Smart Cloud Based Medical base Application Having Data Authentication Control Using Time Constraint

[1]KhusbooHedau, [2]NamrataChaudhari,[3]GayatriDavhale,[4]BabliChoudhary, [5]Prof. M.A. Rane

ABSTRACT:
In the recent years, storage of the data and its security is the big issue in any organization. Cloud Computing is an emerging paradigm which changes the way in which the information is managed. End users can access Cloud services without any expert knowledge. Cloud computing technology provides a huge infrastructure and offers large scale services to the Healthcare industry. Indeed, there are several security challenges such as losing physical control, multitenancy and privacy breach. This project is focusing to develop a website for Healthcare organization. The components are Admin (to start the process), Owner (the doctor, who is going to upload the data on cloud), and Users (Patients, Radiologist, Pathologist etc). It will be a centralized system for all the three components. Radiologist and pathologist will have limited access and the patient will have lifetime access to the data available on cloud. There is no need for patients to carry the prescription and maintain the file as the data is stored on the cloud. The patients can see if the update is done by a doctor and other users. In the proposed scheme, Elliptic curve cryptography (ECC) is used to generate digital signature. Also Attribute based encryption (ABE) is used for encryption and decryption.

Keywords: attribute based encryption, elliptic curve cryptography, and smart health application

INTRODUCTION

There is large amount of data generation. So, to manage this data, cloud is used. Amazon S3 is a "simple storage service" introduced by Amazon Web Services that provides storage through a web service interface. Cloud is useful in different sectors like insurance, healthcare, and banking. It is useful because there is sensitive data on their server and cloud is the best way to manage it. There is a need to secure the sensitive data. Sometimes patients don't want to disclose their data. Also they don't want to disclose their identities. The authentication process normally involves disclosing users' private information such as username and password to the authentication server. If the patient can be linked or tracked by the authentication server or malicious adversaries by their requests, their privacy can be breached. In this paper, we have proposed a system which provides complete privacy and anonymity to the users of health care applications from adversaries and the authentication server. In our proposed authentication scheme, we have utilized rotating group signature scheme based on Elliptic curve cryptography (ECC) to provide anonymity to the patients. The performance of our scheme is evaluated by theoretical analysis which demonstrates that it resists various attacks and provides several attractive security features. Recent advances in biosensors, wireless network and embedded systems have assisted the rapid development of a wide range of wearable and implantable sensors in the human body. To collect crucial health data such as blood pressure level, and heart rate, many smart phone based health applications have been developed in the recent past [1], [2]. The data from the sensors is sent to the cloud server, where hospitals have hosted their services for data processing. The data is analyzed to improve the level of healthcare given to the patients. Ideally, patients want hospitals to assist them with high efficiency without revealing patients' identities. The increasing necessity for massive computation and excessive amounts of storage, is driving the healthcare industry to use cloud based servers, because of many advantages they are offering, such as cost saving and scalability.

LITERATURE SURVEY:

So for that many cryptography techniques are used. Some of the terms used in cryptography:
Plain Text: Any communication in the language that we speak referred as plain text. It is understood by both the sender and the receiver and also it will understand by anyone who gets an access to that message.
Cipher Text: Cipher is also referred as secret message. When a readable text is codified as unreadable text using any suitable scheme the resulting message is called as cipher text.
Encryption: The process of encrypt the plain text into cipher text is called encryption.
Decryption: The reverse process of encryption is defined as decryption that is transforming cipher text messages back to plain text is called as decryption.
Key: It is an important aspect for performing encryption and decryption. It is the key which was used for encryption and decryption that makes the process of cryptography secure

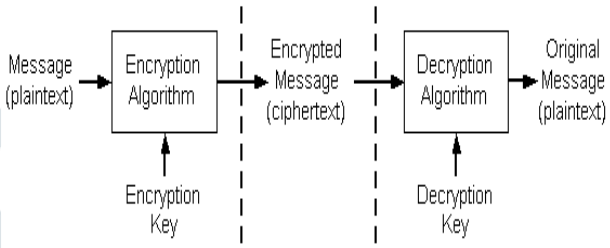

Fig 1: PROCESS OF ENCRYPTIONAND DECRYPTION

D. Aranki, G. Kurillo, P. Yan, D. M. Liebovitz, and R. Bajcsy developed a new system which removes secured channel and constructs a process for verifying the searched result from the cloud server based on key policy attribute-based keyword search (KP-ABKS) of VABKS. It can be effectively to verify the accuracy and integrity of the data file which the data user need for. The major drawback of this system was it lets the users to search the encrypted data without decrypting them.[2]

Deduplication is the techniques which help in saving the storage on cloud. It also reduces the bandwidth of data transferring. Z. Xiao and Y. Xiao studied and presented Deduplication technique. [3]

The public key encryption schemes were studied thoroughly and P. Gope and T. Hwang proposed a technique to conduct approximate equality test. This system gives a solution to search a keyword in mail while routing without revolving the privacy of mail. The issue with this system was that it lacks in security.[5]-[6]

MATHEMATICAL MODEL

Let, S be the System Such that, A= {I, O,
F, Success, failure} Where,

I=. Set of input i.e. text files.

