Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7683978

DESIGN AN EFFICIENT SHARABLE & REACHABLE MOBILE HEALTH SYSTEM EXTENDED WITH DIVISION & REPLICATION TO ENHANCE SECURITY

Shinde Babaso Ananda and Dr. Rajeev G. Vishwakarma
Department of Computer Science & Engineering,
Dr. A. P. J. Abdul Kalam University, Indore (M.P.), India -452016
Corresponding Author Email: shindebabaso@gmail.com

Abstract:
Wireless wearable sensor devices and cloud of things aid patients in current health care. m Health offers more features than traditional health care services. It makes monitoring, sharing, diagnosing, and remotely engaging with patients via cloud of things easier. Wearable gadgets in health care raise various security concerns, including data privacy and security. Patient-driven mobile health has grown. Wearable sensors collect real-time patient data, which is aggregated and encrypted at end user devices. Doctors, nurses, and researchers store and access the encrypted data in the cloud. Sharing scalable encrypted data efficiently is difficult. This Paper proposes a Lightweight Sharable and Traceable (LiST) safe mobile health system. Patient data is encrypted end-to-end. List provides precise keyword search and protected data access control. Traitor tracing and user revocation are supported. Traitors sell their search key to coworkers and steal allowances. How-ever, the cloud handles most cryptographic computations while end user devices perform light tasks. LiST is secure without a random oracle. Extensive experimentation improves system performance. Health care information technology is growing worldwide. Only devolved countries used smart devices in health care. Today, poorer nations are also adopting it. Everyone wants to utilize smartphones and their apps. Users want mobile apps because of this transition. Even doctors and patients are comfortable using mobile devices for patient records and diagnosis. Information technology in healthcare is growing worldwide. In health care, mostly devolved countries used computers and technology. Now developing nations are too. Mobile networks in most of a country make everyone want to utilize them. Smart phone use has skyrocketed in recent years. Users want mobile apps because of this transition. Smartphones can now run most desktop apps.
Keywords: Mobile Health, Sharable & Traceable, LiST, Device, Cloud Computing, Mhealth, EHR,

I. INTRODUCTION

The needs of patients are met in today's modern health care services through the utilization of wireless, wearable sensor devices and the cloud of things. In comparison to the health care services that are already available, newer technologies such as m Health offer a greater variety of options and improvements. It enables greater flexibility in terms of monitoring patients' records, exchanging patients' data, providing patients with the necessary diagnosis, and remotely communicating with patients via the cloud of things. However, if we introduce wearable devices to the health care service, there are a great deal of security concerns, such as

the privacy and protection of health care data that need to be taken into consideration. A new patient-driven approach has contributed to the emergence of the mobile health system. The system enables the aggregation and encryption of patient data at the end user devices, as well as real-time collecting of patient data through the use of wearable sensors. After that, the encrypted data is uploaded to the cloud in a distributed way for the purpose of storage and access by members of the health care personnel such as doctors, nurses, and researchers. Nevertheless, the difficult difficulty is to exchange scaled encrypted data in an effective manner.

In this project, we propose developing a secure mobile health system that is lightweight, sharable, and traceable (LiST). Patients' data are protected using encryption that goes all the way through. LiST is capable of providing both an effective keyword search and an exquisite access control mechanism for encrypted data. Additionally, it allows for the cancellation of users and enables the tracing of traitors. Traitors make a financial profit by selling their search key to their fellow employees as well as access allowances. How-ever, The majority of the cryptographic processing work, which can be quite intensive, is offloaded to the cloud, while just the most basic operations are carried out on the devices used by end users. We use a formal approach to defining LiST's security and demonstrate that it is secure even in the absence of a random oracle. Extensive testing is done in order to attain the desired performance levels in the system.

The field of health care information technology is a relatively new one, but its application is becoming more widespread all over the world. Until recently, the only countries that used smart gadgets in the healthcare sector were those that had decentralized their responsibilities. But things seem rather different now, particularly because developing nations are also making progress in that direction. Everyone has an interest in using mobile phones and the expanding number of applications available for them. The user community is becoming increasingly vocal about the need for mobile application development as a result of this trend. Even health care service providers and patients themselves are beginning to feel more at ease with the usage of mobile devices for the diagnostic procedure and patient records.

The frequency with which information technology is applied to the field of providing medical care is growing on a daily basis in every region of the world. In the past, predominantly devolved countries made use of computers and the various equipments associated with them in the field of healthcare. But in today's world, developing countries are also making progress in that direction. Everyone in a country is more likely to be interested in using mobile phones if mobile networks are covered in the majority of the country's territories. In addition, throughout the course of the past few years, the number of people using smart phones has significantly expanded. The user community is becoming increasingly vocal about the need for mobile application development as a result of this trend. Users can now access the majority of desktop apps on their mobile devices, such as smart phones.

The way that businesses operate in the healthcare sector is also being disrupted by the rise of the internet. It presents astonishing prospects for information sharing amongst specialists in the healthcare industry and for reducing the time-consuming and expensive paper trail. However, in order to safeguard the confidentiality of patient records, businesses need to develop secure architecture. This is necessary given that the privacy and integrity of patient information are two of the most important requirements for mobile healthcare security. It is important to ensure that unauthorized individuals are unable to access such information, which includes details on a person's medical treatment and other aspects of their life, such as their social standing. Protecting patient confidentiality from network-based infractions is one of the benefits of healthcare security. Other benefits include securely providing information to remote physicians, partners, and branch offices and complying with government requirements regarding network security.

