Unidentified endorsement proposal for Cloud Based Medical Applications

[1] Pasme Rutuja Subhash [2], Konde Abhishek Dnyaneshwar [3] Gavane Shubhangi Bhagwan ,
[4] Herkal Neha Rajendra [5] Prof. S. S. Kale

Abstract : Now a days there is a large amount of data generation and we have to store data securely. So here we are developing a healthcare application where we are providing a cloud for storage and provides services to patients. The sensitive data should be saved with the proper authentication. So security and privacy are the main issues while running the cloud applications. So here patient's data can be handled without leaking their data. Here we are considering doctor, patient and admin. Here we are hiding the authentication to cloud server. The authentication server normally involves disclosing of the security like password and username. One easy way to protect their identities from server on cloud is anonymous authentication. The patients information can be tracked by the authentications server and by malicious attack the privacy can be breached. Some traditional approaches fail in the encryption and decryption process 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. To add an extra layer of protection, we have used The Onion Router (TOR) to provide privacy at the network layer. The performance of our scheme is evaluated by theoretical analysis which demonstrates that it resists various attacks and provides several attractive security features.

***IndexTerms* - Component,formatting,style,styling,insert.**

I. INTRODUCTION

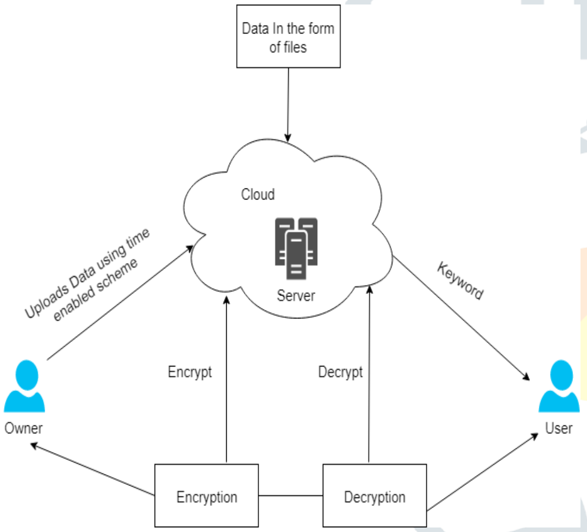
There is large amount of data generation. So we have to manage this data and cloud is used to outsource our data on cloud. To do this we are going to use Amazon s3 to access the data. Cloud is useful in different sectors like insurance, healthcare, and banking. It is useful because there is sensitive data on their server and we have to manage that data. So there is a need to secure this 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. Most of the existing privacy preserving health care applications provide anonymity from the adversaries. However, very few of them provide anonymity from the authentication server. 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. To add an extra layer of protection, we have used The Onion Router (TOR) to provide privacy at the network layer. 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. An example of smart cloud based health applications is shown in

Fig.1. 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.


Data In the form of files
Cloud
Server
Uploads Data using time enabled scheme
Keyword
Encrypt
Decrypt
Owner
User
Encryption
Decryption

Keyword:

Anonymous authentication, rotating group signature, elliptic curve cryptography, smart health applications.

Related Work

The related work on anonymous authentication schemes can be broadly classified into public key cryptosystems (PKC) based schemes [13]–[19], identity based cryptosystems study of STASIS and LSA. These measures of semantic similarity can be applied to short texts for use in Conversational Agents (CAs). CAs are computer programs that interact with humans through natural language dialogue [7]. Tares Finlike proposed a system in which influence of transformation processes in higher education to lower academic standards, changes and deformation in ethical field of global and national higher education. We considered the genesis and modern standards of academic integrity [8]. schemes [4]–[5], pseudonyms based schemes [7], [11], combined scheme [12] using both identity based encryption and pseudonyms, and application oriented schemes [14]–[17]. Anonymous authentication schemes based on PKC in [13], [14] were infeasible for mobile networks because of the computational resources required by PKC modular exponentiation, which consume more resources than what a mobile device can offer. To minimize the computational requirements, various anonymous authentication schemes based on elliptic curve cryptosystem (ECC) have been proposed [15]–[20], which have better performance because of the smaller key size used in ECC. The performance of ECC based schemes are enhanced by identity based cryptosystems [17]–[20] over ECC. Unlike the traditional PKC, the identity based cryptosystems exploit public identity such as ID or email address as the user's public key to eliminate the cost related to the management of public key certificates, which is often desirable in mobile environments.

Motivation:

To secure data. And add privacy to data authentication. To minimize paper work. To prevent data from unauthorized access.

Mathematical Model

Let, S be the System Such that, S= {I, O, F, success, failure}

Where,

S = Proposed system.

Input: Set of Input, Input as patient report. Report in nothing but text,doc file.

Output: Set of Out put

I = Input of system (text file).

F = Functions of the system.

O = Output of the system (Final secure data send).

