solutions.

Healthcare organization create a cloud computing environment for patient's complete history and this Electronic Health Records enables physicians and patients to access information from any place thus reducing the cost of processing, storing and updating. In spite of many advantages of Cloud Computing, it has disadvantage of security of data from unauthorized access. This paper covers the encryption of data by AES and storage of encrypted data in Cloud.

Revised Manuscript Received on April 25, 2020.
* Correspondence Author
Arnav Mehta*, Department of Computer Science and Engineering, SRMIST, Kattankulathur, India. Email: arnavmehta25@gmail.com
Gaurav Jain, Department of Computer Science and Engineering, SRMIST, Kattankulathur, India. Email: gj21041998@gmail.com
Abirami G, Department of Computer Science and Engineering, SRMIST, Kattankulathur, India. Email: abiramig@srmist.edu.in

II. RELATED WORK

In this paper, [1] the author has mentioned about secure and efficient multi-keyword search on encrypted cloud data. The method provide user with protection of data against violate of privacy of encrypted data which is stored in remote data base. The effectiveness of this scheme is incremented by using symmetric key encryption method for encryption of file rather than public key encryption. However, cost of computation is quite high as every query search requires homomorphism encryption. During this paper, [2] the author has mentioned about how the third-party auditor (TPA) efficiently audits the integrity of shared data, however it is not able distinguish among the one who has retrieved data. So in order to remove this confusion here they have used method of providing security key to each user to know which one of them have retrieved data .Here data is kept private from TPA and also TPA is able to check if file is safe or not without retrieving the entire data base. However, this scheme does not support dynamic group. In this paper, [3] the author has mentioned how a user is revoked from the group then the data of that user cannot be used and retrieved by anyone. The which is used by revoked user earlier for retrieving their data is made ineffective so that no other user can use it to get data of revoked user. However, when a user is revoked, a global key is required to be regenerated and shared with existing group, which means a huge eavesdrop on key management and distribution.

III. METHODOLOGIES

The proposed system uses a public auditor who works exactly like a TPA. It sees for if our data (which is stores in our pseudo cloud i.e. D drive) is safe from the intruder or not without accessing whole data.

Here we even do encryption and decryption of data and storing it of in our pseudo cloud at same time. Here we provide client with security key which they receive via an email after registering as our user which can be used to decrypt our data anywhere, at any place and at any time when they want without waiting for TPA hence increasing our efficiency and wasting less time of former .For achieving it we have developed our proposed system in four module. Four steps in proposed approach are:

A. Registry of New User

Registration of new user is done in same way as we create new login in other social networking sites. First, we have to enter all our details such as name, date of birth, mobile number etc. and then we have to select the group in which we want to get add in and then we have to complete our **REGISTRATION**. Once this registration gets completed then we receive a security key on our registered email id by our group manager which can be used to decryption of our file.

B. Public Auditing

We have uniquely integrated Homomorphic authenticator with random mask technique. This help in achieving privacy preservation. The unforgeable verification is generated from individual Meta block. In Homomorphic authenticators, from individual Meta data blocks an unforgeable verification is generated. In this protocol, the randomness is generated by pseudo random function. This random function is used for masking liner combination of sampled block. The scheme to be proposed is as follows:

i. Setup Phase
ii. Audit Phase

C. Sharing Data

Encryption is done with key-aggregate cryptosystem (KAC) which is approved application for Sharing of data. The property of aggregation is very used when we need client to be flexible & efficient. In this scheme a single short aggregate key is provided to each authorized user. With this key content provider is able share data private and selective way by using a fixed short ciphertext expansion. This is done by sending the security key to our client through their email.

D. Integrity Check

For ensuring privacy-preserving, public risk auditing is for supporting data dynamic. This scheme is used to build upon the existing work which supports data dynamics and block level operations of insertion, deletion and modification. We have used this technique with support of data dynamic in public risk design. The user can download the desired file and it is not necessary to download entire files

IV. IMPLEMENTATION

We have used AES (Advanced Encryption Standard) for data encryption and decryption. In existing system, Third Party Auditor (TPA) is required for carrying out encryption and decryption checks for hacker intrusion, however for small scale. Fig. 1 shows the AES communication diagram and it has included cloud server .

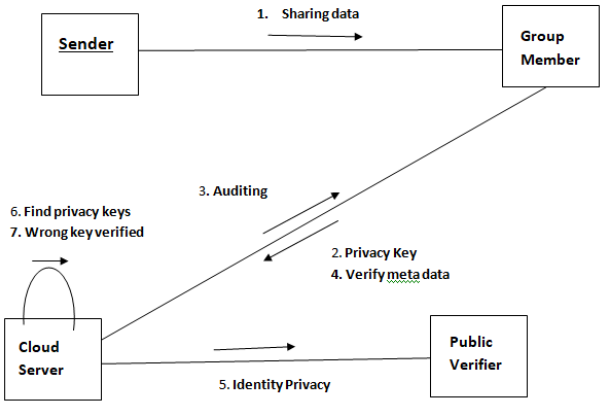

Fig.1. Communication Diagram representing 4 step of AES

Industry and Hospital where they don't have to deal with large amount of data , presence of such a system may not be economical as they have to pay large sum of money to buy a cloud for storing small amount of data and hiring a TPA to maintain it.

