VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

M.Tech Software Engineering - Fall Sem -2019-20

SWE3002-Information and System Security

Review-3

Secured Medical Data Sharing in Cloud

Submitted by:

16MIS0433 – R.Mano Bala

16MIS0020 – M.Thanga Prakash

16MIS0450 – N.Ramya

Faculty : Jeyanthi N

Slot : F1+TF1

ABSTRACT :

In the current society, the transfer of information using internet is rapidly raising up, because it is easier and faster and has also proved security to transfer the data to destination. Security is a very important issue while transferring the sensitive data via internet because any unauthorized user can tamper the data and may make it useless or obtain the information unintended to him, especially in telemedicine. With the proliferation of patient's digital health records, and an increasing number of data breaches, protecting patient information is of utmost importance, with this respect lot of work has been done to secure medical data. Patient's health information confidentiality was an issue even when it was stored on paper. An unauthorized person could enter the hospital and steal the paper documents. Moreover, even any hospital staff can read paper documents which are not supposed to be viewed, as long as they have physical access to the document. So it is very important to protect patient's private information against unauthorized viewers by using cryptosystem confidentiality of these documents is enforced by putting them under some lock state and thereby enforcing physical access control to the document. So in this work, an attempt is made to provide high end security for the patient's sensitive data .This approach dealt with the security for medical data by using a cryptography mechanism named as IB cryptosystem.

Keywords : Cloud Computing, Data Sharing, Revocation, Identity-Based Encryption, Ciphertext Update, Medical data, Security.

INTRODUCTION:

To monitor the environment conditions in the wireless sensor networks use of large number of sensors and this can pass the information to the main location and this wireless sensor networks are mainly motivated by military applications and this sensor networks became very famous today and also used in many consumer and industrial areas, and now a days the promising fields like healthcare applications are maintained very well by these wireless sensor networks. Now a days Wireless medical sensor networks certainly improve quality-of-care, so privacy is ensured. Several modern cryptography mechanisms have been proposed and implemented in recent works. However providing a high end security and maximizing the privacy for the patient's data becomes very much essential. So many experiments are going on with this regard.

PROBLEM STATEMENT :

Wireless Sensor Networks (WSN) is an emerging technology that has the potential to transform the way of human life. Healthcare applications are considered promising fields for Wireless Medical Sensor Network, where patient's health can be monitored using Medical Sensors. Wireless Medical Sensor Networks (WMSNs) are the key enabling technology in healthcare applications that allows the data of a patient's vital body parameters to be collected by wearable biosensors. Current WMSN healthcare research trends focus on patient reliable communication, patient mobility and energy-efficient routing. Wireless medical sensor networks are more vulnerable to eavesdropping ,modification, impersonation and replaying attacks than the wired networks. So protection is an important task for patient data.

CONCEPT

The aim of this project is to revocable storage identity-based encryption (RS-IBE) for fulfills the security requirements of data sharing. And provide confidentiality and backward/forward secrecy simultaneously. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. Also revocable storage identity-based encryptions (RS-IBE) for building a cost-effective data sharing system that fulfills the security goals, and provide formal definitions for RS-IBE and its corresponding security mode.

EXISTING SYSTEM

A. Existing System Using Identity-Based Encryption (IBE)

Securing cloud data sharing. But could not overcome the above security goals. Unauthorized users should be prevented from accessing the plaintext of the shared data stored in the cloud server. In addition, the cloud server, which is supposed to be honest but curious, should also be deterred from knowing plaintext of the shared data.

- Backward secrecy means that, when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the subsequently Shared data that are still encrypted under his/her identity.
- Forward secrecy means that, when a user's authority is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her.

It appears that the idea for revocable identity-based encryption (RIBE) may be a guaranteeing methodology that fulfills the previously stated security prerequisites for information offering. RIBE Characteristics an instrument that empowers A sender will annex those present time period of the ciphertext such-and-such the recipient cam wood unscramble the ciphertext just under those condition that he/she is not renounced toward that time period.

As indicated in Figure.1, a RIBE-based data sharing system works as follows:

Step 1: The data provider first decides the users who can share the data. Then, encrypts the data under the identities, and uploads the ciphertext of the shared data to the cloud server.

Step 2: When user wants to get the shared data, she/ he can download and decrypt the corresponding ciphertext. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available.

Step 3: when the users authorization gets expired, data provider can download the ciphertext of the shared data, and then decrypt-then-re-encrypt the shared data such that user whose authorization expired is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again.

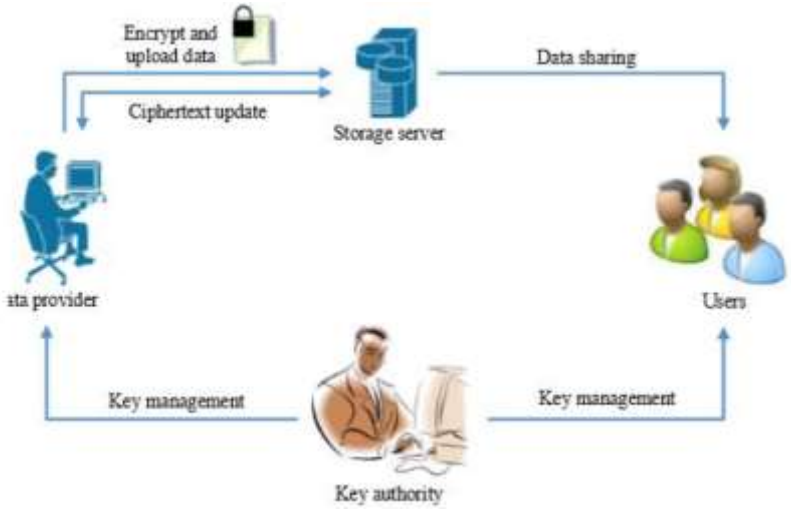


Figure 1: A Natural RIBE based Data Sharing

This data sharing system can provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can provide forward secrecy. This brings new challenges. The process of decrypt-then-re-encrypt necessarily involves users' secret key information, which makes the overall data sharing system vulnerable to new attacks, and it is inadvisable to update the ciphertext periodically by using secret key.

B. Challenges in Existing System

The process of frequent download-decrypt-re encrypt-upload can cause challenge in efficiency. This process cause high computation cost thus it is undesirable for cloud users with low capacity of computation and storage

• Unfortunately, existing solution is not scalable, since it requires the key authority to perform linear work in the number of non revoked users. In addition, a secure channel is essential for the key authority and non revoked users to transmit new keys.
• However, existing scheme only achieves selective security.
• This kind of revocation method cannot resist the collusion of revoked users and malicious non-revoked users as malicious non-revoked users can share the update key with those revoked users.
• Furthermore, to update the ciphertext, the key authority in their scheme needs to maintain a table for each user to produce the re encryption key for each time period, which significantly increases the key authority's workload.

Literature Review

16MIS0433(PAPER 1 TO 10)

PAPER 1: A Security Model for preserving the privacy of medical Big Data in a Healthcare Cloud using a Fog Computing Facility With pairing-Based Cryptography

In this paper (Hamid,2017)1, the authors have discussed about the security system in preserving medical data using fog computing and other various techniques.

They have discussed that nowadays, telemedicine is associate rising tending service wherever the tending professionals can diagnose, evaluate, and treat a patient mistreatment telecommunication technology.
To diagnose and judge a patient, the tending professionals have to be compelled to access the electronic medical history (EMR) of the patient, which might contain large transmission huge information together with X-rays, ultrasounds, CT scans, and magnetic resonance imaging reports.
For economical access and supporting quality for each the tending professionals still because the patients, the EMR has to be unbroken in huge information storage within the tending cloud. In spite of the recognition of the tending cloud, it faces completely different security issues. As an area of securing the cloud knowledge mission, this paper focuses on securing user's transmission knowledge among the cloud by mistreatment fog computing.
Telemedicine is one in all the rising ends for e-health analysis.

Conclusion:

They have a tendency to believe that by setting the default worth of the DMBD as shown and therefore the OMBD as hidden, they have a tendency to keep the original ADD safer. Also, have a tendency to believe that confirmative that the user is legitimate is far easier than police investigation the attacker, that is why they have a tendency to tried to touch upon the offender within the 1st place by giving the DMBD because the commencement.

PAPER 2: Privacy-Enhancing Technologies for Medical Tests Using Genomic Data. In this paper, (Ayday, 2013)2, the authors tend to propose privacy-enhancing technologies for medical tests and personalized medication strategies, which utilize patients' genomic information.

First, they tend to highlight the potential privacy threats on genomic information and therefore the challenges of providing privacy-preserving algorithms. Then, focusing specifically on a typical disease-susceptibility take a look at, they tend to develop a brand new design and propose privacy preserving algorithms by utilizing homomorphic encryption and proxy encryption We tend to extensively analyze the connection between the storage value (of the genomic data), the amount of genomic privacy (of the patient), and therefore the characteristics of the genomic information.

In this paper, they've got introduced privacy-preserving schemes for the employment of genomic information in medical tests and personalized medication ways. They've got planned new models supported the existence of a Storage and process Unit (SPU) between the patient and also the medical unit.