Mobile Health (mhealth):

When it comes to providing public health care and other preventative services, the utilization of smart phones, tablets, and other mobile devices is referred to as mobile health technology. Healthcare professionals make use of this technology so that they can gain access to electronic health records (EHR), coordinate with care teams, communicate with patients through patient portals, carry out real-time monitoring of patients, improve disease diagnosis, and track diseases. Additionally, we provide a service that is known as telemedicine, which is the delivery of medical treatment digitally through the use of the cloud. Patients are able to maintain control of their own medical records, have access to their electronic health records (EHR), and maintain communication with their respective healthcare providers by utilizing this technology. This application gives patients and doctors the ability to access and share data when it is required, which results in time savings for both the patients and the doctors. Everyone's lives are made simpler and healthier because to the advancements that have been made in medical technology in recent decades. Even health care service providers and patients are growing increasingly accustomed to the concept of utilizing mobile devices to access patient records and/or to assist in the process of making a diagnosis for patients. This shift in attitude is due in large part to technological advancements.

Distributed Cloud

It refers to a setup in which a single file system grants access to a variety of clients all at the same time. Each file is split up into multiple fragments, which are then stored on their own individual computers in several distinct locations. It significantly simplifies the process of running multiple programs simultaneously. As a direct consequence of this, both the communication and the performance will advance at a brisker pace. Under the aegis of this program, computerized medical records are sectioned up into ever-more-granular components before being uploaded to the cloud for storage. Because protecting one's privacy, one's integrity, and one's anonymity are the three most important aspects of security. It will perform more quickly while simultaneously cutting down on the amount of time required to carry out the action.

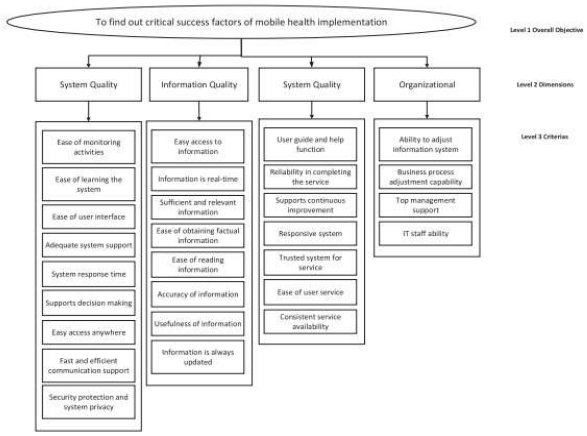


Figure 1: Critical success factors of m-health implementation
(1-s2.0-S2405844018324915-main.pdf)

Health matters. Paper healthcare inefficient cloud, mobile, satellite, and connectivity increased e-health. E-health analyzes health data to improve healthcare. EHRs, EMRs, and PHRs scan paper records.

EHRs are called EMRs in healthcare. Patients keep PHRs. PHRs measure blood pressure, glucose, and heart rate. Global e-health rollout; EHRs are worth it. Patients share EHRs. Electronic documents may help doctors decide. General practitioners and other healthcare providers contribute medical data to a national sickness tracking database. Despite their benefits, health data security and privacy concerns have hindered their use. Patients can disclose. Data security prevents loss, manipulation, disclosure, and access. Health data can ruin one's life, social standing, and stability. Studies suggest people don't communicate health information outside of therapy. E-health systems abuse sensitive health data. Privacy Rights Clearinghouse (2005) reports 22 million healthcare privacy breaches. Statistics include PHI theft. To enjoy e-health systems while respecting users' privacy, advanced security and privacy measures are needed. E-health systems secure sensitive data. Distributed e-health models provide privacy and data mismanagement. Thus, thoughtfulness security and patient privacy problems hinder EMR use in healthcare. This study proposes a healthcare-specific secure multifactor remote user protocol. Password, smart device, and biometrics protect identity. Biometrics can't be stolen, faked, or forgotten. AVISPA verified online. Patient-server authentication protects data and systems. The protocol is secure.

II. RELATED WORK

User authentication, privacy, data stream deletion, and tracking are healthcare security issues. This paper addresses remote user authentication. Remote healthcare system users—patients, doctors, and physicians—authenticate. Authenticated users can access data through mobile or terminal. Most user authentication methods in the literature employ single-factor authentication (passwords). Single-factor authentication proved insecure. Smart cards and biometrics improve

authentication and security. Recent Healthcare user authentication methods are covered here. Mobile cloud computing users can employ multi-factor authentication. Username/password, mobile number, and bio-information authenticate this system. This design includes mobile devices, a management server, storage, and a cluster host. TLS/SSL was assumed for authentication system-wireless access point connections. Protocol registration and authentication; registration requires ID. The management server stores hashed password, face, voice, and mobile device unique values (IMEI, IMSI) after checking for previous storage. After receiving login credentials, the management server calls one or more clustered hosts to authenticate the data against storage. The management server responds to the user with the result. Clustered VMs optimized authentication. However, cloud bio-data should be encrypted. This protocol lacks user-management server mutual authentication. Mobile devices should have good cameras for authentication. Revealed has several security issues and gave a protocol to fix them. Suggested multi-server tele-care medication information system authentication; smart cards and elliptic curve cryptography agree session keys. This authentication method secures patient-doctor communication via unsafe channels. Safe guarded biometric security methods from forgeries, off-line password guessing, and replay attacks. They negotiated USB Mass Storage Device data encryption session keys using mutual authentication. Tele care medical information System authentication methods have forward secrecy, impersonation attack, and known random value attack. They improved it using elliptic curve systems proposed a two-factor ECC-based anonymous authentication and key agreement approach to solve the weakness of

III. PROPOSED SYSTEM

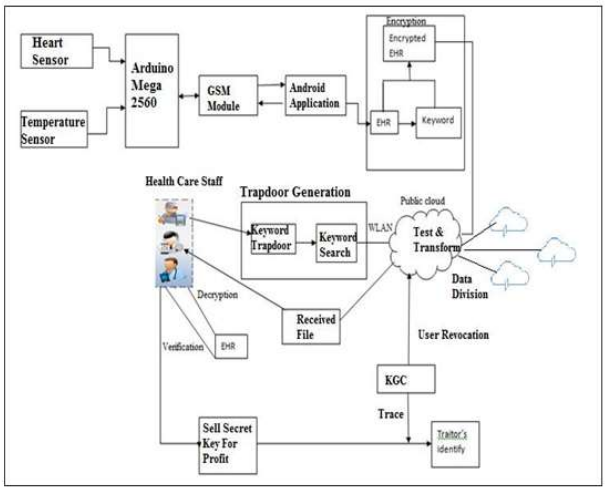


Figure 2: Proposed System

Within the framework of the proposed system, a coordinator node would be implanted within the patient's body. This node would be in a position to receive all of the signals from the wireless sensors and then relay them to the base station. The patient's sensors create what is known as a wireless body sensor network (WBSN) when they are attached to the patient's body.

