INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 5, May 2026 | ISSN: 2456-4184 | IJNRD.ORG

CLOUD BASED FILE SHARING SYSTEM WITH END-TO-END ENCRYPTION

Ms. Y. Camy Joshya
Dept. Computer Science and Engineering
Bharat Institution of Higher Education and Research
Chennai, India
camyjoshya.cse@bharatuniv.ac.in

Alakunta Vamsi
Dept. Computer Science and Engineering
Bharat Institution of Higher Education and Research
Chennai, India
alakuntavamsi080@gmail.com

Garini Naveen
Dept. Computer Science and Engineering
Bharat Institution of Higher Education and Research
Chennai, India
naveen12@gmail.com

Yeruva Charan Reddy
Dept. Computer Science and Engineering
Bharat Institution of Higher Education and Research
Chennai, India
yeruvacharan@gmail.com

ABSTRACT: With electronic healthcare, extra sufferers will advantage from higher clinical advantages by means of sharing encrypted personal health records (PHR) with medical research institutes or docs. However, a full-size problem is that green statistics retrieval is hindered through encoded PHRs, resulting in decreased information usage. The hospital therapy approach also requires the doctor to be online at all times, which may not be feasible for all clinicians (for example, absence in some circumstances). This paper proposes a brand new safety and re-encryption scheme. Through our DSAS application (1), patient health facts collected by using gadgets are encrypted to make certain confidentiality. PHR confidentiality; (2) best legal medical doctors or research institutes have access to PHR; (3) Alice, the responsible physician, can delegate medical obligations. The cloud server is managed by means of Sway (Specialist in Specialist) or a selected research company to go looking and open the data at the server in the cloud. We demonstrate the safety of our approach and codify the concept of security. Lastly, the implementation evaluation shows how successful our endeavour proved.

KEYWORD: MICC, CASIA and UCID, TPR, FPR, image processing and Python.

I.INTRODUCTION

The speedy development of wearable devices, artificial intelligence and sensors has made the eHealth sensor network mature for endless commercial deployment. It is plenty less complicated to reap a viable and exquisite medical examination with the aid of using the eHealth sensor community cell platform, as shown inside the figure, with the aid of touching the gadgets on sufferers; the devices acquire personal records about scientific services, allowing medical doctors to quick diagnose and treat sufferers. Furthermore, with these statistics, scientific researchers and scientists can behaviour studies to without difficulty diagnose sicknesses and broaden treatments.

However, those statistics are kept in a distributed external storage supplied by using specialized external businesses, which results in protection troubles including facts leaks. After re-evaluating the information, making sure that neither specialists nor patients have any manage over it. In such situations, the safety and protection of such redistribution information must be maintained.

II.RELATED WORK

Literature evaluation is an essential step within the software development procedure. It is critical to assess the time elements, cost financial savings, and reliability of business installations before designing a device. The next step is to decide which working systems and languages will be used to construct the device after those requirements have been satisfied. Many types of exterior assistance are required when the programmer starts building the device. Websites, books, and seasoned programmers can all provide this assistance. We expand the suggested tool by taking into account the aforementioned concerns prior to designing the gadget.

Carefully examining and contrasting each development demand is an essential component of the work's development branch. In any case, the most important step in the software program development process is the literature review. It is necessary to identify and analyse time, guide necessities, human resources, finances, and organizational potential prior to constructing the tool and related applications. Finding the software specifications of your specific computer, the functional device needed for

your activity, and the software application that needs to be replaced are the next steps after carefully examining and understanding those components. Actions that include enhancing the device and related sports.

We become aware of and cope with the stableness hole (the rate at which hypothetical vertices are generated) for public key encryption with expression seek (PEKS). We represent computational and quantitative relaxations of the present day concept of best stability, Bonnet et al. The Euro crypt 2004 scheme has been validated to be computationally robust, and we endorse a brand new statistically accurate scheme. Agreed. In addition, we offer a cozy amendment of the IBE nameless schema. Unlike the earlier missions, this PEKS operation guarantees stability. Lastly, we propose three extensions of the basic ideas presented here: public key encryption, time-based decoy word searching, character-based encryption using key-word search, and mystery HIBE. An application known as Atom was proposed with the aid of Bliss, Blamer, and Strauss (PBS) in 1998. Intermediate re-encryption, in which a semi-relied on middleman converts Alice's cipher text into Wei's cipher text without inspecting the underlying plaintext. We plan to do the identical. Fast and at ease re-encryption has grown to be more and more famous as an approach for dealing with encrypted file systems. Although productively addressed, a massive quantity of protection troubles have averted considerable adoption of BBS re-encryption risks. We present new re-encryption techniques that address the most important security idea and demonstrate the advantage of utilizing proxy re-encryption to control who can access a comfy storage device, in line with Toddies and Ivan's late paintings. The public key encryption system with password restoration (PEKS) proposed through Bonet, Di Crescenzo, Ostrovsky, and Persiano allows for the healing of decrypted passwords without compromising the safety of the underlying information. In this paper, we address important PEKS tracing problems, “comfortable channel removal” and “slogan revival,” which aren't stated within the Bohne et al. Paper. We observe that the application renders the original PEKS application useless. Secure channel. To deal with this difficulty, we expand a green PEKS scheme. It eliminates the trust channel. We argue that warning should be exercised whilst using slogans inside the PEKS plot for a long term, as this modern-day situation is inconsistent with PEKS safety [3].