Conclusion:

This analysis may play a key role for customizing the storage redundancy of the genomic knowledge for every patient, whereas keeping the privacy of the patient at a desired level. They tend to area unit assured that our planned privacy-preserving schemes can encourage the utilization of genomic knowledge, by the individual and by the medical unit, and accelerate the move of genetic science into clinical observe.

PAPER 3: Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance.

In this paper (Alanazi, 2010)3, the authors have discussed about on how to secure the electronic medical data over unsecured communications.

Nowadays, health care is one in all the foremost vital subjects in life. In USA, a hundred billion bucks are spent thereon within the next ten years, consistent with consultants. The Electronic medical history (EMR) is typically a computerized legal medical history created in a company that delivers care, like hospital and doctors' surgery. Within the age of technology, one in all the foremost vital factors for EMR is that it secures the records for the patients, protects their rights and is answerable for the speech act of their information. An outline of this study has conferred the importance of the privacy of the EMR and therefore the patients' rights. Additionally, cryptography algorithms and security needs are mentioned and therefore the paper has also mentioned totally different design, styles and systems that are reported within the literature.

Conclusion:

Thus, code resolution with correct security measures could also be incompatible with the present software or different styles of code that may ought to be integrated resolution.

PAPER 4: Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme

In this paper (Zhang, 2017)4, the authors have discussed about protection of medical data using chaotic map based three factor authenticated key agreement scheme.

Telecare medication data Systems (TMIS) provides versatile and convenient e- health care but the medical records transmitted in TMIS square measure exposed to unsecured public networks, thus TMIS square measure a lot of prone to varied sorts of security threats and attacks. To supply privacy protection for TMIS, a secure and efficient documented key agreement theme is desperately required to guard the sensitive medical knowledge.

Recently, one researcher planned a biometrics-based authenticated key agreement theme for TMIS by victimization hash operate and present, they claimed that their theme may eliminate the protection weaknesses of Yan et al.'s scheme and supply dynamic identity protection and user namelessness. During this paper, however, they tend to demonstrate that researcher's theme suffers from replay attacks, man-in-the- middle attacks and fails to supply excellent forward secrecy. To beat the weaknesses of scheme, they tend to then propose a three-factor authenticated key agreement theme to modify the patient get pleasure from the remote care services via TMIS with privacy protection.

Conclusion:

In this paper, they need incontestable that researcher's authentication theme suffers from varied attacks and fails to produce many security properties. And then, they need planned a three-factor documented key agreement theme by victimization chaotic map-based cryptography to handle these issues. The planned theme realizes the protection of medical information transmitted within the open channel and provides privacy protection throughout the remote designation method that permits the patient to get pleasure from the secure and convenient care through the TMIS.

PAPER 5: SECURE MEDICAL DATA TRANSMISSION MODEL FOR IOT-BASED HEALTHCARE SYSTEMS

Due to the significant advancement of the internet of Things (IOT) within the attention sector, the protection, and also the integrity of the medical knowledge became huge challenges for attention services applications. This paper proposes a hybrid security model for securing the diagnostic text knowledge in medical pictures. The projected model is developed through integration either a pair of-D separate rippling rework one level (2D-DWT-1L) or 2-D separate rippling rework 2 level (2D-DWT-2L) steganography technique with a proposed hybrid encryption scheme. The proposed hybrid encryption schema is built using a combination of Advanced Encryption Standard, and Rivest, Shamir, and Adleman algorithms. The proposed model starts by encrypting the secret data; the result in a cover image using 2D-DWT-1 Lor 2D-DWT -2L. Both color and gray-scale images are used as cover images to conceal different text sizes.

Conclusion:

A secure patient's diagnostic information transmission model exploitation each color and gray-scale images as a cover carrier for health-care based IOT environment has been proposed. The planned model engaged either2D-DWT- 1Lor2D-DWT-2L steganography and hybrid mixing AES and RSA science techniques. The experimental results were evaluated on each color and gray-scale pictures with totally different text sizes. The performance was assessed supported the six applied math parameters (PSNR, MSE, BER, SSIM, SC, and correlation). Compared to the progressive strategies, the planned model evidenced its ability to cover the confidential patient's information into a transmitted cover image with high physical property, capacity, and lowest deterioration within the received stego-image.

PAPER 6: HCPP: CRYPTOGRAPHY BASED SECURE EHR SYSTEM FOR PATIENT PRIVACY AND EMERGENCY HEALTHCARE

Privacy concern is arguably the main barrier that hinders the preparation of electronic health record (EHR) systems that square measure thought-about additional efficient, less fallible, and of upper accessibility compared to ancient paper record systems. Patients are un-willing to accept the HER system unless their protected health data (PHI) containing extremely confidential knowledge is warranted correct use and speech act, that cannot be simply achieved while not patients' management over their own alphabetic character.
However, cautions should be taken to handle emergencies within which the patient could also be physically incompetent to retrieve the controlled PHI for emergency treatment.

During this paper, we've a bent to propose a secure EHR system, HCPP (Healthcare system for Patient Privacy), supported cryptologic constructions and existing wireless network infrastructures,to supply privacy protection to patients underneath any circumstances whereas enabling timely alphabetic character retrieval for life-saving treatment in emergency things.

Conclusion:

In this paper, we have a tendency to style a secure EHR system to safeguard patient privacy and change emergency health care. The system is incontestable to be resilient to numerous attacks, fulfill the required functionalities, satisfy the safety necessities, and maintain a decent balance between security and efficiency.

PAPER 7: PIXEL-BASED SCRAMBLING SCHEME FOR DIGITAL MEDICAL IMAGES PROTECTION:

The main aim of this paper is to propose a novel based on pixel scrambling scheme to protect the digital medical images in an effective way. In the proposed system they used simple pixel level XOR operation for scrambling the images but in this paper, we are implementing the innovative idea like cryptographic key uses the structural parameters as their encryption scheme. They also provided the cryptanalysis and the effectiveness of the proposed system is improved which has been proved by the stimulation of experiments. The need for distribution of digital medical pictures over networks has become a necessary a part of standard of living in medical systems

Conclusion:

In this paper, a digital medical pictures protection theme has been projected. Easy XOR operation is employed to scramble the first pictures that may attain a high efficiency. The scrambling key's a real random variety sequence derived from the multi-scroll chaotic attractors. The science security strength of the image scramble theme is provided by verity random variety sequence and huge key area. Identical scrambling key are often reused for multiple sessions that is that the same as in several alternative uneven block cipher coding schemes.

PAPER 8: PRIVACY PROTECTION FOR WIRELESS MEDICAL SENSOR DATA

In recent years, wireless sensing element networks are wide employed in health- care applications, like hospital and residential patient watching. Wireless medical sensing element networks are a lot of liable to eavesdropping, modification, impersonation and replaying attacks than the wired networks. Heaps of labor has been done to secure wireless medical sensing element networks. The present solutions will defend the patient knowledge throughout transmission, however cannot stop the within attack wherever the administrator of the patient information reveals the sensitive patient knowledge. During this paper, we have a tendency to propose a practical approach to prevent the inside attack by using multiple data servers to store patient data.

Conclusion:

In this paper, we've got investigated the safety and privacy problems within the medical detector information assortment, storage, and queries and bestowed a whole resolution for the privacy-preserving medical detector network. To secure the communication between medical sensors and information servers, we tend to use the light-weight secret writing theme and Macintosh generation theme supported SHA-3.

PAPER 9: Hierarchical and dynamic elliptic curve cryptosystem based self- certified public key scheme for medical data protection

Todays medical data are been made into e-data, networks such as zigbee networks plays a major role, which are large scale and low power sensor network. Patient data security must be taken care, in this paper HiDE is used which is self-certified public key scheme.

Hierarchical cluste based framework is used to serve a large amount of sensors. Secure Access point collects the medical data from secure sensors and send it to area cluster. Eliptic curve cryptosystem is introduced to provide security to secure sensors. ESP is better than RSA as it satisfies zero knowledge concept, so that cluster head can create a secure session with cluster member without Cluster member secret key. Thus it ensures confidentiality in medical data. The data are collected from wearable devices such as echo cardiogram etc. In wireless sensor network the medical data are extremely sensitive and person, it should be taken care during transmission. HiDE is used to achieve data confidentiality and low message overhead. It provides great flexibility and easy to manage the data from different hospitals and divisions.

Conclusion:

Thus, the HiDE will defend the confidentiality of sensitive medical information with low computation overhead, and keep appropriate network performance for wireless sensor networks.

PAPER 10: Medical internet of things and big data in healthcare.

These embrace devices that perpetually monitor health indicators, devices that auto-administer therapies, or devices that track real time health knowledge once a patient self-administers a medical care. as a result of they need raised access to high-speed net and smart phones, several patients have began to use mobile applications (apps) to manage numerous health desires. These devices and mobile apps are currently more and more used and integrated with telemedicine and telehealth via the medical net of Things (mIoT). This paper reviews mIoT and large knowledge in health care fields.

Challenges: (1) straightforward connectivity: an honest IoT platform makes it easy to attach devices and perform device management functions, scaled through cloud-based services, and to use analytics accomplish insight and achieve structure transformation.

Simple device management: A thoughtful approach to device management allows improved quality accessibility, exaggerated outturn, reduced unplanned outages and reduced maintenance prices.