This network is equipped with the capability to sense the patient's vitals, including their heart rate and blood pressure. This system is able to recognize abnormal circumstances, trigger an alarm for the patient, and communicate with the attending physician through email or text message when an abnormality is detected. Additionally, a number of wireless relay nodes are incorporated into the system that is under evaluation. These nodes are responsible for conveying the data that has been transmitted by the coordinating node and delivering it to the base station. They do this by communicating with the base station.

When compared to earlier systems, the primary benefit of this one is that it is able to cut down on the amount of energy that is used, which in turn extends the lifespan of the network. Additionally, it is able to speed up and extend the communication coverage, which in turn increases the freedom for patients and improves their quality of life. Finally, it is able to do all of these things simultaneously, which is another advantage. We have built this system in a multi-patient architecture for hospital health care, and we have compared it to other contemporary networks that are based on multi-hop relay nodes in terms of coverage, energy consumption, and speed. This was done in order to determine which system is superior.

Goals

- We have planned to develop an application that will provide interface to both physicians and patients.
- We have developed an healthcare application that will provide secure, trustful and reliable communication for different communities in healthcare area.
- The Objective of the system is to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers.
- To adopt Cipher text Policy Attribute-Based Encryption (CP-ABE) as a promising technique to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers.
- To implement a system with multiple attribute authorities to share the load of user legitimacy verification and each of the authorities to manage the whole attribute set individually.
- To implement a system with CA (Central Authority) who should be chosen one among the AAs, to generate secret keys for legitimacy verified users and the load of user verification is shared by multiple AAs.
- To implement a system with an observer system for CAs behavior and protocol to verify owner and his/her data to be uploaded to make the system secure and efficient.
- The main goal of the project is to provide secure sharing of personal health records in cloud. Hospitals are now benefitting from data sharing as this provides better, safe care of patients.

IV. CLOUD COMPUTING

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software , and information are provided to computers and other devices

as a metered service over a network (typically the Internet).Cloud computing provides computation, software, data access, and storage resources without requiring cloud users to know the location and other details of the computing infrastructure. End users access cloud based applications through a web browser or a light weight desktop or mobile app while the business software and data are stored on servers at a remote location. Cloud application providers strive to give the same or better service and performance as if the software programs were installed locally on end-user computers.

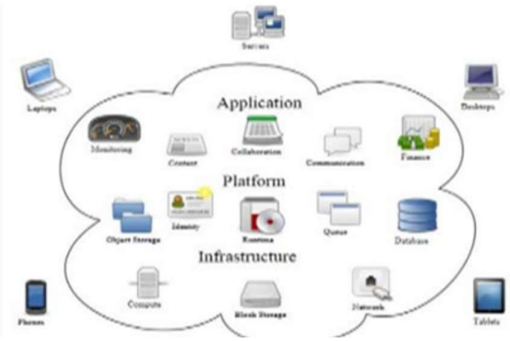


Figure 3: Cloud Architecture

Characteristics

Cloud computing exhibits the following key characteristics:

- Empowerment of end-users of computing resources by putting the provisioning of those resources in their own control, as opposed to the control of a centralized IT service.
- Agility improves with users ability to re-provision technological infrastructure resources.
- Application programming interface (API) accessibility to software that enables machines to interact with cloud software in the same way the user interface facilitates interaction between humans and computers. Cloud computing system typically use REST-based APIs.

- Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation (in-house).
- Virtualization technology allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.
- Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
- Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford.

Service Models

Cloud computing providers offer their services according to three fundamental models: Infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) where IaaS is the most basic and each higher model abstracts from the details of the lower models.

Infrastructure as a Service (IaaS) :

In this most basic cloud service model, cloud providers offer computers as physical or more often as virtual machines, raw (block) storage, firewalls, load balancers, and networks. IaaS providers supply these resources on demand from their large pools installed in data centers. Local area networks including IP addresses are part of the offer. For the wide area connectivity, the Internet can be used or – in carrier clouds – dedicated virtual private networks can be configured.

Cloud Clients:

Users access cloud computing using networked client devices, such as desktop computers, laptops, tablets, and smartphones. Some of these devices- cloud clients – rely on cloud computing for all or a majority of their applications so as to be essentially useless without it. Examples are thin clients and the browser –based chrome book. Many cloud applications do not require specific software on the client and instead use a web browser to interact with the cloud application.

V. HARDWARE DETAILS

Heartbeat Sensor:

A person's heartbeat is the sound of the valves in his/her's heart contracting or expanding as they force blood from one region to another. The number of times the heart beats per minute (BPM), is the heartbeat rate and the beat of the heart that can be felt in any artery that lies close to the skin is the pulse.

Two Ways to Measure a Heartbeat:

Manual Way: Heartbeat can be checked manually by checking one's pulses at two locations-wrist (the **radial pulse**) and the neck (**carotid pulse**). The procedure is to place the two fingers (index and middle finger) on the wrist (or neck below the windpipe) and count the number of pulses for 30 seconds and then multiplying that number by 2 to get the heartbeat rate. However, pressure should be applied minimum and also fingers should be moved up and down till the pulse is felt.

