JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CAM - Cloud Assisted Privacy Preserving mHealth Monitoring System

[1]A V Murali Krishna, [2]Sravani Gurram, [3]B Santharam, [4]V Rohan Rao

1Assistant Professor in Department of CSE Matrusri Engineering College,Saidabad, Hyderabad, Telangana, India.

2,3,4 UG Scholar in Department of CSE Matrusri Engineering College, Saidabad, Hyderabad,Telangana, India.

Abstract - The use of current cellphone and cloud-based technology to give feedback and decision assistance is known as cloud-assisted mHealth, or mobile health, surveillance, and it has been hailed as a breakthrough method of raising healthcare service quality. reducing the cost of healthcare. Unfortunately, it also offers a significant risk to both customers' privacy and the proprietary information owned by surveillance service providers, which may prevent mHealth technology from being widely used. In order to secure the privacy of the persons involved and their data, this study will address this significant issue and create a cloud-assisted mobile health monitoring system. Additionally, a newly suggested key private proxy re-encryption method and outsourced decryption methodology are modified to move the participating parties' computing complexity to the cloud without sacrificing security Client confidentiality and service providers' proprietary information. Finally, the success of our suggested architecture is demonstrated by our security and performance study.

1. INTRODUCTION

1.1 Introduction

Widespread use of mobile devices, such as cellphones with inexpensive sensors, has already demonstrated significant promise for raising the caliber of healthcare services. Remote portable health monitoring has previously been acknowledged as a viable and a useful technology. A good mobile health (mHealth) application, particularly for underdeveloped nations. The recently released Microsoft project "Medi Net" aims to provide remote information on the health status of cardiac and diabetic disorders in isolated Caribbean nations. A client might use a remote mHealth tracking device to place portable sensors in wirelessly body sensor networks to gather different physiological information, including blood pressure (BP), breathing rate (BR), electrocardiogram (ECG/EKG), peripheral oxygen saturation (SpO2), and blood sugar levels. Then, such physiological information might be blood sugar. Then, a central server might process multiple web medical apps on the physiological data to provide the client with immediate recommendations. These programs may provide a variety of medical consultations, including heart diagnostic systems, exercise monitors, physical activity helpers, and sleep pattern analyzers. A practical solution can also be sought through the incorporation of the application as a service (SaaS) model and pay-as-business arrangement into cloud computing, allowing small businesses (healthcare service providers) to succeed in this medical treatment market. It has been noted that the use of automated decision support technologies in cloud-assisted mobile health tracking has been predicted to become more common in the future. Sadly, despite cloud assistance Although mHealth monitoring might be a terrific way to boost healthcare quality and possibly cut costs, there remains a barrier to making this technology widely available. Client privacy may be seriously compromised throughout collecting, storing, being diagnosed, communications, and processing if data management in a mHealth system is not appropriately addressed. According to recent research, 75% of Americans find the privacy of their medical records to be either important or extremely important. Additionally, when people worry that their voluntarily provided health data may have been compromised, their motivation to participate in health monitoring programmed may be significantly reduced. Due to the rising tendency of privacy violations involving electronic health data, this privacy risk will only become worse.

2. Literature Survey

In the old CAM, accuracy must be maintained throughout the whole system's operation since, under the former paradigm, incorrect input to clinicians might lead to incorrect prescriptions or suggestions from the system. The identity symbol set for a client's characteristic vector v is known to the trust authority, therefore trust authority may readily deduce the client's private attributes vector since the basic CAM includes secure enervation. Additionally, since the cloud may quickly determine the identity symbol for the private key pie by executing a verification test in MDRQ, the client is unable to secure his privacy against the cloud. The redesigned system makes use of the AES algorithm and authentication for messages code (MAC) hash functions. Additionally, it has a number of modules that talk to one another for improved integrity and a straightforward user interface. This section outlines a literature review of several methods that have been used in the past to protect data privacy in cloud computing.

To protect information privacy, Benefit and Mini created the Genetic Grey Wolf Optimization Algorithm (GGWO). Although the GGWO approach efficiently hides the sensitive information, a lot of details was lost in the process. To keep the data in the cloud, Georges and Sumathi created the Crow search-based Lion method for producing the key matrix coefficient. The highest levels of usefulness and privacy were achieved by this strategy. This approach has a significant level of computational complexity, though. Majeed modelled the safe anonymization method for preserving the confidentiality of medical data stored in the cloud. Despite the great privacy and utility achieved by this technology, it has failed in a diversified context.