Info ingestion: showing intelligence rework and store IoT information. arthropod genus bridge the divide between the info and also the cloud, creating it simple to drag within the information that's required. information is eaten from various information sources and platforms, then the essential values area unit extracted exploitation wealthy analytics.

Methods: mIoT may be a essential piece of the digital transformation of health care, because it permits new business models to emerge and allows changes in work processes, productivity enhancements, value containment and increased client experiences.

Results: Wearables and mobile apps nowadays support fitness, health education, symptom following, and cooperative illness management and care coordination. All those platform analytics will raise the connectedness of information interpretations, reducing the number of your time that finish users pay piecing along knowledge outputs.

Conclusions:

A brand new class of "personalized preventative health coaches" (Digital Health Advisors) can emerge. These staff can possess the abilities and also the ability to interpret and perceive health and well-being knowledge. They're going to facilitate their purchasers avoid chronic and diet-related malady, improve psychological feature perform, reach improved psychological state and reach improved lifestyles overall. Because the international population ages, such roles can become more and more vital.

16MIS0020(PAPER 11-20)

PAPER 11: Diagonal queue medical image steganography with Rabin cryptosystem.

The patient info like patient medical records with personal identification info of patients may be hold on in each storage and transmission. This paper describes a unique methodology for activity medical records like HIV reports, female child foetus, and patient's identity info within their brain disorder medical image files viz. scan image or imaging image victimisation the notion of obscurity with regard to a diagonal queue least significant bit substitution. organization queue plays a dynamic role in resource sharing between multiple communication parties. Rabin cryptosystem is employed for secret medical information writing, since it's computationally secure against a chosen-plaintext attack and shows the difficulty of number factorization. the result of the cryptosystem is organized in numerous blocks and equally distributed sub-blocks. the key cipher blocks and sub-blocks area unit assigned dynamically to chose diagonal queues for embedding.

The receiver gets four values of medical information plaintext like one ciphertext, thus solely licensed receiver will establish the right medical information. The Rabin cryptosystem could be a public key enciphering technique. it's established on number-theoretic issues allied to the stiffness of number factorization and computing sq. roots modulo of number, that is easy once the resolving is acquainted, however terribly complicated once it's hid. The Rabin cryptosystem needs a receiver's public key to write the text and a non- public key to decode it. After Rabin coding, cipher text are going to be obtained. currently cipher text are going to be divided into blocks and every block has sixteen bits. After that, every block is split into equally distributed 4-bit sub- blocks. Then the every image block's sixty four bits area unit organized in fifteen diagonal queues from right bit to left bit insertion victimisation inventory accounting property of queue from prime to bottom. A novel secret transmission theme has been planned mistreatment the notion of opacity with reference to a diagonal queue least significant bit substitution, that is a very effective different for sending secure medical records and patient's personal identification data along side the acceptable medical neurological disorder image. the key message blocks and sub-blocks ar allotted dynamically by the sender to the neurological disorder cowl image blocks with reference to diagonal queues, that will increase security levels and offers dynamic impact to the planned algorithmic program. The planned algorithmic program has used Rabin public key cryptosystem at cryptography level to supply confidentiality of Brain medical data of patient at medical information center and end-to-end communication, since it's computationally secure associated chosen-plaintext attack, hugely smaller liable to prevalence investigation attack and enciphered message attacks

PAPER 12: Improved Quality of Patient Care and Data Security Using Cloud Crypto System in EHR.

Information storing and retrieving is vital in care sector in order that the physicians adopt EHR (Electronic Health Record) for maintaining the patient's record, that makes quick access by workers, specialists and patient's.consequently, EHR's area unit crucial to the digitisation of care since, it improves patient care thereby guaranteeing patient safety, quality and potency by reducing care prices. Cloud is turning into the infrastructure for many of the EHR to produce less costly associate degreed measurability of an application while not comprising the privacy of information. This paper deals with varied ways employed in text mining beside cloud security in EHR and knowledge protection in care. we've got additionally created a study on cloud that uses Health level7 (HL7) message exchange commonplace interface for the record exchange, integration, sharing and retrieval of electronic health data. The adoption of EHR considered with the three components viz., secure storage, repository and Exchange of clinical information are more prominent in data capturing, storing and retrieval of structured and unstructured data which improve patient safety, quality and evidence based practice due to standardization of heath care. The important aspect of text mining in EHR involves a formulation of clinical diagnosis along with complicated surgery protocols, functional status scores or stages of disease. Extraction of knowledge from such records is very important with respect to modeling of medical care and scientific tasks as well. Accessing and securing medical data is more complicated in healthcare sector so that cloud provides the infrastructure for EHR access thereby ensuring the privacy of data, so that physicians and patient's uses authorized key control system mechanisms. There is no security for patient data due to data

breach which happens in various private healthcare centers. Record exchange is very important. In health care sector, and accordingly, cloud uses Health level7 (HL7) message exchange standard interface for the record exchange, integration, sharing and retrieval of electronic health information.

Paper 13: Social networking healthcare

The world of "Social Networking", a cultural phenomenon of recent years, has evolved an application paradigm, Instant Messaging (IM), into a feature rich, highly interactive and context sensitive service delivery environment. Terms such as buddy lists, presence and IM-bots have emerged as building blocks for services that significantly enhance the user experience. Mapping this paradigm to healthcare can deliver a highly innovative communication platform for information sharing, monitoring and care plan execution. Buddy lists become care groups, presence becomes patient context (e.g. blood sugar level) and IM-bots become Ehealthcare services, capable of delivering appropriate contextual information to care groups. This paper outlines the benefit of such a crossover and proposes a component based architecture to meet the ever evolving health care needs of society.

Paper 14: Privacy preserving multi-keyword ranked search over encrypted data

With the advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data have to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. In this paper, for the first time, we define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). We establish a set of strict privacy requirements for such a secure cloud data utilization system. We first propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. To improve search experience of the data search service, we further extend these two schemes to support more search semantics. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given. Experiments on the real-world data set further show proposed schemes indeed introduce low overhead on computation and communication.

Paper 16: PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs

Wireless Body Area Networks (WBANs), as a promising health-care system, can timely monitor human physiological parameters. Due to the limitation of communications, power, storage and computation in WBANs, a cloud assisted WBAN flourishes and provides more reliable, real-time, and intelligent health-care services for patients and mobile users. In addition, security and privacy concerns are also of paramount importance during the communications between WBAN and cloud. In this paper, we propose a priority based health data aggregation (PHDA) scheme with privacy preservation for cloud assisted WBANs to improve the aggregation efficiency among different types of health data. Specifically, we first explore social spots to help forward health data and enable users to select the optimal relay according to their social ties. According to different data priorities, the adjustable forwarding strategies can be selected to forward the user's health data to the cloud servers with the reasonable communication overheads. The security analysis demonstrates that the PHDA can achieve identity and data privacy preservation, and resist the forgery attacks. Finally, the performance evaluation shows that the PHDA achieves the desirable delivery ratio with reasonable communication costs and lower delay for the data in different priorities

Paper 17: Privacy protection and intrusion avoidance of medical data in cloudlet.

With the popularity of wearable devices, along with the development of clouds and cloudlet technology, there has been increasing need to provide better medical care. The processing chain of medical data mainly includes data collection, data storage and data sharing, etc. Traditional healthcare system often requires the delivery of medical data to the cloud, which involves users' sensitive information and causes communication energy consumption. Practically, medical data sharing is a critical and challenging issue. Thus in this paper, we build up a novel healthcare system by utilizing the flexibility of cloudlet. The functions of cloudlet include privacy protection, data sharing and intrusion detection. In the stage of data collection, we first utilize Number Theory Research Unit (NTRU) method to encrypt user's body data collected by wearable devices. Those data will be transmitted to nearby cloudlet in an energy efficient fashion. Secondly, we present a new trust model to help users to select trustable partners who want to share stored data in the cloudlet. The trust model also helps similar patients to communicate with each other about their diseases. Thirdly, we divide users' medical data stored in remote cloud of hospital into three parts, and give them proper protection. Finally, in order to protect the healthcare system from malicious attacks, we develop a novel collaborative intrusion detection system (IDS) method based on cloudlet mesh, which can effectively prevent the remote healthcare big data cloud from attacks. Our experiments demonstrate the effectiveness of the proposed scheme.

Paper 18: SPOC: A secure and privacy preserving opportunistic framework for mobile health care emergency

With the pervasiveness of smart phones and the advance of wireless body sensor networks (BSNs), mobile Healthcare (m-Healthcare), which extends the operation of Healthcare provider into a pervasive environment for better health monitoring, has attracted considerable interest recently. However, the flourish of m-Healthcare still faces many challenges including information security and privacy preservation. In this paper, we propose a secure and privacy-preserving opportunistic computing framework, called SPOC, for m-Healthcare emergency. With SPOC, smart phone resources including computing power and energy can be opportunistically gathered to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure. In specific, to leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in m-Healthcare emergency, we introduce an efficient user-centric privacy access control in SPOC framework, which is based on an attribute-based access control and a new privacy-preserving scalar product computation (PPSPC) technique, and allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data. Detailed security analysis shows that the proposed SPOC framework can efficiently achieve user-centric privacy access control in mHealthcare emergency. In addition, performance evaluations via extensive simulations demonstrate the SPOC's effectiveness in term of providing high-reliable-PHI process and transmission while minimizing the privacy disclosure during m-Healthcare emergency.