Using a sensor: Heart Beat can be measured based on optical power variation as light is scattered or absorbed during its path through the blood as the heartbeat changes

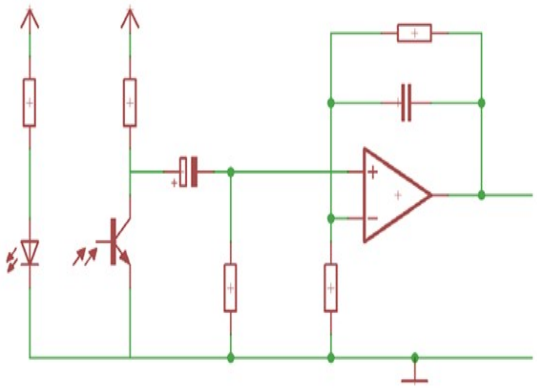
Principle of Heartbeat Sensor:

The heartbeat sensor is based on the principle of photoplethysmography. It measures the change in volume of blood through any organ of the body which causes a change in the light intensity through that organ (avascular region). In the case of applications where the heart pulse rate is to be monitored, the timing of the pulses is more important. The flow of blood volume is decided by the rate of heart pulses and since light is absorbed by the blood, the signal pulses are equivalent to the heartbeat pulses.

Working of a Heartbeat Sensor:

The basic heartbeat sensor consists of a light-emitting diode and a detector like a light detecting resistor or a photodiode. The heartbeat pulses cause a variation in the flow of blood to different regions of the body. When tissue is illuminated with the light source, i.e. light emitted by the led, it either reflects (a finger tissue) or transmits the light (earlobe). Some of the light is absorbed by the blood and the transmitted or the reflected light is received by the light detector. The amount of light absorbed depends on the blood volume in that tissue. The detector output is in the form of the electrical signal and is proportional to the heartbeat rate.

This signal is a DC signal relating to the tissues and the blood volume and the AC component synchronous with the heartbeat and caused by pulsatile changes in arterial blood volume is superimposed on the DC signal. Thus the major requirement is to isolate that AC component as it is of prime importance.



To achieve the task of getting the AC signal, the output from the detector is first filtered using a 2 stage HP-LP circuit and is then converted to digital pulses using a comparator circuit or using simple ADC. The digital pulses are given to a microcontroller for calculating the heartbeat rate, given by the formula-

BPM (Beats per minute) = 60*f

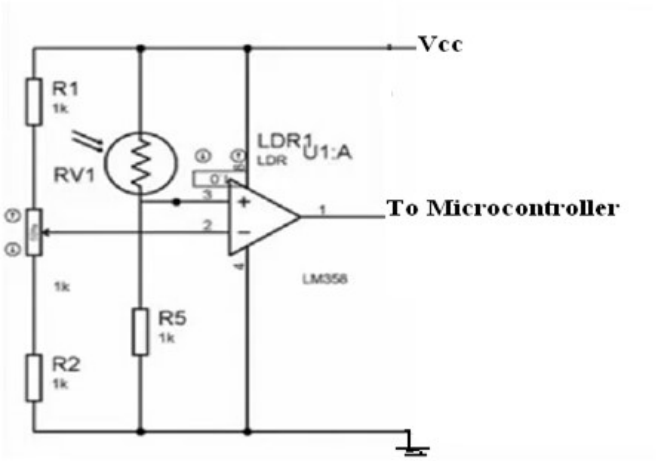
Where f is the pulse frequency

Practical Heartbeat Sensor

It consists of an infrared led and an LDR embedded onto a clip-like structure. The clip is attached to the organ (earlobe or the finger) with the detector part on the flesh.

Application Developing your Heartbeat Sensor System:

A basic Heartbeat Sensor system can also be built using basic components like an LDR, comparator IC LM358, and a Microcontroller as given below



As described above regarding the principle of a heartbeat sensor, when the finger tissue or the earlobe tissue is illuminated using a light source, the light is transmitted after getting modulated i.e. a part getting absorbed by the blood and the rest being transmitted. This modulated light is received by the light detector.

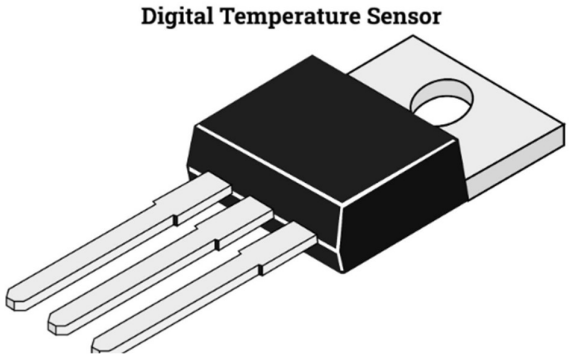
Here a Light Dependent Resistor (LDR) is used as a light detector. It works on the principle that when light falls on the resistor, its resistance changes. As the light intensity increases, the resistance decreases. Thus the voltage drop across the resistor decreases.

Here a comparator is used which compares the output voltage from the LDR to that of the threshold voltage. The threshold voltage is the voltage drop across the LDR when the light with fixed intensity, from the light source, falls directly on it. The inverting terminal of the comparator LM358 is connected to the potential divider arrangement which is set to the threshold voltage and the noninverting terminal is connected to the LDR. When human tissue is illuminated using the light source, the intensity of the light reduces. As this reduced light intensity falls on the LDR, the resistance increases and as a result of the voltage drop increases. When the voltage drop across the LDR or the noninverting input exceeds that of the inverting input, a logic high signal is developed at the output of the comparator and in case voltage drop being lesser a logic low output is developed. Thus the output is a series of pulses. These pulses

can be fed to the Microcontroller which accordingly processes the information to get the heartbeat rate and this is displayed on the Display interfaced with the Microcontroller.

Temperature Sensors:
What are Temperature Sensors?

Temperature sensors are devices that detect and measure coldness and heat and convert it into an electrical signal. Temperature sensors are utilized in our daily lives, be it in the form of domestic water heaters, thermometers, refrigerators, or microwaves. There is a wide range of applications of temperature sensors, including the geotechnical monitoring field.



A temperature sensor can also be defined as a simple instrument that measures the degree of coldness or hotness and then converts it into a readable unit. There are specialized temperature sensors used to measure the temperature of the boreholes, soil, huge concrete dams, or buildings.

What do Temperature Sensors do?