Therefore, we have designed our proposed system in such a way that we can use the system to encrypt and decrypt our file. Fig 2 eliminated the need of a TPA and, we have used a pseudo cloud i.e. Storage area (D drive) of the system to store our file.

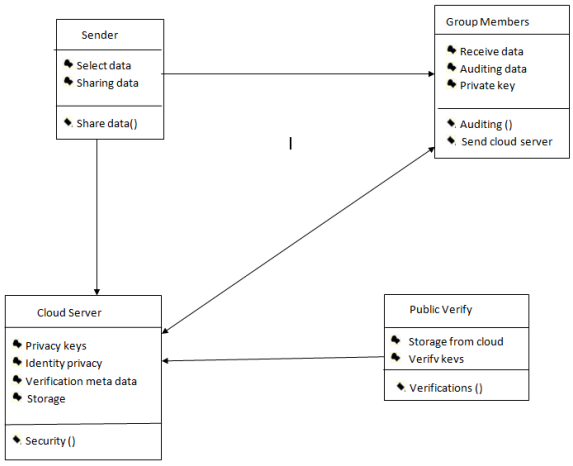

Fig.2. Class Diagram representing component of existing System

Use of AES algorithm provides us with great security to our data as offenders cannot hack encrypted data except by Brute Force Attack.

V. RESULT

After following 4 steps of 10 cycles of size 128 bytes our data gets encrypted in fig. 3 and doing the reverse will get our data decrypted in fig. 4.

ag3 - Notepad

File Edit Format View Help

patient_name	patient_id	doctor_consulting	doctor_roon_no	doctor_id
arnav mehta	100	dr.gaytonde	502	200
gaurav jain	101	dr.hariom	504	202
rohan kumar	102	dr.krishna	500	201
rahul kumar	103	dr.haroi	501	203
raunak	104	dr.hari	503	204
hritik c	105	dr.sasi	505	205
hritik s	106	dr.sasi	505	205
nischal l	107	dr.haroi	501	203
apurv	108	dr.hariom	504	202
anurag m	109	dr.haroi	501	203

Fig. 3. Data set Pre encryption

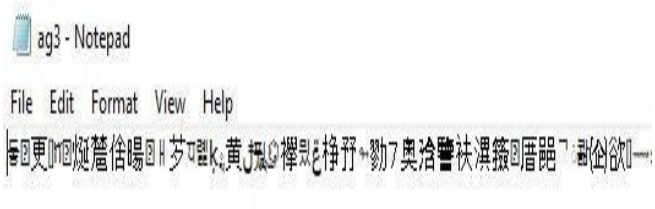

Fig. 4. Data set post encryption

VI. CONCLUSION

Hence, we conclude this paper by proposing elimination of cloud and using a drive instead which we use as a pseudo cloud, removing Third Party Auditor from system and include hacker intrusion detector known as auditor to detect hacking of file. Hence we are easily be able to encrypt and decrypt the data set of hospital and store it safely into our pseudo cloud by providing it with greater security and provide less time to our intruder to intrude into our system and hack into our data.

REFERENCE

1. The MD5 Message-Digest Algorithm (RFC1321). https://tools.ietf.org/ html/rfc1321, 2016.
2. Revathy B, Anubani, Rohith V. "Enabling Secure and Efficient Multi Keyword Ranked Search over Encrypted Cloud Data" .
3. B. Wang, B. Li, and H. Li, "Certificate less Public Auditing for Data Integrity in the Cloud," Proc. IEEE Conf. Comm. and Network Security (CNS'13), pp. 276-284, 2018.
4. B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data withEfficient User Revocation in the Cloud," Proc. IEEE INFOCOM, pp.2904-2912, 2017.
5. C. Wang, S.S. Chow, Q. Wang, K. Ren , and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans.Computers, vol. 62, no. 2, pp. 362-375, Feb. 2018.
6. Qiang Duan, Yuhong Yan, A.V. VasilakosA Survey on Service-Oriented Network Virtualization Toward Convergence of Networking and Cloud Computing Network and Service Management
7. Mohit Marwaha1, Bedi. RajeevApplying Encryption Algorithm for Data Security and Privacy
Cloud in International Journal of Computer Science Issues (2013)
8. Gartner worldwide total public cloud Market. http://www.gartner.com/newsroom/id/2352816.
9. Hassan Tabaki, James T.B. Joshi,Gail joon Ahn, Security and privacy computing Challenge in cloud computing IEEE(2017)

AUTHORS PROFILE

Arnav Mehta is pursuing his Bachelor of Technology in the department of Computer Science and Engineering at SRMIST (formerly known as SRM University). He has also completed an internship in data base management from Center of Railway Information System., Chennai in 2018. Currently, he is placed in a well-known IT company as associate programmer.

Gaurav Jain is pursuing his Bachelor of Technology in the department of Computer Science and Engineering at SRMIST(formerly known as SRM University). He has also completed an internship in Web Development from Keen Infotech., Udaipur in 2018 .Currently, he is placed in a well-known IT company as assistant programmer.

G. Abirami is an Assistant Professor in the Department of Computer Science and Engineering at SRMIST (formerly SRM University). She received her B.E. degree in Computer Science and Engineering from the Bharathidasan University, India in 2003 and an M.E. degree from Annamalai University, India in 2008. She is pursuing a Ph.D. degree in Access control mechanism at the Department of Computer Science and Engineering in SRMIST, India. She is a member of IET, ACM, and ISCA.