Paper 19: A home healthcare system in the cloud – addressing security and privacy challenges

Cloud computing is an emerging technology that is expected to support Internet scale critical applications which could be essential to the healthcare sector. Its scalability, resilience, adaptability, connectivity, cost reduction, and high performance features have high potential to lift the efficiency and quality of healthcare. However, it is also important to understand specific risks related to security and privacy that this technology brings. This paper focuses on a home health care system based on cloud computing. It introduces several use cases and draws an architecture based on the cloud. A comprehensive methodology is used to integrate security and privacy engineering process into the software development lifecycle. In particular, security and privacy challenges are identified in the proposed cloud-based home healthcare system. Moreover, a functional infrastructure plan is provided to demonstrate the integration between the proposed application architecture with the cloud infrastructure. Finally, the paper discusses several mitigation techniques putting the focus on patient-centric control and policy enforcement via cryptographic technologies, and consequently on digital rights management and attribute based encryption technologies

Paper 20: A Secure Electronic Medical Record Sharing Mechanism in the Cloud Computing Platform

Privacy is a very important issue when storing electronic medical records. According to the definition set out in the Health Insurance Portability and Accountability Act (HIPPA), the confidential section of the electronic medical record needs to be protected. Thus, a mechanism to protect the patient's privacy is needed during electronic medical record exchange and sharing. The privacy protection mechanism can be categorized into four types, namely anonymity, pseudonymity, unlinkability, and unobservability. In previous research in this area, mathematical conversions and cross reference tables

have been utilized to conceal the confidential part of the electronic medical record to achieve privacy protection. However, it is harder to use these methods with respect to the unlinkability and unobservability mechanisms. Thus, this paper tries to improve on this aspect, and improves the unlinkability mechanism between the patient and the electronic medical record. Cloud computing is known for its fast computation capability and provides large storage space. Through cloud computing, the electronic medical record system in a hospital can be integrated, to facilitate the exchange and sharing of electronic medical records, and to provide smaller hospitals or clinics that have fewer resources with adequate electronic medical record storage space.

16MIS0450(PAPER 20-30)

PAPER 21 :Privacy Protection and Intrusion Avoidance for Cloudlet- based Medical Data Sharing

[1] In this paper the author has build up a novel healthcare system by utilizing the flexibility of cloudlet. The functions of cloudlet consist of privacy protection, data sharing and intrusion detection. In the stage of data collection, firstly utilize Number Theory Research Unit (NTRU) method to encrypt user as body data collected by wearable devices. Those data will be end to nearby cloudlet in an energy efficient fashion.

Secondly, present a new trust model to help users to select trustable partners who want to share stored data in the cloudlet. The trust model also helps identical patients to communicate with each other about their diseases. Thirdly, divide users medical data stored in remote cloud of hospital into three parts, and give them proper protection. Finally, in order to protect the healthcare system from malicious attacks, design a novel collaborative intrusion detection system (IDS) method depend on cloudlet mesh, which can effectively prevent the remote healthcare big data cloud from attacks.

PAPER 22 :Privacy- preserving multi- keyword ranked search over encrypted cloud data

[2] In this paper, for the first time, it was defined and solved the challenging issue of privacy preserving multi-keyword ranked search over encrypted cloud data (MRSE). They establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multi-keyword semantics, they choose the efficient similarity measure of “coordinate matching”, i.e., as many matches as possible, to capture the relevance of data documents to the search query. They further use “inner product similarity” to quantitatively evaluate such similarity measure. First propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. Thorough study of inspecting privacy and efficiency guarantees of proposed schemes is given.

PAPER 23 : Spoc: A secure and privacy- preserving opportunistic computing framework for mobile- healthcare emergency

[3] In this paper, author developed a secure and privacy-preserving opportunistic computing framework, called SPOC, for m-Healthcare emergency. With SPOC, smart phone resources involving computing power and energy can be opportunistically collected to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure. In specific, to leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in m- Healthcare emergency, They introduce an efficient user-centric privacy access control in SPOC framework, which is depend on an attribute-based access control and a new privacy preserving scalar product computation (PPSPC) technique, and permits a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data. Detailed security study display that the proposed SPOC framework can efficiently achieve user- centric privacy access control in mHealthcare emergency.

PAPER 24 :Emerging information technologies for enhanced healthcare

[4] This paper first introduces the main aim of this special issue and gives a brief guideline. Then, the present situation of the adoption of EMRs is reviewed. After that, the emerging data technologies are presented which have a great impact on the healthcare provision. These include health sensing for medical data collection, medical data study and utilization for accurate detection and prediction. Next, cloud computing is discussed, as it may offer scalable and cost-effective delivery of healthcare services.

PAPER 25 :Privacy preserving health data processing

[5] This paper developed a practical solution for privacy preserving medical record sharing for cloud computing. On the basis of the classification of the attributes of medical records, they use vertical partition of medical dataset to achieve the consideration of distinct parts of medical information with different privacy concerns. It mainly consisting four components that is:

(1) vertical data partition for medical information publishing,

(2) data combining for medical dataset accessing,

(3) integrity checking, and
(4) hybrid search across plaintext and cipher text, where the statistical analysis and cryptography are innovatively combined together to provide multiple paradigms of balance among medical data utilization and privacy protection. A prototype system for the huge scale medical data access and distributing is implemented.

The usage of electronic health data from distinct sources for statistical analysis requires a toolset where the legal, security and privacy concerns have been taken into consideration. The health data are typically placed at different general practices and hospitals. The data analysis includes of local processing at these locations, and the locations become nodes in a computing graph. To support the legal, security and privacy concerns

PAPER 26 : In this paper the proposed toolset for statistical study of health data uses a combination of secure multi-party computation (SMC) algorithms, symmetric and public key encryption, and public key infrastructure (PKI) with certificates and a certificate authority (CA). The proposed toolset should cover a wide range of data analysis with different data distributions. To accomplish this, huge set of possible SMC algorithms and computing graphs have to be supported.

PAPER 27 : In this paper , author propose a priority based health data aggregation (PHDA) scheme with privacy preservation for cloud assisted WBANs to improve the aggregation efficiency between different types of health data. Specifically, first explore social spots to help forward health data and enable users to select the optimal relay according to their social ties. According to distinct data priorities, the adjustable forwarding methods can be selected to forward the user as health data to the cloud servers with the reasonable communication overheads. The security analysis describes that the PHDA can achieve identity and data privacy preservation, and resists the forgery attacks.

PAPER 28 : In this article, investigate security and privacy protection in MHNs from the perspective of QoP, which offers users adjustable security protections at fine- grained levels. Specifically, first introduce the architecture of MHN, and point out the security and privacy limitations from the perspective of QoP. Then present some countermeasures for security and privacy protection in MHNs, consisting privacy-preserving health data aggregation, secure health data processing, and misbehavior detection.

PAPER 29 : Chen, Min, et al. (2016). In this paper the present scenarios of traditional wearable devices have many shortcomings like insufficient accuracy, long-term wearing, etc. So, carrying out a health monitoring with traditional wearable devices is very difficult to be sustainable.

This research designed a Smart Clothing in order to acquire healthcare huge information by sustainable health monitoring. This proposed design will facilitate the unobtrusive gathering of numerous physiological indicators of the human body. Here, the smart clothing was built by using cloud computing, big data analytics, and mobile internet. Particularly, the collection of electrocardiograph signals by smart clothing is mainly used for emotion detection and mood monitoring

PAPER 30 : Raj, Arjun,and Rani, Suja MS (2015). In the current scenarios, the demand for MCPS (medical cyber-physical systems) is increasing day by day. Each and every healthcare firm are making use of MCPS in order to ease the complicated tasks. These systems will assess the status of the patient by making use of physical sensors and employ the corresponding reaction by making use of actuators. The sensor devices are attached to the patient that states the real-time data. Currently, CPS (cyber-physical systems) is being used as a tool for the cyber-attacks. So these attacks will definitely have an effect on the patient either directly or indirectly on their life. So, here the researcher deployed intrusion detection system where it makes use of behavioral rule specification that is efficient in order to identify the unknown attack.

Table of Content

S.NO	AUTHOR	TECHNOLOGY AND SOFTWARE	ATTACKS ADDRESSED	DRAWBACKS
1.	Al Hamid	Photo encryption algorithm, Fog computing , Decoy file, Bilinear pairing function, Elliptic curve Diffie Hellman	To diagnose and evaluate patients Electronic media Record.	Data theft, legal and policy issues, cyber security, input of information, output for information and command.
2.	Ayday	Pallier cryptosystem, homo-morphic encryption, proxy encryption	Prevents privacy in patient's medical and genomic data.	Storage issues, Criminal evidences in DNA research.
3.	Alanazi	RSA, Elliptic curve cryptosystems, Symmetric cryptography	Securing data over un-trusted communications.	Asymmetric cryptography does not provide repudiation, integrity and confidentiality.
4.	Zhang	Cryptanalysis, chaotic map based three-factor authenticated key agreement scheme	Protecting tele- care medical, man in the middle attacks, modification attacks.	Duplicate three-factor key generated, guessing the entropy.
5.	M Elhoseny, G Ramirez-Gonzalez	Hybrid(AES &RSA) algorithm; Embedding 2D-DWT-2L algorithm, Hybrid decryption algorithm.	Less distortion occurs within the original cover data set so that it can be easily cracked by the attacker.	Difficulty increased in Decrypting the original data.
6.	J Sun, X Zhu, C Zhang, Y Fang	Cryptographic construction method; Wireless network infrastructure; Electronic health record system.	Less privacy of the patient's high confidential data.	Lost or the path of the patient's file was changed due to wireless network.