Temperature sensors are devices designed for measuring the degree of coolness and hotness in an object. The voltage across the diode determines the working of a temperature meter. The change of temperature varies directly proportional to the diode's resistance.

The cooler the temperature, the lesser the resistance will be and vice-versa. A measurement of the resistance across the diode is done, and the measurement is converted into units of temperature that are readable and displayed in numeric form over readout units. In the field of geotechnical monitoring, these temperature sensors are utilized in the measuring of internal temperatures of structures such as dams, bridges, power plants.

Temperature Sensors Working:

The working principle of a temperature sensor is the voltage across the terminals of the diode. If there is an increase in the voltage, the temperature also increases. This is followed by a drop in the voltage between the terminals of the transistor of base and emitter in a diode. There are

also temperature sensors that work on the principle of stress change caused by changes in temperature.

In a vibrating wire temperature meter, dissimilar metals have different linear coefficients of expansion. It mainly consists of a magnetic stretched wire of high tensile strength with two ends fixed to any dissimilar metal so that any temperature change will directly affect the tension in the wire and its natural vibration frequency.

The dissimilar metal can be made from aluminum since it has a larger linear expansion coefficient than steel. When the conversion of the temperature signal into frequency occurs, the very same read-out unit that is used for other vibrating wire sensors can also be utilized in the monitoring of temperature also.

The specially built vibrating wire sensor is the one that senses the temperature change and then the temperature change is converted into an electrical signal which is then transmitted to the read out the unit as a frequency.

Temperature Sensor Components:

There are three types of components in temperature sensors. There are essential components of a temperature sensor including thermocouple or extension cables and wires, as well as the sensing elements. The following are examples of components which complete the sensor: insulating beads, connectors, connecting heads, and protecting tubes. There are also associated components that are necessary in the use of sensors like converters and controllers.

Temperature Sensors in Control and Compensation Circuits:

The detection circuit must offer an output in a usable format in order to use a temperature sensor in a control or compensation circuit. For analog circuits, usually, the output is resistance. The measurement must be converted to a digital format for processing by an MCU for digital control and compensation. Commonly, this is achieved by reading the measurement as a voltage by means of an analog-to-digital converter.

Temperature Sensor Elements:

RTD elements are utilized in the manufacturing of temperature sensors. A resistance element is a component that senses temperature at the heart of a resistance thermometer or an RTD. They can't be used in their bare form typically, but they may be built into a probe or assembly that enables them to withstand different conditions of their application. Each has a resistance value that is pre-specified at a known temperature which changes in a predictable fashion. In this way, by measuring the element's resistance, that element's temperature can be determined from calculations, tables, or instrumentation.

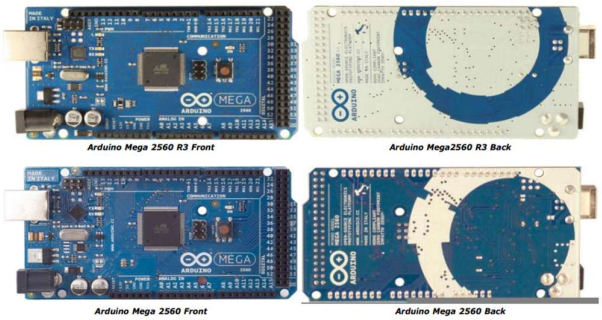
Thin Film Temperature Elements:

These elements are mass produced by automated equipment, which deposits a layer of platinum onto the ceramic substrate and utilizes photolithography in the etching of an electrical current path that corresponds to the value required in ohms. The elements have a smaller size than that of traditional wire wound elements and as a result have a response time that is fast and are suitable in more applications, while reducing the costs of the user at the same time.

Ceramic Temperature Elements

Ceramic elements can be used to make temperature sensors. These elements are wound on either ceramic or glass former, or a helix of platinum wire can be semi-supported within a ceramic tube's bores. This semi-supported type is capable of providing the widest temperature range of operation and, typically, the best stability. Although there are other usable metals, platinum is the most prevalent and widely used type with either ceramic or glass insulators.The use of metals, aside from platinum, can lead to linearity at low temperatures and drift, which throws off temperature processing. The error corrections and adjustments necessary with other metals is why platinum is preferred.

Arduino Mega 2560 :



Overview:

The Arduino Mega 2560 is a microcontroller board based on the ATmega2560 (datasheet). It has 54 digital input/output pins (of which 14 can be used as PWM outputs), 16 analog inputs, 4 UARTs (hardware serial ports), a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started. The Mega is compatible with most shields designed for the Arduino.

Summary:

Microcontroller ATmega2560
Operating Voltage 5V
Input Voltage (recommended) 7-12V
Input Voltage (limits) 6-20V
Digital I/O Pins 54 (of which 14 provide PWM output)
Analog Input Pins 16
DC Current per I/O Pin 40 mA
DC Current for 3.3V Pin 50 mA
Flash Memory 256 KB of which 8 KB used by bootloader
SRAM 8 KB
EEPROM 4 KB
Clock Speed 16 MHz

Power:

The Arduino Mega can be powered via the USB connection or with an external power supply. The power source is selected automatically. External (non-USB) power can come either from an AC-to-DC adapter (wall-wart) or battery. The adapter can be connected by plugging a 2.1mm center-positive plug into the board's power jack. Leads from a battery can be inserted in the Gnd and Vin pin headers of the POWER connector.

Memory:

The ATmega2560 has 256 KB of flash memory for storing code (of which 8 KB is used for the bootloader), 8 KB of SRAM and 4 KB of EEPROM (which can be read and written with the EEPROM library).

Input and Output:

Each of the 54 digital pins on the Mega can be used as an input or output, using pin Mode(), digital Write(), and digital Read() functions. They operate at 5 volts. Each pin can provide or receive a maximum of 40 mA and has an internal pull-up resistor (disconnected by default) of 20- 50 k Ohms.