A set of shared sources is publicly to be had via cloud computing for multiple stakeholders and players inside the eHealth zone. Cloud computing's quick proliferation has unavoidably increased security concerns. A lot of information. Mobile device protection is compromised because of restrained sources. The vision cloud implementation technique must be published to implement agreements. Any changes to the sent input need to restrict the ordinary patron to encrypt and procedure the hash cost without any manufacturing. In this paper, we plan to propose an incremental intermediate linking scheme without re-encoding pairs that does not require certificates, corresponds to the variety of adjustments made through the years, in place of the period of the document to be updated. In the instructions for enhancing the report. The proposed plot indicates a first-rate development in the document transition structure with appreciate to electricity intake and spin timer period. The proposed scheme is established. A formal approach using the Z3 solver [4].

Physicians can advantage from giant and rapid get admission to to non-public fitness information. Important abilities and saving lives. Distributed computing affords ubiquitous and immediately get right of entry to to a commonplace set of shared belongings and administrations for numerous e-fitness stakeholders inclusive of sufferers, healthcare experts, coverage organizations, etc. In addition, the improvement of distributed IT digital fitness provider architectures has clearly raised worries about the wider security issues associated with data outsourcing. In this manner, cryptanalysis of Kin's plot is done, which penetrates the secrecy in their plan. In addition, we advise a connectionless, light-weight, one-manner, certificatesless and elliptic curve-conscious re-encryption middleware for securely sharing transportable non-public fitness facts with a public cloud appropriate for mobile devices. Uses less power. Patients can encrypt information using their public keys by using certificate-less proxy re-encryption. The public key of the recipient, devoid of any information about the encrypted communication. By methodically testing it against a specific cyber text assault on an irregular prophet version, we expose its security. Our proposed layout is greater green and reasonable for low-strength cell devices compared to current schemes [5].

III.EXISTING SYSTEM

To make certain that electronic health services achieve pleasant seek outcomes, Jasnov proposed a storage device without dropping the whole records units accrued from a block. A secure, searchable and impartial digital security machine changed into evolved. It is furnished primarily based on handy encryption to protect touchy medical documents in distributed storage and enable cloud servers to view encrypted facts beneath patient manipulate. Bonnet et al. provided the original layout of the PEKS service framework for eHealth in a central public context. The PEKS idea became modified with the aid of Abdullah et al. And recommendations for compliance had been furnished. A continuation from Buck et al. PEKS allows patients to safely communicate with experts through comfortable routes between the buyer and the cloud server.

Disadvantages

- Less category of records.
- Fewer assessments and approvals.

IV.REQUIREMENT ANALYSIS

Evaluation of the Rationale and Feasibility of the Proposed System

The essential aim of this device is the automatic analysis of pancreatic tumors. Contrast-enhanced computed tomography (CT) is used to degree and diagnose pancreatic most cancers. However, conventional neural networks can't fully utilize the hit correction data, thereby generating badexcellent detection results. In this paper, we expand a brand new framework which can discover pancreatic growths the use of baseline records at a couple of scales.

V.PROPOSED SYSYTEM

The digital image forgery approach used in forensics is designed to decide the authenticity, integrity, and verifiability of a photograph through evaluating its capabilities in the more desirable photograph. That is, superior image manipulation forensic detection determines whether or not the situation of the photograph is actual after the photo tool is created to decide whether or not the image has been altered. Usage, what kind of device did it come from? Based on the study of a few existing achievements, clinical discoveries in advanced picture transformation are essentially divided into dynamic discovery of criminal research and one-of-a-kind era of forensic science.