7.	J Hu, F Han	Pixel based image scrambling scheme; ISA algorithm; Cryptographic key uses the chaotic theory.	Less efficient in validation of the digital medical images and it was 100 times slower than the popular AES.	Need well trained professionals to work on this technique and it need frequent Update of the system/software.
8.	X Yi, A Bouguettaya, D Georgakopoulos	Paillier encryption; Elgamal cryptosystems; Lightweight encryption scheme; MAC generation scheme based on SHA-3	Database can be accessed easily, when one of the data server is compromised.	Too difficult to get the simple info of the patient from the database even by the authorized person.
9.	Tseng, C.H., Wang, S.H., & Tsaur, W. J.	HiDE	Authentication and Verification.	It is difficult to maintain all the cluster member and cluster head keys separately. It takes lot of storage pace
10.	Dimitrov, D. V.	mIOT	Data storage and Confidentiality.	Verification is less done on the receiver side. Thus this system may fail to achieve the verification.

S.No	Paper Title	Methodology Used	Attacks Addressed	Drawbacks
11	Diagonal queue medical image steganography with Rabin cryptosystem.	Diagonal queue least significant bit substitution. Rabin Cryptosystem	Secret transmission scheme of the medical data such as MRI, HIV reports.	Plain Text Attack. The transmission channel is not encrypted from the external
12.	Improved Quality of Patient Care and Data Security Using Cloud Crypto System in EHR.	Electronic Health card. Health Level 7 Message Exchange	Key Control System. Confidentiality.	Authentication and verifications of keys is difficult. It requires huge cost
13.	Social networking healthcare	Uses instant messaging and buddy list	Meets the evolving needs of patients	No guarantee of security and privacy of data
14.	Privacy preserving multi-keyword ranked search over encrypted data	Co-ordinate matching	It has low overhead on computation and communication	Integrity of the rank order in cloud search is not trustable.
15.	Cloudlet-based efficient data collection in wireless body area networks	Virtual machine and virtualized cloudlet is used	Provide cost effective communication	Maintenance cost is high
16.	PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs	Used health data aggregation	Low delay and less communication cost	Time consuming
17.	Privacy protection and intrusion avoidance of medical data in cloudlet.	Number theoretic research method used(NTRU)	Has flexibility to use cloudlet for data storage and provide security	IDS might fire false alarm
18.	SPOC: A secure and privacy preserving opportunistic framework for mobile health care emergency	Uses user-centric privacy access control method based on attribute based access control	Provide efficient user centric approach and improves performance.	Need to have smartphone always.
19.	A home healthcare system in the cloud – addressing security and privacy challenges			
20.	A Secure Electronic Medical Record Sharing Mechanism in the Cloud Computing Platform			

S.No	AUTHOR	TECHNOLOGY AND SOFTWARE	ATTACKS ADDRESSED	DRAWBACKS
21.	Min Chen, Yongfeng Qian, Jing Chen, Kai Hwang, Shiwen Mao, Long Hu,	Number Theory Research Unit intrusion detection system (IDS)	privacy protection, data sharing and intrusion detection protect the healthcare system from malicious attacks	IDS might fire false alarm.
22	N. Cao, C. Wang, M. Li, K. Ren, and W. Lou,	coordinate matching	privacy preserving multi-keyword ranked search over encrypted cloud data (MRSE) strict privacy requirements	Integrity of the rank order in the search result assuming the cloud server is untrusted
23	R. Lu, X. Lin, and X. Shen, "Spoc	Uses user – centric privacy access control method based on attribute-based access control	user- centric privacy access control in mHealthcare emergency.	Can carry on Smartphone-based experiments to verify the effectiveness of the SPOC framework.
24	J.-J. Yang, J. Li, J. Mulder, Y.Wang, S. Chen, H.Wu, Q.Wang, and H. Pan	cloud computing is discussed	medical data collection, medical data study and utilization for accurate detection and prediction	Does not cover all the aspects and applications
25	J.-J. Yang, J.-Q. Li, and Y. Niu	a combination of secure multi- party computation	(1) vertical data partition for medical information publishing, (2) data combining for medical dataset	none

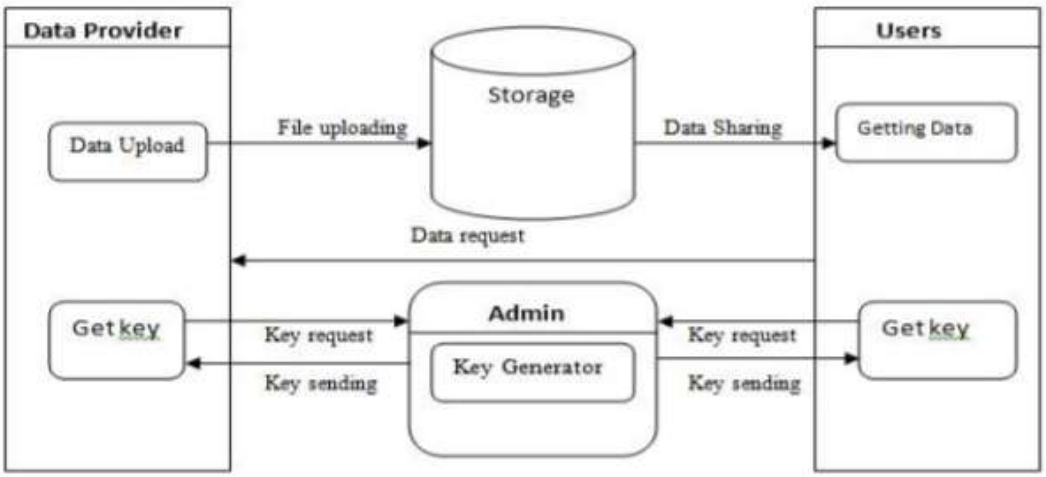
			accessing, (3) integrity checking, and (4) hybrid search	
26	A. Andersen, K. Y. Yigzaw, and R. Karlsen	secure multi-party computation (SMC) algorithms, symmetric and public key encryption, and public key infrastructure (PKI) with certificates and a certificate authority (CA)	wide range of data analysis with different data distributions.	
27	K. Zhang, X. Liang, M. Baura, R. Lu, and X. S. Shen	WBANs priority based health data aggregation (PHDA)	data privacy preservation, and resists the forgery attacks.	Time consuming
28	K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen, and H. H. Luo	privacy- preserving health data aggregation, secure health data processing, and misbehavior detection	privacy-preserving health data aggregation, secure health data processing, and misbehavior detection.	
29	Chen, Min, et al	Smart Clothing	traditional wearable devices have many shortcomings like insufficient accuracy, long-term wearing. traditional wearable devices is very difficult to be sustainable	

30	**Raj, Arjun,and Rani, Suja MS**	CPS (cyber-physical systems) is being used as a tool for the cyber-attacks deployed intrusion detection system	cyber-attacks	

PROPOSED SYSTEM

In our proposed system using revocable identity-based encryption (RIBE) that fulfills the aforementioned security requirements for data sharing. RIBE features a mechanism that enables a sender to append the current time period to the cipher text such that the receiver can decrypt the cipher text only under the condition that he/she is not revoked at that time period. Such a data sharing system can provide confidentiality and backward secrecy.