In addition, some pins have specialized functions:

- Serial: 0 (RX) and 1 (TX); Serial 1: 19 (RX) and 18 (TX); Serial 2: 17 (RX) and 16 (TX); Serial 3: 15 (RX) and 14 (TX). Used to receive (RX) and transmit (TX) TTL serial data. Pins 0 and 1 are also connected to the corresponding pins of the ATmega16U2 USB-to-TTL Serial chip.
- External Interrupts: 2 (interrupt 0), 3 (interrupt 1), 18 (interrupt 5), 19 (interrupt 4), 20 (interrupt 3), and 21 (interrupt 2). These pins can be configured to trigger an interrupt on a low value, a rising or falling edge, or a change in value. See the attach Interrupt() function for details.
- PWM: 0 to 13. Provide 8-bit PWM output with the analog Write() function.
- SPI: 50 (MISO), 51 (MOSI), 52 (SCK), 53 (SS). These pins support SPI communication using the SPI library.
- LED: 13. There is a built-in LED connected to digital pin 13. When the pin is HIGH value, the LED is on, when the pin is LOW, it's off.
- TWI: 20 (SDA) and 21 (SCL). Support TWI communication using the Wire library.

Communication

The Arduino Mega2560 has a number of facilities for communicating with a computer, another Arduino, or other microcontrollers. The ATmega2560 provides four hardware UARTs for TTL (5V) serial communication. An ATmega16U2 (ATmega 8U2 on the revision 1 and revision 2 boards) on the board channels one of these over USB and provides a virtual com port to software on the computer (Windows machines will need a .inf file, but OSX and Linux

machines will recognize the board as a COM port automatically. The Arduino software includes a serial monitor which allows simple textual data to be sent to and from the board. The RX and TX LEDs on the board will flash when data is being transmitted via the ATmega8U2/ATmega16U2 chip and USB connection to the computer (but not for serial communication on pins 0 and 1). A Software Serial library allows for serial communication on any of the Mega2560's digital pins.

GSM Technology:

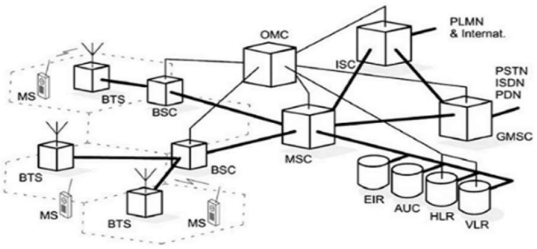
Digital cellular technology like GSM (Global System for Mobile Communication) is used to transmit mobile data as well as voice services. This concept was implemented at Bell Laboratories using a mobile radio system in 1970. As the name suggests, it is the standardization group name that was established in the year1982 to make a general European mobile telephone standard. This technology owns above 70% of the market share of the digital cellular subscriber around the world. This technology was developed by using digital technology. At present, GSM technology supports above 1 billion mobile subscribers around the world in the above 210 countries; this technology provides voice and data services from fundamental to complex. This article discusses an overview of GSM technology. Digital cellular technology like GSM (Global System for Mobile Communication) is used to transmit mobile data as well as voice services. This concept was implemented at Bell Laboratories using a mobile radio system in 1970. As the name suggests, it is the standardization group name that was established in the year1982 to make a general European mobile telephone standard. This technology owns above 70% of the market share of the digital cellular subscriber around the world. This technology was developed by using digital technology. At present, GSM technology supports above 1 billion mobile subscribers around the world in the above 210 countries; this technology provides voice and data services from fundamental to complex. This article discusses an overview of GSM technology.

What is GSM Technology?

GSM is a mobile communication modem; it stands for global system for mobile communication (GSM). The idea of GSM was developed at Bell Laboratories in 1970. It is a widely used mobile communication system in the world. GSM is an open and digital cellular technology used for transmitting mobile voice and data services operate at the 850MHz, 900MHz, 1800MHz, and 1900MHz frequency bands. GSM technology was developed as a digital system using the time division multiple access (TDMA) technique for communication purposes. A GSM digitizes and reduces the data, then sends it down through a channel with two different streams of client data, each in its own particular time slot. The digital system has the ability to carry 64 kbps to 120 Mbps of data rates.

GSM Technology Architecture

The main elements in the GSM architecture include the following.



The Architecture of GSM Technology

- Network and Switching Subsystem (NSS)
- Base-Station Subsystem (BSS)
- The mobile station (MS)
- Operation and Support Subsystem (OSS)

Network Switching Subsystem (NSS):
In GSM system architecture, it includes different elements, which are frequently known as the core system/network. Here, it is basically a data network including a variety of units to provide the major control as well as interfacing of the entire mobile network system. The core network includes the major elements which are discussed below.

Mobile Switching Centre (MSC) :
The Mobile Switching Centre or MSC is the key element in the core network region of the GSM network architecture. This mobile services switching center works like a standard switching node in an ISDN otherwise PSTN, however, it also gives extra functionality to allow the mobile user necessities to be supported like authentication, registration, inter-MSC handovers call location & routing of the call to a cell phone subscriber.

Home Location Register (HLR):
This HLR database includes the information regarding the administrative like every subscriber with their previous identified location. Like this, the GSM network is capable to connect the calls to the related base station for the mobile switch. Once an operator turns ON his/her phone, and then the phone registers through the network so that it is probable to decide which base transceiver station is communicating so that incoming calls can be connected properly. Even once the mobile is switched on, but not active then it again registers to make sure that the HLR network is responsive to its most recent location. There is one HLR for each network, even though it may be dispersed across a variety of sub-centers for operational causes.

Visitor Location Register (VLR):
The VLR includes preferred information that is received from the HLR network to allow the preferred services for the separate subscriber. The visitor location register can be executed like a separate unit; however, it is usually realized like an essential element of the MSC, before an individual unit. Thus, access is finished quicker & more convenient.