Function:

F1=Encryption Function (This function is used for files)

F2=Conjunctive Keyword Search Function (This function is used for searching)

F3=Time Enabled Proxy-Re-Encryption Function

F4= Decryption Function (This function is used for Decrypting files)

Output:

O1=Success Case (It is the case when all the inputs are given by system are entered correctly)

O2=Failure Case (It is the case when the input does not match the validation Criteria)

SYSTEM ARCHITECTURE:

The figure shows three modules i.e. Admin, Owner and User.

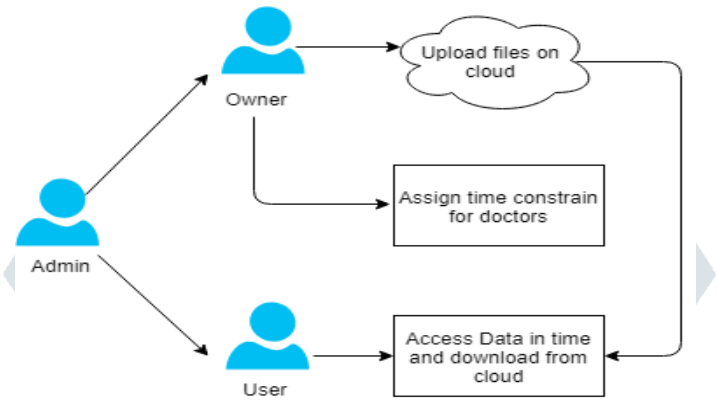

Fig 2: SYSTEM ARCHITECTURE

METHODOLOGY:

The system consists of three modules owner, user and admin. Owner is doctor who will upload file on cloud with time constraint for Radiologist and Pathologist. Users have three type i.e. radiologist, pathologist, and patient. Radiologist and pathologist will have limited access to the data while the patient has a lifetime access. Attribute based encryption technique is used for encryption and decryption. In this system, a signature is generated for file to save the data confidentiality. That signature will be link to file. The signature will be generated using elliptical curve cryptography.[7]

Conclusion:

We have developed this website to preserve the data uploaded on the cloud by encryption and decryption technique. Here we provide duplex security to any file uploaded to cloud with the help of ABE and ECC which generates the digital signature, verifying the correctness of document. This system developed, provides time constraints to particular users. For validation of any user and owner, the admin have to activate or deactivate the account. There is a minimization in the documents as the data is present on cloud. The proposed scheme preserves the privacy of patients when they access the services hosted on the cloud.

ACKNOWLEDGMENT

It gives us great pleasure in presenting the preliminary project report on '**Smart Cloud Based Healthcare Application Having Data Authentication Control Using Time Constraint'.**

I would like to take this opportunity to thank my internal guide for giving me all the help and guidance I needed I am really grateful to them for their kind support. Their valuable suggestions were very helpful.

I am also grateful to HOD for her indispensable support and suggestion.

Name of Students

[1]KhusbooHedau, [2]Namrata Chaudhari, [3]Gayatri Davhale, [4]BabliChoudhary

REFERENCES

[1] A. Martinez-Balleste, P. A. Perez-Martinez, and A. Solanas, “The pursuit of citizens’ privacy: a privacy aware smart city is possible,” IEEE Commun. Magazine, vol. 51, no. 6, pp. 136–141, Jun. 2013.

[2] D. Aranki, G. Kurillo, P. Yan, D. M. Liebovitz, and R. Bajcsy, “Realtime tele-monitoring of patients with chronic heart-failure using a smartphone: lessons learned,” IEEE Trans. on Affective Computing, vol. 7, no. 3, pp. 206–219, Apr. 2016.

[3]Z. Xiao and Y. Xiao, “Security and privacy in cloud computing,” IEEE Commun. Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, May 2013.

[4] D. Ding, M. Conti, and A. Solanas, “A smart health application and its related privacy issues,” in Proc. Smart City Security and Privacy Workshop (SCSP-W), Apr. 2016, pp. 1–5.

[5]P. Gope and T. Hwang, “Untraceable sensor movement in distributediot infrastructure,” IEEE Sensors J., vol. 15, no. 9, pp. 5340–5348, Jun.2015.

[6] X. Su, J. Hyysalo, M. Rautiainen, J. Riekki, J. Sauvola, A. I. Maarala, H. Hirvonsalo, P. Li, and H. Honko, “Privacy as a service: Protecting the individual in healthcare data processing,” Comput., vol. 49, no. 11, pp. 49–59, Nov. 2016.

[7] W. Lei, Y. Li, Y. Sang, and H. Shen, “A secure anonymous authentication scheme for electronic medical records system,” in Proc. 13th Int. Conf. on e-Business Engineering, Nov. 2016, pp. 48–55.