The Security-Preserving Data Mining (PPDM) system was created by Yusra and Malena to protect the privacy of datasets. This approach had a fast-processing speed, but it also had a large computational cost. For the purpose of assisting patients with cardiac disorders in an emergency, Vijayakumar et al. designed an alert system. To the hospital, emergency service, and even a doctor, the system transmits a confidential and personal communication from the heart patient. The system's relatively high degree of security was achieved with little compute and communication costs.

An identity-based shared decryption technique for a private medical record sharing system has been put forth by Zhou et al. With this approach, it is possible to exchange the data with several people without having to reassemble the decryption key. Additionally, it is suggested that it is safe from selected ciphertext attack (CCA). The user may search the continually changing data from the IIOTH system thanks to the static searchable asymmetric encryption (DSSE) approach.

3. OVERVIEW OF THESYSTEM

3.1 Existing System

- Due to the growing number and complexity of mHealth systems, traditional privacy protection strategies that only remove clients' personal identifying information (such as names or SSN) or use anonymization techniques are ineffective in addressing the issue of privacy. range of personally identifying data. Traditionally, methods of anonymity like anonymity or l-diversity are used to address the privacy issue. However, it has been suggested that these methods may not be enough to stop re-identification attacks.

3.2 Proposed System

In this study, we propose a mHealth surveillance system (CAM) using cloud assistance. Before offering our solutions, we first pinpoint the design issues relating to privacy protection. We begin with the most basic design to make it easier to grasp and so that we can see any potential privacy violations. We follow up with a better plan by resolving the privacy issues found. 9 The resulting enhanced system enables the mHealth service supplier (the firm) to safely transfer its data or programs to the cloud while allowing it to go offline following setup. We implement the newly developed outsourced decryption approach into the underlying multifaceted range queries system to move the computational difficulty of clients over to the internet without exposing any information about either clients' query input. or the cloud with the decrypted choice. We suggest another change, which eventually leads to our final design, to reduce the computational complexity on the company's side, which is inversely related to the number of clients. It is based on a new key private re-encryption via proxy plan in which the business only needs to complete safeguarding once during the setup phase and transfers the remaining computational duties to the cloud without jeopardizing privacy, further decreasing the processing and interactions burden on clients along with the cloud..

3.3 Proposed System Design

In this project work, I used four modules and each module has own functions, such as:

1. Clients
2. Cloud server
3. Trust authority
4. Company Module

3.3.1 Clients

The client submits the token associated with its query to the cloud, which then executes the query execution phase, after which we construct the Clients module. The primary computationally demanding process for the consumer's decryption is finished by the cloud, which then gives the client the partly decrypted ciphertext. After acquiring the partially deciphered ciphertext, the client accomplishes all of the remaining decoding tasks and gets its decryption result, which reflects the monitoring program's determination based on the client's input. After executing the search phase, the cloud receives no meaningful data on the private query input from the 18 clients and the decryption outcome. Here, we identify the privacy violation of the query input based on what can be deduced from the computations or communication data CAM may hinder the cloud from inferring relevant data from a client's query input or output that corresponds to the information the client has provided.

3.3.2 Cloud Server

In this module, CSP must first obtain the key. The file may then only be stored on his cloud server by him. The only thing a TTP (Recommended Third Party) can do is verify if a server located in the cloud is legitimate or not. If the file is fraudulent, TTP won't let it to be stored on a cloud server.

3.3.3 Trust Authority

According to a certain business model, such as the "pay-peruse" model, TA is in charge of providing Private keys to customers and collecting service fees from clients. TA can be seen of as a coworker or management agent for a company (or numerous firms), and as such, the two parties have some degree of common commercial interests. We'll briefly go through each of CAM's four main phases in the sections that follow: setup, store, token generation, and query. Here, we only show how these components operate. We provide extra details when necessary because the precise input and output of those processes may change in different systems. The setup phase is run by the TA in the beginning, and the system parameters are published.

3.3.4 Company Module

The corporation describes a mHealth tracking program's flow chart as a branching program in the first place (see Sec.), which is secured under the corresponding directed branching tree. The resultant Ciphertext, which in this situation corresponds to the Store algorithm, and its corporate index will then be sent by the corporation to the cloud. The it client and TA execute the Tok Engen algorithm whenever a client requests a cloud query for a certain mHealth monitoring programmed. The client feeds TA the business index, and TA then inputs the algorithmic master password and the client's confidential query, whose is the attribute vector that represents the gathered health data. While TA receives no meaningful information about the query, the client receives the token according to its query input.