Base Station Subsystem (BSS):

It acts as an interface between the mobile station and the network subsystem. It consists of the Base Transceiver Station which contains the radio transceivers and handles the protocols for communication with mobiles. It also consists of the Base Station Controller which controls the Base Transceiver station and acts as an interface between the mobile station and mobile switching center. The network subsystem provides the basic network connection to the mobile stations. The basic part of the Network Subsystem is the Mobile Service Switching Centre which provides access to different networks like ISDN, PSTN, etc. It also consists of the Home Location Register and the Visitor Location Register which provides the call routing and roaming capabilities of GSM. It also contains the Equipment Identity Register which maintains an account of all the mobile equipment wherein each mobile is identified by its own IMEI number. IMEI stands for International Mobile Equipment Identity. The BSS or Base Station Subsystem section of the second generation GSM network architecture is basically connected with the mobiles over the network. This subsystem includes two elements which are discussed below.

Base Station Controller (BSC):

The BSC (base station controller) is used to form the next phase reverse into the GSM technology. This controller is used to control a collection of base transceiver stations & it is frequently co-located through one of the transceiver stations within the group. This controller manages the resources of radio to control different items like handover in the collection of BTSs, assigns channels. It converses with the Base Transceiver Stations over Abis interface.

The subsystem element in the base station of the GSM network uses the radio allowable technology to allow a number of operators to right to use the system concurrently. Every channel supports up to 8 operators by allowing a base station to include different channels; a huge number of operators could be accommodated through every base station. These are located carefully through the provider of the network to allow whole area coverage. This area can be enclosed with a base station that is often being called a cell. Because it is not achievable to stop the signals from overlapping into the nearby cells and channels which are used in single-cell are not utilized in the next.

Mobile Station:

It is the mobile phone which consists of the transceiver, the display, and the processor and is controlled by a SIM card operating over the network. The MS (Mobile stations) or ME (mobile equipment) are most generally identified through cell otherwise mobile phones which are the part of a GSM mobile communications n/w that the operator observes & operates. At present, their dimension has reduced radically whereas the functionality level has very much increased. And one more benefit is that the time among charges has drastically enlarged. There are different elements to the mobile phone, though the two essential elements are the hardware & the SIM. The hardware includes the major elements of the mobile phone like the case, display, battery, & the electronics utilized to produce the signal & process the data receiver to be broadcasted. The mobile station includes a number called the IMEI. This can be set up on the mobile phone while manufacturing & it cannot be modified. It is accessed by the network

during registration to check whether the equipment has been reported as stolen. The SIM (Subscriber Identity Module) card includes the data which gives the user identity toward the network. And also, it includes different information like a number called the IMSI (International Mobile Subscriber Identity). When this IMSI is used in the SIM card, the mobile user could simply change mobiles by moving the SIM from one mobile to another. So mobile changing is easy without changing the same mobile number means that people would frequently improve, thus making a further income stream for the providers of network & serving to enhance the total financial victory of GSM.

Operation and Support Subsystem (OSS) :

The operation support subsystem (OSS) is a part of the complete GSM network architecture. This is connected to the NSS & the BSC components. This OSS is mainly used to control the GSM network & the BSS traffic load. It should be noted down that when the number of BS enhances through the subscriber population scaling then some of the preservation tasks are moved to the base transceiver stations so that the ownership cost of the system can be reduced. The GSM network architecture of 2G mainly follows a logical technique of operation. This is very simple as compared with present architectures of mobile phone network which utilize software-defined units to allow extremely supple operation. But the architecture of 2G GSM will demonstrate the voice & operational fundamental functions that are required & how they arranged together. When the GSM system is digital, then the network is a data network.

VI. RESULT AND ANALYSIS

Admin Login:

The implementation environment has software such as java in Windows XP operating system. The Login Screen provides the login for the admin and the already existing admin. Existing admin can login directly by entering the username and the password. If he is a new user then he has to register.

Figure 4: Screen shot for Admin login

PHR Owner Login:

The Login Screen provides the login for the PHR owner and the already existing Owner. Existing owner can login directly by entering the username and the password. If he is a new user then he has to register.

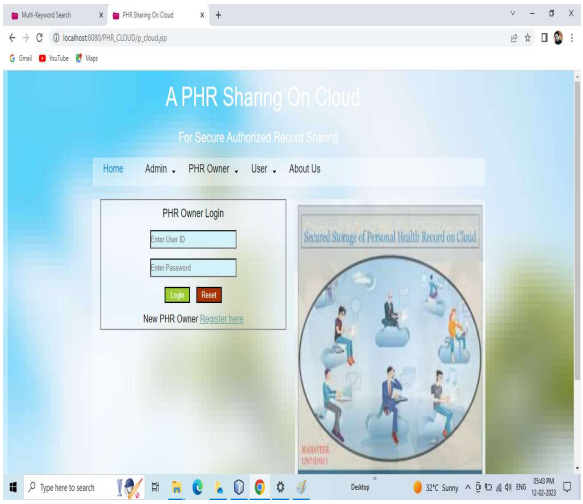


Figure 5: PHR Owner Login

PHR Owner Registration:

For the registration the owner has to enter the name, username, password, mobile name, email id .

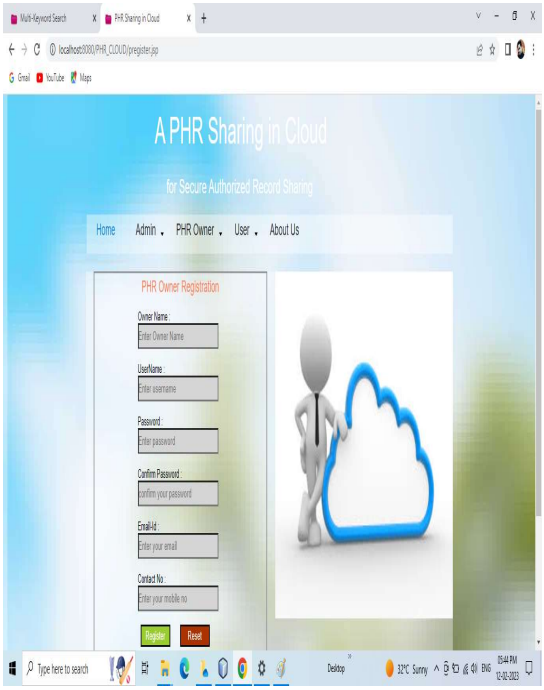


Figure 6: PHR Owner Registration

User Login and Registration:

For the registration the user has to enter the id, name, username, password, mobile name, email id and date of birth.