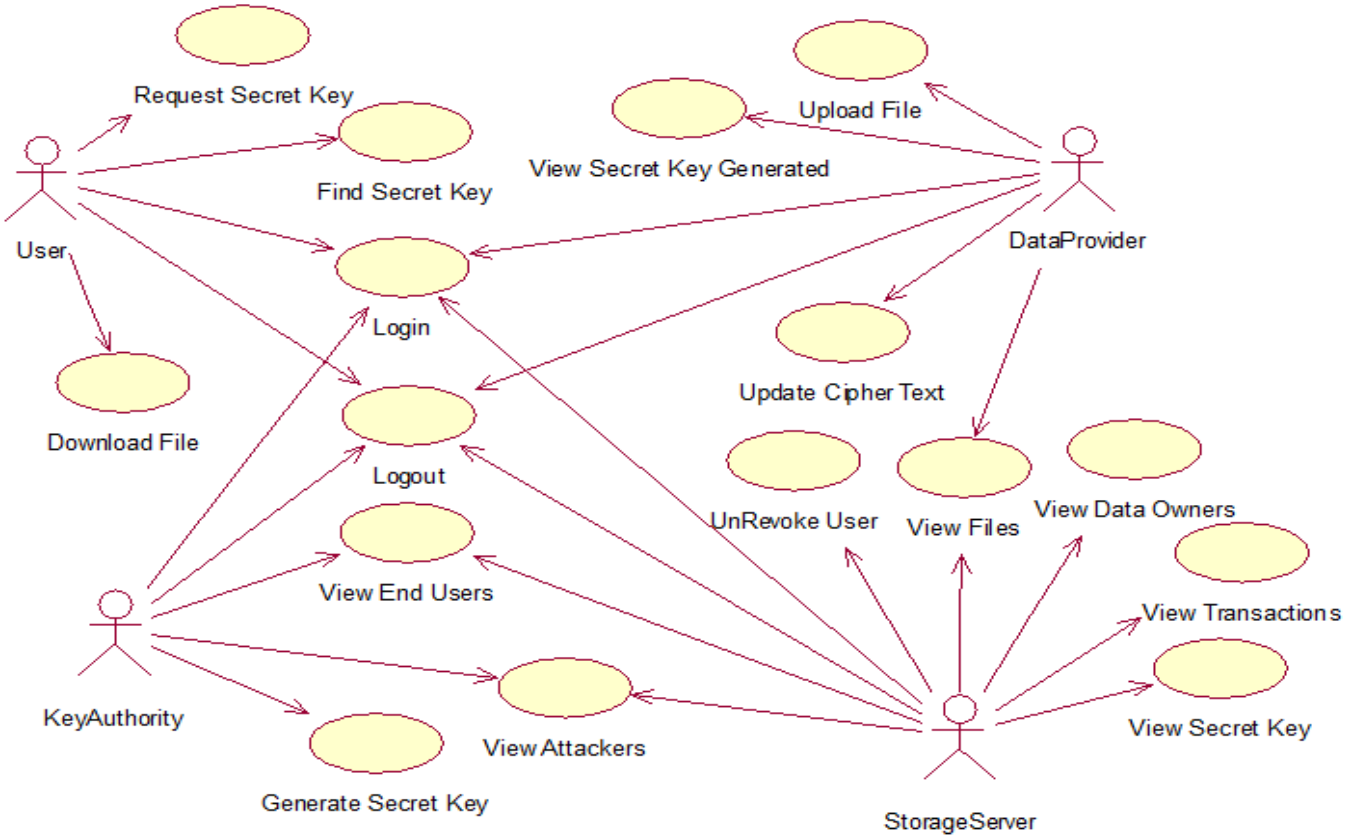
SYSTEM ARCHITECTURE



IMPLEMENTATION MODULES

- Data Provider
- Key Authority(KA)
- Cloud Storage
- Users

USE CASE



DATA PROVIDER:
The data provider first decides who will share the data and he will upload the data with their identities. The data provider uploads the data by encrypting it. Data provider can check for number of uploads and number of downloads of the data.

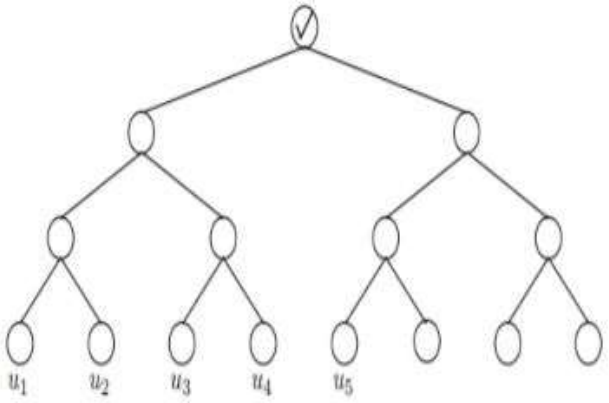
KEY AUTHORITY:
The key authority generates secret key when a user requests for data accessing.

CLOUD STORAGE:
The data uploaded by data provider is stored in cloud. The cloud enables the users to download by entering the secret key. The cloud storage will also have a revocation list, if an unauthorized/authority expired user tries to access data he/she is revoked. The revoked user is not allowed to login again.

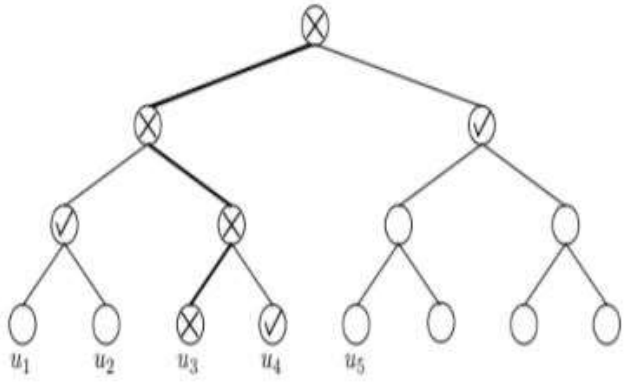
USER:
The function of the user is to request for secret key and accessing the data stored in cloud. The user decrypts the data by downloading it from cloud. If a unauthorized user attempts to login it will show a message you are under revocation.

If the user is authorized and yet revoked due to his/her expiration he/she can be unrevoked by checking the validity to access the data. To implement this we propose an identity based encryption model using a binary tree structure for storing identities and time period functionalities of the users. Now we take a binary tree B, revocation list RL, current time ct, revocation time rt and nodes as vi. Take two null sets X,Y corresponding to non-revoked and revoked users. If an unauthorized/authority expired client wants to access the shared data he/she must use secret key. At the time of accessing cipher text, if the users current time is more than the revocation time he/she is marked as revoked and thus prevented from further access of shared data. The non-revoked users secret key is updated and

they can access the data using updated secret key which is provided by the key authority. This overcomes the un-scalability problem mentioned in previous schemes.The pictorial representation of revoked and non-revoked users are shown in Fig



(a). No user is under revocation



(b).User u3 is under revocation.

IMPLEMENTATION

In this paper we introduce cost-effective RS-IDE that fulfills our three security goals data confidentiality, forward secrecy and backward secrecy. We constructed an algorithm KUNodes[10] to update the key when user tries to access and revokes unauthorized user. The flow diagram for the above mentioned model is shown below in Fig

The KUNodes algorithm works as follows:

a. First when a user have to access data from cloud storage, the cloud server asks for secret key.
b. If the user enters the secret key correctly he/she will be allowed to access the data.
c. If the user fails to enter correct secret key or the authorization is expired, the cloud server restricts the user by revoking his identity by checking the time period of user in revocation list.
d. Now the cloud server checks the revocation list to find if there are any valid users that belongs to the organization. e. If cloud finds a valid user it again un-revokes the user and allow to access data stored in cloud.

A.MODIFIED KUNODES ALGORITHM

The modified KUNodes algorithm takes two null sets X,Y to store corresponding non-revoked and revoked users. If an user whose authority got expired tries to access the shared data he/she is marked under revocation and is given as output to set Y. The non-revoked users are given as output to set X and their secret keys are updated.

ALGORITHM:

KUNodes(B,RL,tp)

$X, Y \leftarrow \emptyset$

$\forall (u_i, ct_i) \varepsilon RL$

If $ct_i \leq tp$ then add path(u_i) to X.

Return X

$\forall ct_i \geq tp$ then add path(u_i) to Y.

Return Y.

If Y → Valid(B) then

Unrevoke.

The KUNodes algorithm helps in validating the authorized users by checking the revocation list. This RS-IBE scheme reduces the computational costs and un-scalability than the previous KU-CSP scheme.

B.ENCRYPTION AND DECRYPTION:

The data shared is encrypted to the cloud server based on identity of the data provider, so that when he/she wants the decrypt the data they can access the cipher text by providing name of the data provider and file name. A trusted third party provides the secret key to the users while accessing stored data in cloud. The simultaneous key updation when a user is revoked results in achieving our three security problems data confidentiality, forward secrecy and backward secrecy.

C.REVOCATION:

The user is revoked when his/her authority is expired or security key is compromised and thus preventing the data from unauthorized access.

D.UN-REVOKE:

The cloud checks for the validity of users in the revocation list and un-revokes if he/she is valid and grant access for previously or subsequently shared data.

ADVANTAGES OF PROPOSED SYSTEM:

- The proposed scheme can provide confidentiality and backward/forward2 secrecy simultaneously
- The procedure of ciphertext update only needs public information. Note that no previous identity-based encryption schemes in the literature can provide this feature;
- The additional challenges in computation and storage complexity, which are brought in by the forward secrecy are overcomed.