4 Architecture

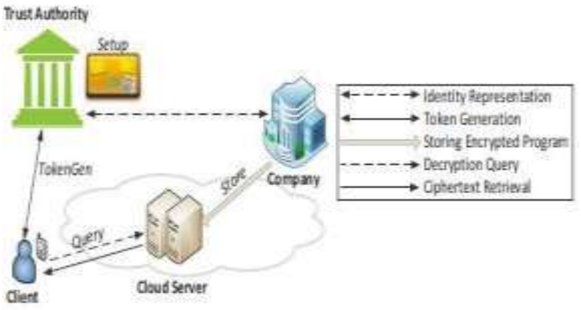


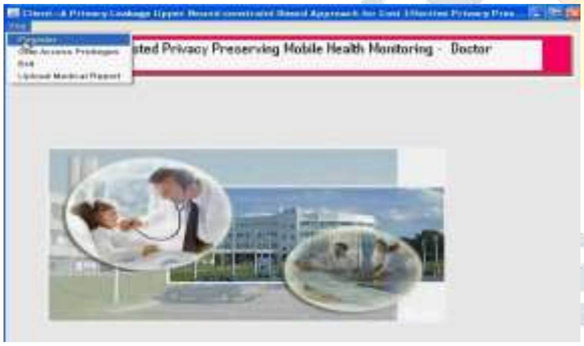
Fig 1: System Architecture

5 RESULTS SCREEN SHOTS

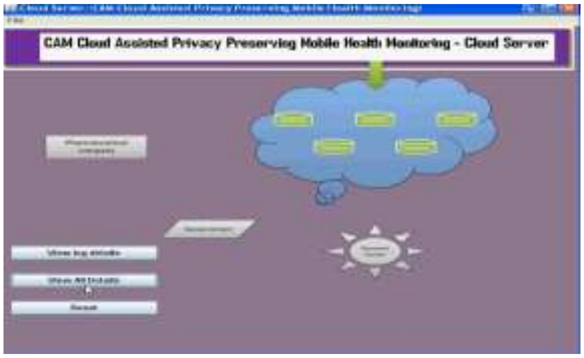
HSP Interface:

File
CAM Cloud Assisted Privacy Preserving Mobile Health Monitoring - Doctor

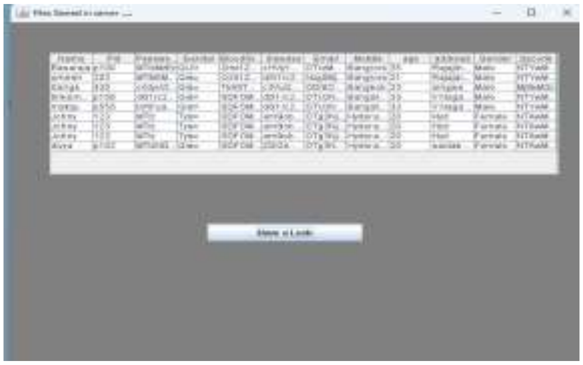
DashBoard Page:


Client - A Privacy Leakage Upper Bound constraint Based Approach for Cost Effective Privacy Pres...
File
Register
Give Access Privileges
Exit
Upload Medical Report
...sted Privacy Preserving Mobile Health Monitoring - Doctor

Cloud Server Page:

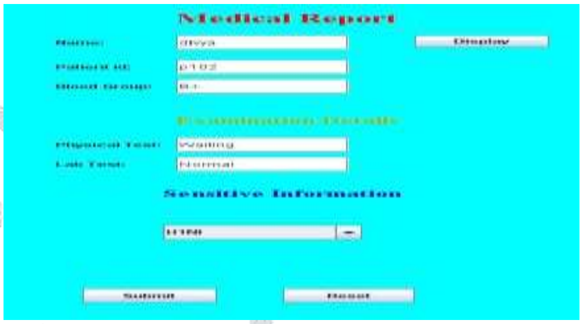

Cloud Server - CAM Cloud Assisted Privacy Preserving Mobile Health Monitoring
File
CAM Cloud Assisted Privacy Preserving Mobile Health Monitoring - Cloud Server
View log details
View All Details
Reset

Registered Data in Cloud:



Name	Pid	Password	Gender	[illegible]	[illegible]	Email	Mobile	age	address	Gender	Secure
[illegible]	p102	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Bangalore	35	[illegible]	Male	NTYaW
umesh	123	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Bangalore	21	[illegible]	Male	NTYaW
[illegible]	122	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Bangalore	23	[illegible]	Male	[illegible]
[illegible]	p100	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Bangalore	33	[illegible]	Male	NTYaW
[illegible]	p555	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Bangalore	33	[illegible]	Male	NTYaW
Johny	123	MTIz	Tyse	[illegible]	[illegible]	[illegible]	Hydera	20	Hari	Female	NTAwM
Johny	123	MTIz	Tyse	[illegible]	[illegible]	[illegible]	Hydera	20	Hari	Female	NTAwM
Johny	123	MTIz	Tyse	[illegible]	[illegible]	[illegible]	Hydera	20	Hari	Female	NTAwM
divya	p102	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Hydera	20	[illegible]	Female	NTAwM

Medical Report:



Name: divya

Patient Id: p102

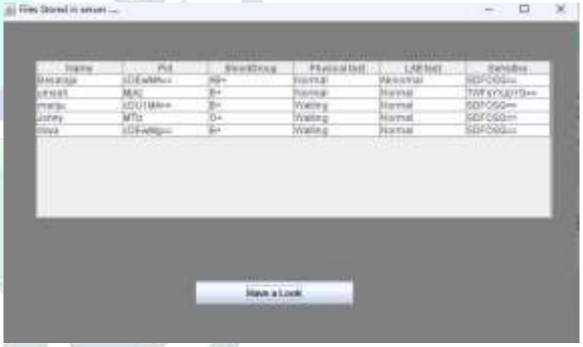
Blood Group: B+

Physical Test: Waiting

Lab Test: Normal

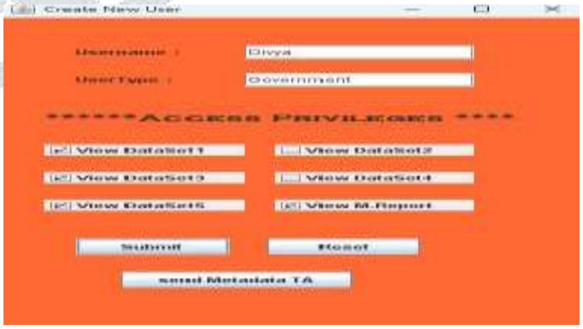
HIV

Registered Medial Reports:



Name	Pid	BloodGroup	Physicaltest	LABTest	Sensitive
Mavaraja	zDEwMNu==	AB+	Normal	Abnormal	SDFOSQ==
umesh	MjAI	B+	Normal	Normal	TWFyYXJpYS==
manju	zDU1MA==	B+	Waiting	Normal	SDFOSQ==
Johny	MTIz	O+	Waiting	Normal	SDFOSQ==
divya	zDFwMg==	B+	Waiting	Normal	SDFOSQ==

Access privileges:



Username : Divya

UserType : Government

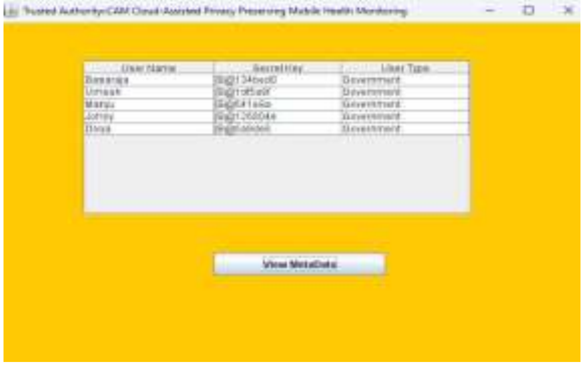
******ACCESS PRIVILEGES ****

☑ View DataSet1 ☐ View DataSet2

☑ View DataSet3 ☐ View DataSet4

☑ View DataSet5 ☑ View M.Report

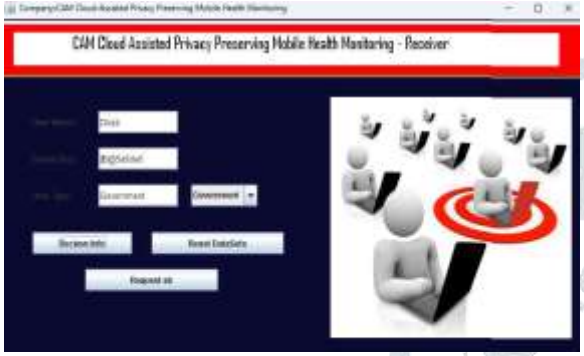
Trusted Authority Page:



Trusted Authority/CAM Cloud-Assisted Privacy Preserving Mobile Health Monitoring

User Name	Secret Key	User Type
[illegible]	[B@134bcd0	Government
Umesh	[illegible]	Government
Manju	[illegible]	Government
Johny	[illegible]	Government
Divya	[illegible]	Government