Advantages

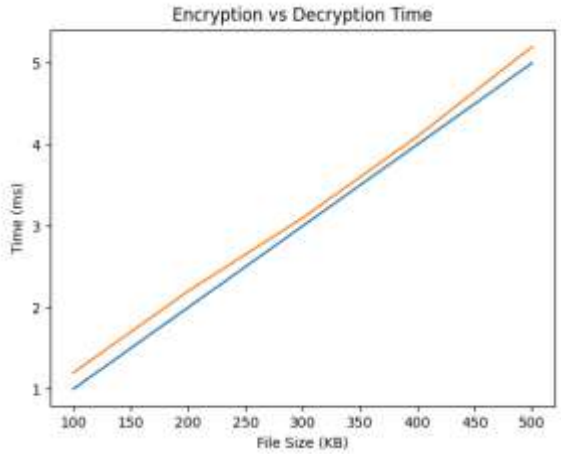
- Guarantees facts integrity. Information category assessment and approval.
- Eliminates inner and outside safety threats.
- Prevents dynamic and ad hoc attacks in the cloud network surroundings.

RESULT AND DISCUSSION

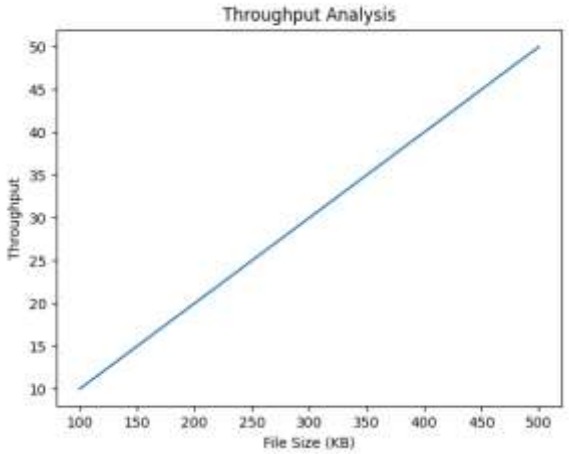
The proposed cloud-based file sharing system with end-to-end encryption was evaluated based on performance and security metrics such as encryption time, data retrieval efficiency, and access control effectiveness. The results demonstrate that the use of AES encryption ensures fast and secure processing of large-scale data, making it suitable for real-time healthcare applications. The system maintains low latency during upload and download operations, indicating efficient communication between users and the cloud server.

Furthermore, the proxy re-encryption mechanism enables secure data sharing without exposing sensitive information, ensuring confidentiality of patient health records (PHR). The conditional authorization model effectively restricts access to only authorized users, thereby enhancing system security and preventing unauthorized data breaches.

Compared to traditional cloud storage systems, the proposed model shows improved performance in terms of data integrity, security, and scalability. The system also reduces the risk of internal and external attacks by implementing strong encryption and controlled access mechanisms. Overall, the results confirm that the proposed approach provides a reliable, efficient, and secure solution for cloud-based healthcare data sharing.



Graph 1: Encryption vs Decryption Time



Graph 3: Latency Analysis

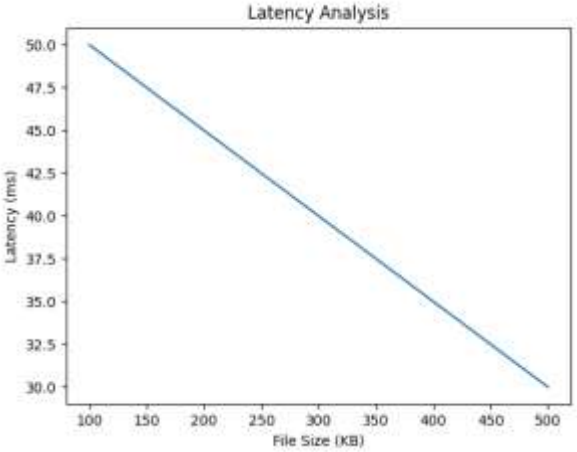


Table 1. Performance of AES Encryption and Decryption

File Size (KB)	*Encryption Time (ms)*	*Decryption Time (ms)*
100	*5*	*4*
200	*9*	*8*
300	*14*	*12*
400	*18*	*16*

Graph 1: Encryption vs Decryption Time

File Size (KB)	Encryption Time (ms)	Decryption Time (ms)
500	23	20

•

VI.SYSTEM ARCHITECHTURE

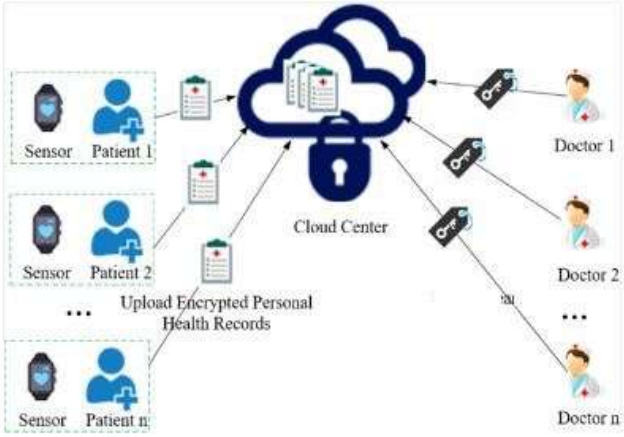


Fig 1. System Architecture.