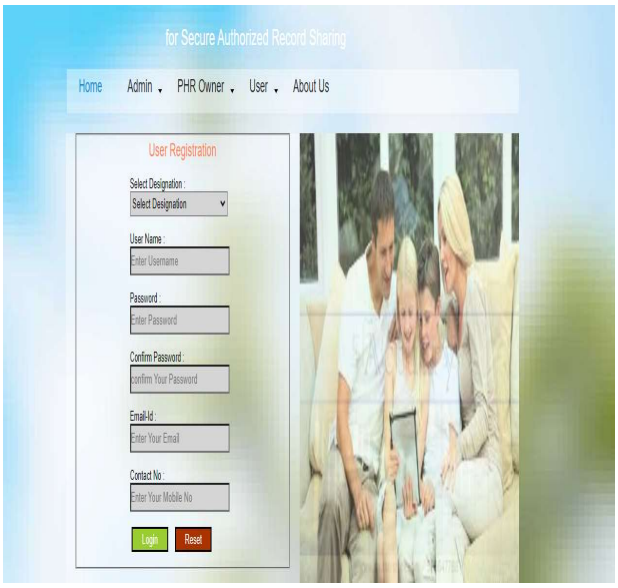


Figure 7: User Register Page

Admin has the following options enter personal health records and maintain personal health records.

Figure 8: File Upload

VII. CONCLUSION AND FUTURE ENHANCEMENT

Conclusion:

Cloud computing is changing our lives in many ways at a very quick space. Day by day utilization of cloud computing technologies is increasing in every part of the world. The cloud

computing solutions in healthcare can help the physicians to stay in touch with their patients and examine their health condition effectively at a low cost. The system discusses only about the account creation for both physician and patient. Further, the admin will view the patient details list.

With the increasing popularity of modern healthcare systems based on cloud storage, how to protect PHRs stored in the cloud is a central question. Cryptographic techniques are getting more versatile and often involve multiple keys for a single application which increases the key management overhead.

Future Enhancement:

The personal health records are now considered as the emerging trend where the security of data is the main privacy issue. In future work, the attribute based encryptions and its related techniques are applied in order to enforce for the security purpose and also it will be helpful in minimizing the key management problems and complexity.

REFERENCES

1. Dr.P.S.Jagadeesh Kumar and Ms.A.S.Chaithra,"A Survey on Cloud Computing based Health Care for Diabetes: Analysis and Diagnosis," in Proc. of IOSR Journal of Computer Engineering,2015.
2. Dr.S.S.Lomte and Ms. Jyoti Madhukar Shinde,"Physical Health Record System of a Patient using Cloud Computing", in Proc. of International Journal of Advance Scientific Research and Engineering Trends,2016
3. Murugalakshmi.K, Mrs.G.Geetha and Mrs.K.Sundara Velrani,"Cloud based healthcare monitoring system using wearable sensors," in Proc. of International Journal of Emerging Technology in Computer Science & Electronics, 2016.
4. R.NandhaKumar and Antony Selvadoss Thanamani,"A Survey on EHealth Care for Diabetes using Cloud Framework," in Proc. Of International Journal of Advanced Reasearch Trends in Engineering and Technology,2017.
5. Nidhi Jaini and Archana Jadhav,"A Survey paper on CDA generation and integration for Health Information Exchange based on Cloud Computing System,in Proc. Of International Journal of Innovative Research in Computer and Communication Engineering,2016.
6. Sushma S.A and Priyadarshini D.Kalewad,"Survey on Cloud Computing in Healthcare Systems," in Proc. Of International Journal of Engineering and Computer Science,2014.
7. C. Chu, S. Chow, and W. Tzeng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25 468- 477.
8. Kuo-Hsuan Huang, En-Chi Chang, and Shao-Jui Wang, "A Patient-Centric Access Control Scheme for Personal Health Records in the Cloud", Fourth International Conference on Networking and Distributed Computing, 2014.
9. Dixit, G. N. "Patient Centric Frame Work For Data Access Control Using Key Management In Cloud Server", International Journal of Engineering, 2 (4), 2013.

10. Chen, Y. Y., Lu, J. C., & Jan, J. K. "A secure EHR system based on hybrid clouds," Journal of medical systems, 36 (5), 3375 - 3384, 2012.
11. Leng, C., Yu, H., Wang, J., & Huang, J. "Securing Personal Health Records in the Cloud by Enforcing Sticky Policies," TELKOMNIKA Indonesian Journal of Electrical Engineering, 11 (4), 2200-2208, 2013.
12. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records", Proc. ACM Workshop Cloud Computing Security (CCSW 09), pp. 103 -114, 2009.
13. Chen Danwei, Chen Linling, Fan Xiaowei, He Liwen, Pan Su, and Hu Ruoxiang "Securing Patient-Centric Personal Health Records Sharing System in Cloud Computing", China Communications, Supplement No.1, 2014.
14. Ming Li, Shucheng Yu, and Yao Zheng, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE Transactions on Parallel and Distributed Systems, 24(1), pp. 131-143, 2013.
15. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "AttributeBased Encryption for Fine-Grained Access Control of Encrypted Data", Proc. 13th ACM Conf. Computer and Comm. Security (CCS 06), pp. 89-98, 2006.
16. M. Chase, and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption", Proc. ACM Conf. Computer and Comm. Security, pp. 121-130. 2009.
17. R. Canetti, and S. Hohenberger, "Chosen-Ciphertext Secure Proxy Re- Encryption", Proc. 14th ACM Conf. Computer and Comm. Security (CCS 07), pp. 185-194, 2007.