Double Standard Security Mechanism In The Management Cloud Based Mobile Application
1Student of M.Tech (CSE), 2Asst. Professor, and 3HOD, Professor
Department of Computer Science Engineering, QIS Institute of Technology, Ongole.

Abstract: Patient care is the focus of many clinical disciplines application but it is very complex as patient care is the essential information for direct patient care is defined on the applications. The present applications are not provide security on health monitoring system. The patient details are stored in cloud for the purpose of privacy and security but these are not retrieved accurate and not provide efficient privacy. However we are having major question in cloud health monitoring system What information does each professional generate? Where, when, and in what form is it needed? Even broader definitions of e-health and e-environment are used for describing processes in health care and the environment that are electronically / digitally covered, instead of just being available on the Internet. So this paper address above problem and solved the problem of patient health details are monitored very and retrospective analysis of patient-care data had become a priority need of all customers. So we are providing section health monitoring..

Key words: Mobile health (mHealth), Healthcare, Privacy, Outsourcing

I. Introduction:
The genesis of patient care systems occurred in the mid-1960. One of the first and most successful systems was the Technical Medical Information System (TMIS), begun in 1965 as a collaborative project between Lockheed and El Camino Hospital in Mountain View, California. Designed to simplify documentation through the use of standard order sets and care plans, TMIS defined the state of the art when it was developed. More than three decades later, versions of TMIS are still widely used, but the technology has moved on. The hierarchical, menu-driven arrangement of information in TMIS required users to page through many screens to enter or retrieve data and precluded aggregation of data across patients for statistical analysis. Today’s users have a different view of what can be done with data, and they demand systems that support those uses. Part of what changed users’ expectations for patient care systems was the development and evolution of the HELP system at LDS Hospital in Salt Lake City, Utah Initially providing decision support to physicians during the process of care (in addition to managing and storing data), HELP has subsequently become able to support nursing care decisions and to aggregate data for research leading to improved patient care. Today, both vendors of information systems and researchers in health care enterprises are working to incorporate decision support and data aggregation features in systems that use the latest technologies for navigating and linking information. Based on World Health Organization’s Statistics (WHO) and other sources, chronic diseases and psychological pressures are behind the death of 80% of elderly people (e.g. in Algeria). The greater part of elderly suffer from various chronic diseases. We plan to elucidate on how recent advancement in wireless communication and smart phone technology have empowered tremendous improvement in health monitoring services. Provide behavioral feedback about someone’s health in order to prevent diseases. The consumers and healthcare service providers using smart phones are growing exponentially throughout last decade. The adoption of this technology is rapid; two-thirds of physicians and 42% of the public used smart phones as of late 2009. [1] As of February 2010, there were nearly 6,000 such apps within the Apple App Store. Of these, 73% were intended for use by consumer or patient end-users, while 27% were targeted to healthcare professionals.

II Related Work:
The basic CAM has the security enervation such as the identity representation set for a client’s attribute vector v is known to trust authority and hence trust
authority can easily infer the clients private attribute vector. Also it the client cannot protect his privacy from the cloud either because the cloud can easily find out the identity representation for the private key \( pk_i \) by running identity test in MDRQ. [1, 3, 4]. Modified system uses AES algorithm with hash functions which in corporate message authentication code (MAC). It also comprises the various modules which communicate with each other for better integrity and uses simple user interface. Existing Cloud-assisted mobile health (Health) monitoring, which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support[9], has been considered as are evolutionary approach to improving the quality of health care service while lowering the healthcare cost. But these systems depend completely upon the proper operation of their sensors. So they cannot be used along with the existing cardiac sensors of the bedside monitors in ICU, also a variation in the placement of the sensors of blood flow might lead to false alarms or a critical condition being over looked. Most of current private tele monitoring schemes is dependent on anonymization techniques, which are deemed to be ineffective in the proposed scenario as we discussed before. Another line of work focuses on privacy preserving diagnostic programs. At the end of the protocol, a client obtains nothing on the diagnostic program but the diagnostic result while the program owner, i.e., the company obtains no information on the individual private data. All the existing solutions require a client to run multiple instances of oblivious transfer protocol with the company after setup phase, which means the company has to stay online constantly. All the current solutions are based on garbled circuits, which implies a client must download the whole circuit to his device and complete the decryption. Besides, the private computation or processing of medical information over cloud has also attracted attention from both the security community [3] and signal processing community. The flourish of m-Healthcare still faces many challenges including information security and privacy preservation. The Smartphone’s energy could be insufficient when an emergency takes place.

III Proposed Work:

In this system we are concentrated on wonderful health monitoring system like below levels.

Fig 1: system architecture

This paper is to address this important problem and design a cloud-assisted privacy. It preserving mobile health monitoring system to protect the privacy of the involved parties and their data. The outsourcing decryption technique and a newly proposed key private proxy re encryption are adapted. It uses to shift the computational complexity of the involved parties to the cloud without compromising clients’ privacy and service providers ‘intellectual property. Identity (ID)-based encryption, or IBE for short, is an exciting alternative to public-key encryption, which eliminates the need for a Public Key Infrastructure (PKI) that makes publicly available the mapping between identities, public keys, and validity of the latter. The senders using an IBE do not need to look up the public keys and the corresponding certificates of the receivers, because the identities (e.g. emails or IP addresses) together with common public parameters are sufficient for encryption.

IV Conclusion:

Cloud Computing technology provides human advantages such as economical cost reduction and effective resource management. However, if security accidents occur, economic damages are inevitable. Our paper proposed “A secured patient healthcare monitoring in cloud infrastructure” for effective resource. Proposed method consists of Identity Based Encryption (IBE) in which a master key helps to deliver the report and Outsourcing Decryption Technique in which a master key helps to viewing the prescription.
V Future Enhancements:
In future we can use some other encryption and decryption techniques and compare it with existing system. By this comparison we can find the accuracy which one gives more privacy in cloud storage. We have proposed secure cloud architecture to address the user privacy problem in a cloud. By using OTP and WTP in cloud computing system, our proposed architecture achieves better goal of preserving the privacy of a user [9].

VI References:

AUTHORS:
Sandhya Rani.P is a student of Computer Science Engineering from QIS Institute of Technology, Presently pursuing M.Tech (CSE) from this college.

Mahesh.N is a Asst. Professor of QIS Institute of Technology, Ongole. He received M.Tech in Computer Science Engineering from JNTU Kakinada University.

Lakshmi Tulasi.R is a Professor, H.O.D of QIS Institute of Technology, Ongole. She received M.Tech from JNTUCEA. she is pursuing Ph.D at JNTUH.She is a good Researcher in semantic web, Computer Networks. She attended Various National and International Workshops and Conferences.