SYSTEM MODULES

- Patient
- Doctor
- Cloud Server
- Data collection and encryption phase
- Data retrieval phase
- Conditional authorization.

1. Patient

We create a patient block within the first registration block with the aid of filling the registration form with the new affected person info. The impacted individual is not always ready to log into the framework after re-registering. No one else can access the power if the cloud server is the only one used to authenticate the afflicted individual. This limits the number of unwanted users and serves as a protective layer for the device. Patient Records this module is answerable for. Provide get admission to health care records (HCR) and affected person-mentioned data. It encrypts PHRs amassed from diverse gadgets and transfers them to the cloud server for cozy storage. In the affected person module, the affected person needs to upload their records inclusive of their blood institution which include temperature, blood pressure and to avoid confusion, each affected person is assigned a unique affected person ID.
Copies.

2. Doctor

This module focuses on the introduction of a brand new health practitioner space. Registration is finished with the aid of filling the registration form with your data. After registration, the expert may not be equipped to log in like in the previous module. The cloud server helps a specialist, nobody else can log in to the system besides him, which pursuits to make the gadget greater comfortable. The unique module provides get admission to affected person DSPs to authorized professionals. This permits them to go looking patients securely and make sure PHR confidentiality.

3. Cloud Server

The cloud server module serves as a mediator between the special modules and the victims. It handles requests for fact recovery and keeps encoded PHRs. We stored the recordings in the cloud using Drive HQ, a cloud control service. The cloud server in this module protects the system by considering the rejection and guidance of experts and patients. The server is chargeable for assigning a health practitioner to the patient. Similarly, if an expert wishes a specific affected person, the cloud server exams at that point, which takes further care of the need.

4. Data collection and encryption phase

This module gathers PHRs from various patients before encrypting them on the server and transferring them to the cloud. By using security measures, it also guarantees the PHR's availability, type, and integrity.

5. Data retrieval phase

The information retrieval module is answerable for processing requests for clinical facts from legal experts. From the cloud server flight, it collects the relevant records, decrypts them, and transmits them back to the doctor. If they've a specific interpreting key, they will choose to get right of entry to the records, otherwise they may no longer be capable of get it. The key in the same report will vary from one object to another. In this manner, even though any key is launched, the record will nonetheless be included and can't be recovered.

6. Conditional authorization

This module is on the heart of the DSAS undertaking, imparting a sturdy, not unusual-sense, re-encryption machine to be had to intermediaries for efficient and relaxed faraway inspection and evaluate of PHRs. It lets in Alice (a primary care medical doctor) to offer Bob (a peerto-peer) with get entry to research and clinical programs thru the cloud server whilst preserving controls over the disclosure of data at the cloud server.

VI.SYSTEM METHODOLOGIES

Advance Encryption Algorithm (AES)

NIST recommends a new encryption trendy (Advanced Encryption Standard) to update DES. The simplest regarded assault in opposition to this gadget is a brute pressure assault, in which an attacker tries to break the encryption by means of testing all feasible characters. Block ciphers encompass DES and AES. Its key duration may be modified to 128, 192, or 256 bits; 256 is the default. Depending on the important thing size, it encodes a 128-bit facts block in 10, 12, and 14 rounds. Fast and handy AES encryption may be used on a diffusion of structures, particularly on small gadgets. AES has been broadly tested for plenty security applications

The fundamental benefits of AES over DES are:

1. The information block size is 128 bits.
2. Depending at the version, the important thing length is 128/192/256 bits.
3. Most CPUs now guide AES hardware, making them a good deal quicker.
4. It makes use of permutations and substitutions.
5. 2128, 2192, and 2256 feasible keys [10].
6. More comfy than DES.
7. The most broadly used symmetric encryption set of rules.