Receiver Page:



Company/CAM Cloud-Assisted Privacy Preserving Mobile Health Monitoring

CAM Cloud Assisted Privacy Preserving Mobile Health Monitoring - Receiver

Divya

[illegible]

Government

7. CONCLUSION

✓ In this study, we build CAM, a cloud-assisted confidentiality-preserving mobile wellness tracking system, to efficiently safeguard customers' privacy and the intellectual property mHealth service providers' property. We use the anonymized Bone Franklin encryption algorithm based on identity (IBE) in health care diagnostic branching programs to secure the customers' privacy. We employ newly suggested decryption outsource with security for privacy to move clients' pairing computations to the cloud server in order to lessen the decryption difficulty caused using IBE. We utilize a random permutation to grow the branching program tree and randomize the decision standards used at the decision branches nodes in order to safeguard the programs provided by Health service providers. Finally, our CAM design assists small businesses with little resources in participating in the mHealth market.

Future Enhancement

✓ Here are a few upcoming improvements that will be made to the present project. Deploy machine learning algorithms to find abnormalities in patient health data in real-time, which might help identify possible health issues and notify medical professionals or emergency personnel. Machine intelligence-based anomaly detection.

✓ Wearing device integration: Combine with wearable devices, such as smartwatch or fitness trackers, to record extra health information, such as heart variation sleep structures, or physical action, which may offer a more thorough picture of the health and wellbeing of the patient.

✓ Personalized health suggestions as follows: Create a personalized health recommendation engine that uses patient health information and machine learning techniques to give consumers individualized health advice, such as food or exercise regimens. Add telemedicine features to allow for online meetings with medical professionals, which might offer users convenient and easy access to medical services.

✓ Blockchain-based data storage: Use a blockchain-based records storage to give patient medical data an increasingly greater level of confidentiality and privacy, which might boost user confidence and system adoption.

8. References

[1] Mohan, D. Marin, S. Sultan, A. Deen,"Medinet: Personalizing the self-care process for patients with diabetes and cardiovascular disease using mobile telephony", In Proc. 30th Ann. Int. Conf. IEEE Engineering in Medicine and Biology Society, 2008 (EMBS 2008), 2008, pp. 755–758.

[2] A. V. Dhukaram, C. Baber, L. Elloumi, B.-J. van Beijnum, P. D.Stefanis,"End-user perception towards pervasive cardiac healthcare services: Benefits, acceptance, adoption, risks, security, privacy and trust", In Proc. Pervasive Health, 2011, pp. 478–484.

[3] M. Delgado,"The evolution of health care it: Are current U.S. privacy policies ready for the clouds?", In Proc. SERVICES, 2011, pp. 371–378.

[4] A. Tsanas, M. Little, P. McSharry, L. Ramig,"Accurate telemonitoring of parkinson's disease progression by noninvasive speech tests", IEEE Trans. Biomed. Eng., Vol. 57, No. 4, pp. 884–893, Apr. 2010.

[5] P. Baldi, R. Baronio, E. D. Cristofaro, P. Gasti, and G. Tsudik, "Countering gattaca: Efficient and secure testing of fully-sequenced human genomes," in Proc. ACM Conf. Computer and Communications Security, 2011, pp. 691–702.

[6] A. Cavoukian, A. Fisher, S. Killen, and D. Hoffman, "Remote home health care technologies: How to ensure privacy? Build it in: Privacy by design," Identity in the Information Society, vol. 3, no. 2, pp.

363–378, 2010.

[7] A. Narayanan and V. Shmatikov, “Robust de-anonymization of large sparse datasets,” in Proc. IEEE Symp. Security and Privacy, 2008 (SP 2008), 2008, pp. 111–125. ϖ A. Narayanan and V. Shmatikov, “De-anonymizing social networks,” in Proc. IEEE Computer Society, IEEE Symp. Security and Privacy, 2009, pp. 173–187.

[8] I. Neamatullah, M. Douglass, L. Lehman, A. Reisner, M. Villarroel, W. Long, P. Szolovits, G. Moody, R. Mark, and G. Clifford, “Automated de-identification of free-text medical records,” BMC Med. Inform. Decision Making, vol. 8, no. 1, p. 32, 2008.

[9] S. Al-Fedaghi and A. Al-Azmi, “Experimentation with personal identifiable information,” Intelligent Inf. Manage., vol. 4, no. 4, pp. 123–133, 2012.