SAMPLE CODE

GenerateKey.jsp

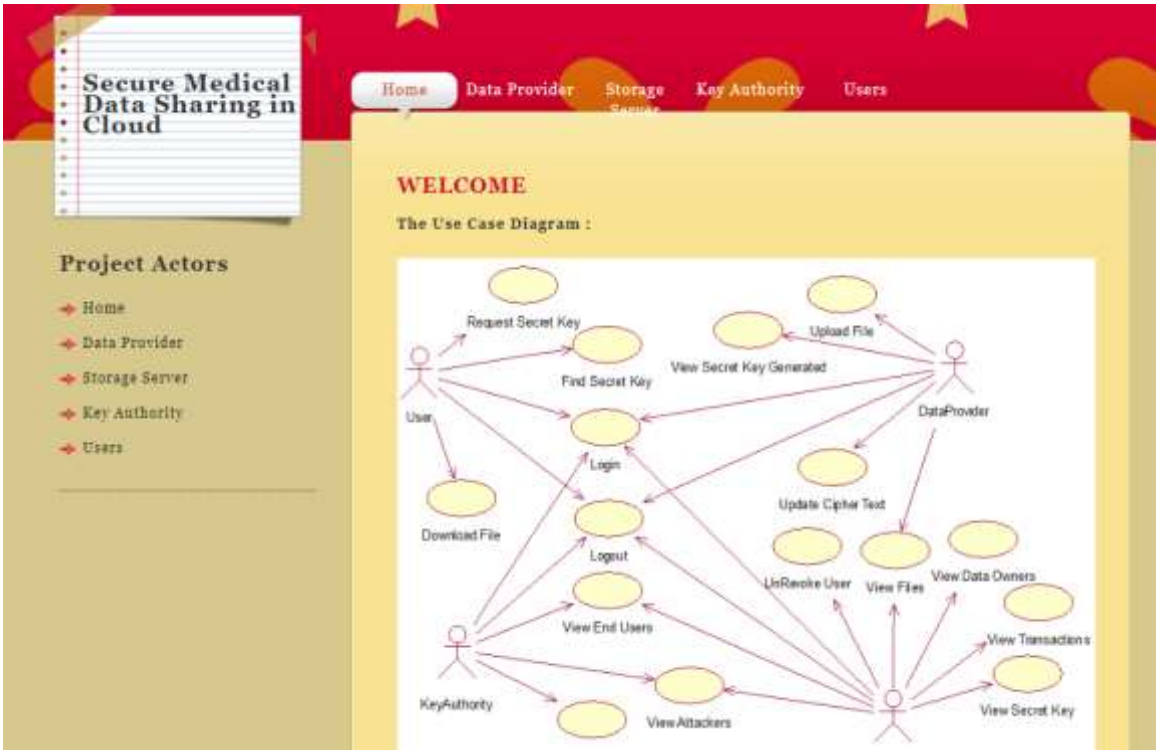
```
<html>
<style type="text/css">
body {
```

```
        background-color: #FFFFFF;
    }
    </style>
    <body>
    <center>
     
    </center>
    <br><br><br>
     <%
                    int uid = Integer.parseInt(request.getParameter("usid"));

      try {

                    KeyPairGenerator kg = KeyPairGenerator.getInstance("RSA");
                    Cipher encoder = Cipher.getInstance("RSA");
                    KeyPair kp = kg.generateKeyPair();
                    PublicKey pubKey = kp.getPublic();

                    // RSA produces 1024 bits Key

                   byte[] pub = pubKey.getEncoded();
                   String s = pub.toString();

         String str="Yes";
        Statement st1 = connection.createStatement();
        String query1 ="update request set sk='"+s+"' where id='"+uid+"' ";
           st1.executeUpdate (query1);

           connection.close();
          }

          catch(Exception e)
          {
            out.println(e.getMessage());

          }
      response.sendRedirect("GenerateKey.jsp");

    %>

</body>
</html>
```

RESULTS AND FUTURE SCOPE

By following the RS-BIE scheme reached our one of the security problem i.e un-scalability. The scheme proposed by Li et al lacks in reducing the computational costs and un-scalability. So we proposed a model by introducing key authority to overcome these security problems. The major challenge in cloud is security of data. So we concentrated mainly on data confidentiality, forward and backward secrecy but this results in reducing computation costs and increasing complexity. So we look forward to reduce the complexity in our future work by re-encryption of cipher text without any key updation process.

SCREENSHOTS




Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
WELCOME TO bala
The data provider (e.g., David) first decides the users (e.g., Alice and Bob) who can share the data. Then, David encrypts the data under the identities Alice and Bob, and uploads the ciphertext of the shared data to the cloud server.
Data Provider Main
Upload Data
View Uploaded Files
View Secret Key Generated
Update ciphertext
Logout


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
Upload Data
Select File :-
Choose File
manobala.txt
File Name :-
manobala.txt
Hi THis is Sample Data
Encrypt
Data Provider Main
Home
Logout


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
Upload Data
File Name :-
bWFub2JhbGEudHh0
SGkgVEhpcyBpcyBTYW1wbGUgRGF0YQ0K
Upload
Data Provider Main
Upload Data
View Uploaded Files
View Secret Key Generated
Update ciphertext
Logout


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
Data Uploaded Successfully !!!
BACK
SDS
Data Provider Main
Upload Data
View Uploaded Files
View Secret Key Generated
Update ciphertext
Logout


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
YOUR DATA FILES:: bala
User ID | File Name | Provider Name | Date & Time
15 | connect.jsp | bala | 20/10/2019 23:25:34
16 | hello.txt | bala | 21/10/2019 08:37:05
17 | mano.txt | bala | 07/11/2019 11:39:14
18 | ramya.txt | bala | 07/11/2019 13:17:18
19 | prakash.txt | bala | 07/11/2019 14:56:29
20 | karthik.txt | bala | 07/11/2019 15:46:41
21 | manobala.txt | bala | 08/11/2019 19:38:37
<<<Back
Data Provider Main
Home
Logout


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
YOUR DATA FILES KEY:: bala
User ID | Owner Name | File Name | Date & Time
mano | bala | connect.jsp | [B@5a82c23d
mano | bala | hello.txt | [B@53aae98f
mano | bala | mano.txt | [B@241d3aff
mano | bala | ramya.txt | [B@34b190fd
mano | bala | prakash.txt | [B@1001b998
mano | bala | karthik.txt | [B@1c4e56e
<<<Back
Data Provider Main
Home
Logout


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
CIPHER TEXT DECRYPTED CONTENTS
Data Provider Main
Home
Logout
manobala.txt
Hi THis is Sample Data
Encrypt


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
END USER MAIN :: mano
End User Menu
Home
Request Secret Key
Find Secret Key
Download
Log Out


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
Request Secret Key
Enter Owner Name : bala
Enter File Name : manobala.txt
Request SKey
End User Menu
Home
Log Out


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
Requested Secret Key Details
Request Already Sent To KA (Key Authority) !!!
BACK
End User Menu
Home
Request Secret Key
Find Secret Key
Download
Log Out


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
WELCOME TO KEY AUTHORITY
Key Authority Menu
Home
GENERATE SECRET KEY
View End Users
View Attackers
Log Out


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
KEY GENERATION
Menu
Home
User ID
User Name
Owner Name
File Name
Secret Key
4
mano
bala
connect.jsp
[B@5a82e23d
5
mano
bala
hello.txt
[B@53aae98f
6
mano
bala
mano.txt
[B@241d3aff
7
mano
bala
ramya.txt
[B@34b190fd
8
mano
bala
prakash.txt
[B@1001b998
9
mano
bala
karthik.txt
[B@1c4e56e
10
mano
bala
manobala.txt
Generate Key

Secure Medical Data Sharing in Cloud

Home | Data Provider | Storage Server | Key Authority | Users

Menu

- Home

KEY GENERATION

User ID	User Name	Owner Name	File Name	Secret Key
4	mano	bala	connect.jsp	[B@5a82c23d
5	mano	bala	hello.txt	[B@53aae98f
6	mano	bala	mano.txt	[B@241d3aff
7	mano	bala	ramya.txt	[B@34b190fd
8	mano	bala	prakash.txt	[B@1001b998
9	mano	bala	karthik.txt	[B@1c4e56e
10	mano	bala	manobala.txt	[B@10edca8b

Secure Medical Data Sharing in Cloud

Home | Data Provider | Storage Server | Key Authority | Users

Menu

- Home

VIEW ALL END USERS

User Image	User Name	DOB	E-Mail	Mobile	Location
	mano	16/07/1998	mano@gmail.com	9876543210	India

Secure Medical Data Sharing in Cloud

Home | Data Provider | Storage Server | Key Authority | Users

End User Menu

- Home
- Log Out

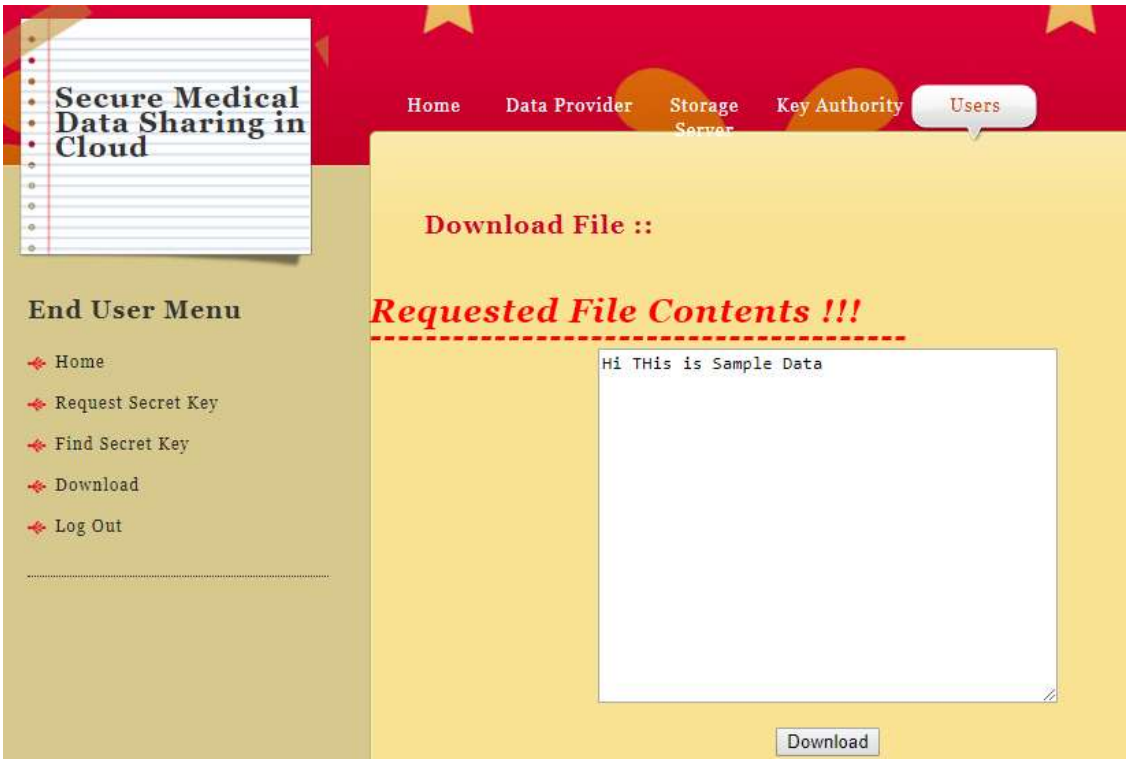
Requested Secret Key Details

Enter File Name :