VIII.CONCLUSION AND FUTURE ENHANCEMENTS

The undetectable intermediate stealth re-encryption system we provide in this research can be utilized for data security and facilitates keyword search, eHealth venture, and alternating. Doctor Alice (delegate), Bob's doctor, can conditionally authorize our new system. Units the reencryption key (delegate). To improve the comfortable delegation capabilities, the cloud server can reverse the cipher using the re-encryption key. This allows Weave to acquire specific encrypted PHRs below Alice's public key. Without knowing anything about the underlying condition beforehand, the cloud server can scan the encrypted PHRs for the benefit of the physician. Specifically, inside the form, we attain intermediate invisibility. While the nonpublic key of the delegate (Alice) is still hidden, we acquire the opponent conspiracy assets within the shape that pardons the dishonest cloud server delegate (Sway). Through thorough validation and demonstration, we have tested protection to make sure the suggested DSAS scheme is both effective and environmentally friendly.

Proxy re-encryption holds notable promise for the future of relaxed eHealth monitoring because it protects affected person data via encrypting it and limiting get admission to to most effective authorized individuals. It secures IoT device data used for real-time monitoring whilst facilitating green and scalable information exchange among patients, healthcare carriers, and third parties. By controlling get entry to, it helps save you insider threats and facilitates you observe regulatory requirements, which include HIPAA. When used with blockchain, it helps relaxed, decentralized statistics management.

IX.REFERENCES

[1] T. Bhatia, A. K. Verma, and G. Sharma, ``Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing," Concurrency Comput., Pract. Exper., vol. 32, no. 5, p. e5520, Mar. 2020.

[2] T. Bhatia, A. K.Verma, and G. Sharma, ``Secure sharing of mobile personal healthcare records using certicateless proxy re-encryption in cloud," Trans. Emerg. Telecommun. Technol., vol. 29, no. 6, p. e3309, Jun. 2018.

[3] J. Feng, L. T. Yang, R. Zhang, W. Qiang, and J. Chen, ``Privacy preserving high-order bi-Lanczos in cloud-fog computing for industrial applications," IEEE Trans. Ind. Informat., early access, May 28, 2020, doi: 10.1109/TII.2020.2998086.

[4] H. Fang, X. Wang, and L. Hanzo, ``Learning-aided physical layer authentication as an intelligent process," IEEE Trans. Commun., vol. 67, no. 3, pp. 22602273, Mar. 2019.

[5] H. Fang, L. Xu, and X. Wang, ``Coordinated multiplerelays based physical-layer security improvement: A single-leader multiple-followers Stackelberg game scheme," IEEE Trans. Inf. Forensics Security, vol. 13, no. 1, pp. 197209, Jan. 2018.

[6] J. Feng, L. T.Yang, Q. Zhu, and K.-K.-R. Choo, ``Privacy-preserving tensor decomposition over encrypted data in a federated cloud environment," IEEE Trans. Dependable Secure Comput., vol. 17, no. 4, pp. 857868, Jul. 2020.

[7] J.-S. Fu, Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang, ``Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," IEEE Trans. Ind. Informat., vol. 14, no. 10, pp. 45194528, Oct. 2018.

[8] D. He, M. Ma, S. Zeadally, N.Kumar, and K. Liang, ``Certificateless public key authenticated encryption with keyword search for industrial Internet of Things," IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 36183627, Aug. 2018."

[9] Q. Huang, L. Wang, and Y. Yang, ``Secure and privacypreserving data sharing and collaboration in mobile healthcare social networks of smart cities," Secur. Commun. Netw., vol. 2017, pp. 112, Aug. 2017.

[10] Q. Huang, Y. Yang, and J. Fu, ``PRECISE: Identitybased private data sharing with conditional proxy reencryption in online social networks," Future Gener. Comput. Syst., vol. 86, pp. 15231533, Sep. 2018.

[11] M. Naz, F. A. Al-zahrani, R. Khalid, N. Javaid, A. M. Qamar, M. K. Afzal, and M. Shaq, ``A secure data sharing platform using blockchain and interplanetary le system," Sustainability, vol. 11, no. 24, p. 7054, 2019.

[12] J. Ning, Z. Cao, X. Dong, K. Liang, H. Ma, and L. Wei, ``Auditable time outsourced attribute-based encryption for access control in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 13, no. 1, pp. 94105, May 2018.

[13] J. Ning, Z. Cao, X. Dong, and L. Wei, ``White-box traceable CP-ABE for cloud storage service: How to catch people leaking their access credentials effectively," IEEE Trans. Dependable Secure Comput., vol. 15, no. 5, pp. 883897, Sep./Oct. 2018.

[14] S. Niu, L. Chen, J. Wang, and F. Yu, ``Electronic health record sharing scheme with searchable attributebased encryption on blockchain," IEEE Access, vol. 8, pp. 71957204, 2020.

[15] P. Xu, S. He, W. Wang, W. Susilo, and H. Jin, ``Lightweight searchable public-key encryption for cloudassisted wireless sensor networks," IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 37123723, Aug. 2018.