Function:

F = {F1, F2, F3,F4}

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

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

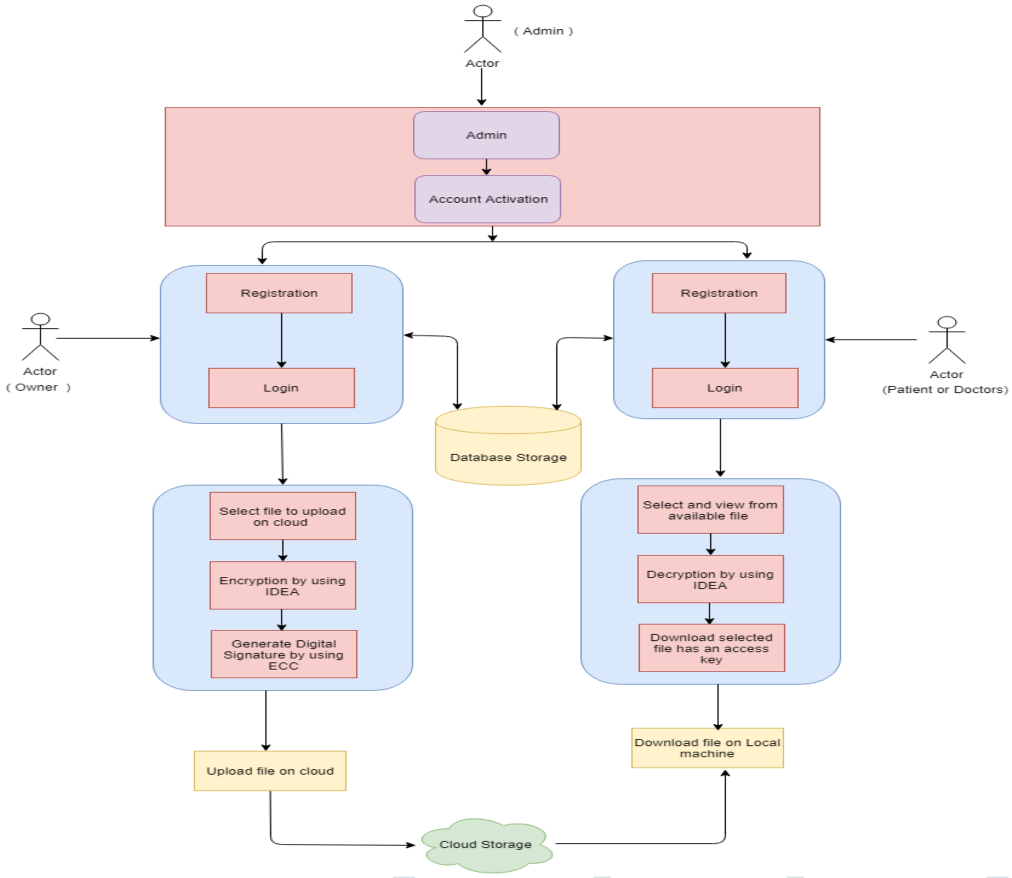
F3=Digital key Generation Function

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

System Architecture:

Figure Shows detailed flow healthcare system here our system consists of three modules owner, user and admin. Owner is doctor who will upload file on cloud with a time period. Users have three types radiologist, pathologist, and patient. Radiologist and pathologist will have limited access and the patient is having lifetime access so that it will be easy to maintain those documents online that to have paper work. Encryption Technique: To encrypt the data using encryption. This process will continue at the time of file upload. For this we are going to use the IDEA(International Data Encryption Standard) algorithm Decryption Technique: Here in this process we are performing decryption at the time of file download to get data in original form.

ECC(Elliptic curve cryptography): In this algorithm we are generating a signature for file to save the data confidentiality. That signature will be link to file.



Conclusion:

In this paper, we have proposed a Encryption, Decryption scheme to realize the timing enabled privacy-preserving keyword search mechanism for the EHR cloud storage, which could support the automatic delegation revocation. The experimental results and security analysis indicate that our scheme holds much higher security than the existing solutions with a reasonable overhead for cloud applications. To the best of our knowledge, until now this is the first searchable encryption scheme with the timing enabled proxy re-encryption function and the designated tester for the privacy–preserving HER cloud record storage. The solution could ensure the confidentiality of the EHR and the resistance to the unauthorized attacks. It has also been formally proved secure based on the standard model under the hardness assumption of the truncated decisional.

ACKNOWLEDGMENT

It gives us great pleasure in presenting the preliminary project report on '**Anonymous Authentication Scheme for Cloud Based Healthcare Applications:**'

I would like to take this opportunity to thank my internal guide Prof. S. S. Kale 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 Prof. Dr. A. V. Dhumane Head of Computer Engineering Department, for his indispensable support and suggestions.

Name of Students

[1] Pasme Rutuja Subhash [2,] Konde Abhishek Dnyaneshwar [3] Gavane Shubhangi Bhagwan, [4] Herkal Neha Rajendra

REFERENCES

- *[1] J. Dauwels et al., "Diagnosis of Alzheimer's Disease from EEG Signals: Where Are We Standing?,"* Current Alzheimer Research, vol. 7, no. 6, pp. 487-505, Sep, 2010.

- *[2] E. Gallego-Jutgla et al., "A hybrid feature selection approach for the early diagnosis of Alzheimer's disease,"* Journal of Neural Engineering, vol. 12, no. 1, Feb, 2015.

- *[3] P. Ghorbanian et al., "Identification of Resting and Active State EEG Features of Alzheimer's Disease using Discrete Wavelet Transform,"* Annals of Biomedical Engineering, vol. 41, no. 6, pp. 1243-1257, Jun, 2013.

- *[4] S. S. Poil et al., "Integrative EEG biomarkers predict progression to Alzheimer's disease at the MCI stage,"* Frontiers in Aging Neuroscience, vol. 5, Oct 3, 2013.

- *[5] J. R. Petrella et al., "Neuroimaging and early diagnosis of Alzheimerdisease: A look to the future,"* Radiology, vol. 226, no. 2, pp. 315-336, Feb, 2003.