FIND SECRET KEY

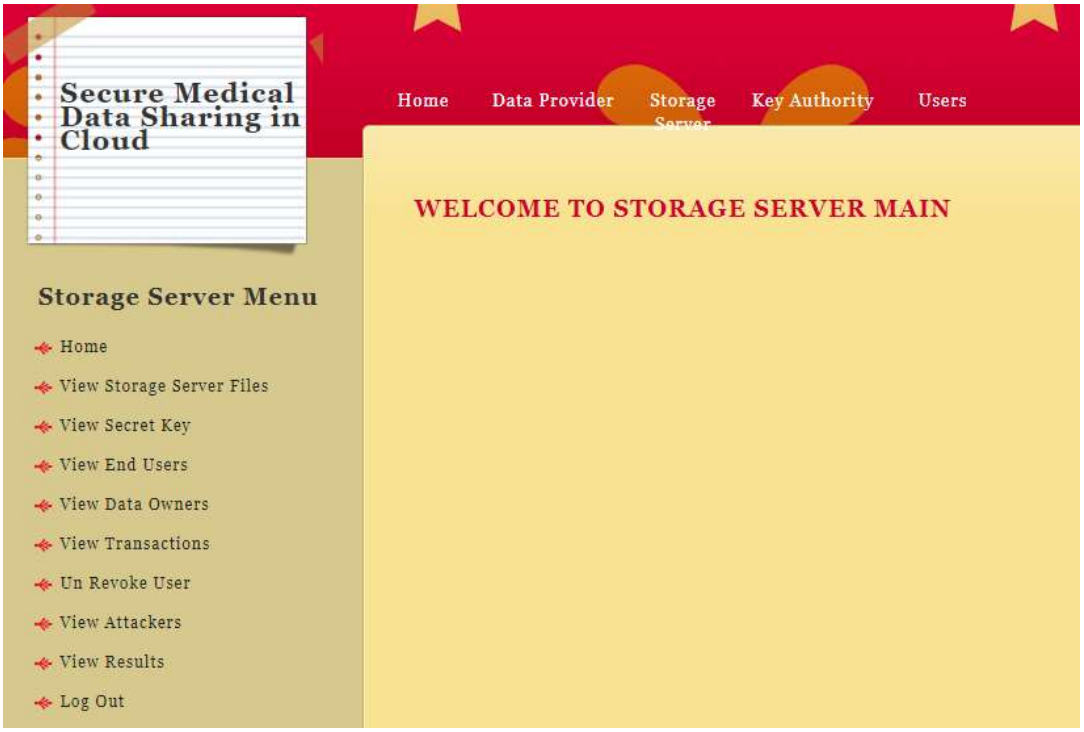
Secret Key : [B@10edca8b


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
End User Menu
Home
Log Out
Request Secret Key
Enter File Name & Secret Key ::
User Name :-
mano
Enter File Name :-
manobala.txt
Secret Key :-
[B@10edca8b
DOWNLOAD


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
End User Menu
Home
Request Secret Key
Find Secret Key
Download
Log Out
Download File ::
Requested File Contents !!!
Hi THis is Sample Data
Download


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
End User Menu
Home
Log Out
Request Secret Key
Enter File Name & Secret Key ::
User Name :-
mano
Enter File Name :-
manobala.txt
Secret Key :-
123
DOWNLOAD


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
End User Menu
Home
Request Secret Key
Find Secret Key
Download
Log Out
File Name / Secret Key Mismatch !!!
You Are An Attacker !!! Now U R Under Revokation
Back


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
Storage Server Menu
Home
View Storage Server Files
View Secret Key
View End Users
View Data Owners
View Transactions
Un Revoke User
View Attackers
View Results
Log Out
WELCOME TO STORAGE SERVER MAIN


Secure Medical Data Sharing in Cloud
Home
Data Provider
Storage Server
Key Authority
Users
Storage Server Menu
Home
Log Out
Un Revoke User
Select User Name To Un Revoke
mano
UnRevoke

Secure Medical Data Sharing in Cloud

Home | Data Provider | Storage Server | Key Authority | Users

Storage Server Menu

- Home
- Log Out

DATA Owner Details

User ID	User Name	File Name	Operation	Date & Time
26	bala	connect.jsp	Upload	20/10/2019 23:25:34
27	mano	connect.jsp	Download	20/10/2019 23:30:15
28	bala	hello.txt	Upload	21/10/2019 08:37:05
29	mano	hello.txt	Download	21/10/2019 08:47:30
30	bala	mano.txt	Upload	07/11/2019 11:39:14
31	mano	mano.txt	Download	07/11/2019 11:42:19
32	bala	ramya.txt	Upload	07/11/2019 13:17:18
33	mano	ramya.txt	Download	07/11/2019 13:19:37
34	bala	prakash.txt	Upload	07/11/2019 14:56:29
35	mano	prakash.txt	Download	07/11/2019 15:01:58
36	bala	karthik.txt	Upload	07/11/2019 15:46:41
37	mano	karthik.txt	Download	07/11/2019 15:48:28
38	bala	manobala.txt	Upload	08/11/2019 19:38:37
39	mano	manobala.txt	Download	08/11/2019 19:45:08
40	mano	manobala.txt	Download	08/11/2019 19:45:43

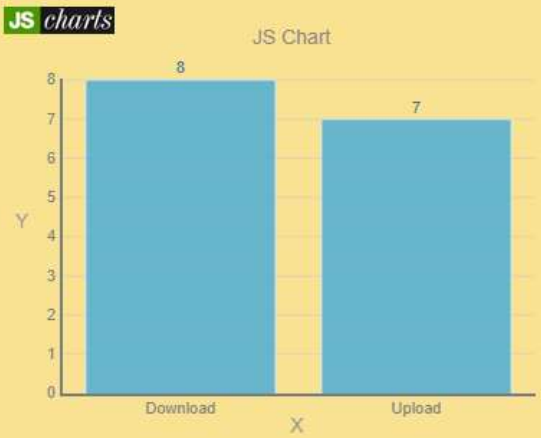
Secure Medical Data Sharing in Cloud

Home | Data Provider | Storage Server | Key Authority | Users

Storage Server Main

- Home
- Logout

DATA TRANSACTION RESULTS



REFERENCE -16MIS0433

1. Al Hamid, H. A., Rahman, S. M. M., Hossain, M. S., Almogren, A., & Alamri, A. (2017). A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing- based cryptography. IEEE Access, 5, 22313-22328.

2. Ayday, E., Raisaro, J. L., & Hubaux, J. P. (2013, February). Privacy- Enhancing Technologies for Medical Tests Using Genomic Data. In NDSS.

3. Alanazi, H. O., Alam, G. M., Zaidan, B. B., & Zaidan, A. A. (2010). Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance. Journal of Medicinal Plants Research, 4(19), 2059-2074.

4. Zhang, L., Zhu, S., & Tang, S. (2017). Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme. IEEE Journal of Biomedical and health informatics, 21(2), 465-475.

5. Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A. (2018). Secure medical data transmission model for IoT-based healthcare systems. IEEE Access, 6, 20596-20608.

6. Sun, J., Zhu, X., Zhang, C., & Fang, Y. (2011, June). HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare. In 2011 31st International Conference on Distributed Computing Systems (pp. 373-382). IEEE.

7. Hu, J., & Han, F. (2009). A pixel-based scrambling scheme for digital medical images protection. Journal of Network and Computer Applications, 32(4), 788-794.

8. Yi, X., Bouguettaya, A., Georgasskopoulos, D., Song, A., & Willemson, J. (2016). Privacy protection for wireless medical sensor data. IEEE transactions on dependable and secure computing, 13(3), 369-380.

9. Tseng, C. H., Wang, S. H., & Tsaur, W. J. (2015). Hierarchical and dynamic elliptic curve cryptosystem based self-certified public key scheme for medical data protection. IEEE Transactions on Reliability, 64(3), 1078-1085.

10. Dimitrov, D. V. (2016). Medical internet of things and big data in healthcare. Healthcare informatics research, 22(3), 156-163.