Implementation of Cloudlet-Based Medical Data Sharing Using NTRU Cryptosystem Method

Sourabh Sanjay Kate[1], Akshay Sunil Waghmare[2], Mayur Bapu Dange[3], Prof. Sachin D. Pandhare[4]
[1,2,3]*Student, SMSMPITR, Akluj, Maharashtra - 413118*
[4]*Professor, Dept. of Computer Science & Engineering, SMSMPITR Akluj, Maharashtra - 413118*

Abstract-This paper presents an innovative approach to securely share medical data using a cloudlet-based system. We propose the utilization of the NTRU cryptosystem method to ensure the secure transfer of data from mobile devices to cloudlets. By leveraging cloudlets for data transmission and employing NTRU encryption, we enhance the security of the data transfer process. Additionally, we introduce a trust model to enable selective information sharing among trusted partners. The framework we propose not only facilitates secure and personalized data sharing but also guarantees robust privacy protection for patient data stored remotely.

I. INTRODUCTION

Distributed computing revolutionizes venture IT delivery, offering cost-effective solutions and democratizing web processing. Healthcare, a vital industry, faces challenges in data security and privacy. Cloud platforms provide storage services, but encryption is crucial to safeguard data confidentiality and integrity. Economical searchable encryption techniques facilitate efficient data retrieval. Advanced distributed computing allows information to be stored across various clouds, enabling information sharing and intensive computations. However, ensuring the security of user data during transmission and storage in cloudlets and remote clouds remains a critical concern. This paper proposes a cloudlet-based healthcare framework to address these challenges and enhance the security of healthcare data in distributed cloud environments your paper.

II. LITERATURE SURVEY

The functions of the cloudlet encompass privacy protection, data sharing, and intrusion detection. In the data collection stage, user body data from wearable devices is encrypted using the NTRU method and sent to nearby cloudlets efficiently. A new trust model is introduced to enable users to select trustworthy partners for data sharing and communication. Medical data stored in remote cloud is divided into three parts for proper protection. Additionally, a collaborative intrusion detection system based on cloudlet mesh is designed to protect the healthcare system from malicious attacks.

Addressing the challenging issue of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE), the proposed solution establishes strict privacy requirements and utilizes the "coordinate matching" similarity measure for relevance assessment. Two improved MRSE schemes are presented to meet various privacy requirements in different threat models, ensuring both privacy and efficiency.

A practical solution for privacy-preserving medical record sharing for cloud computing is developed based on attribute classification. It includes vertical data partitioning, data combining, integrity checking, and hybrid search across plaintext and ciphertext. The system implements statistical analysis and cryptography to balance medical data utilization and privacy protection, enabling access to large- scale medical data while ensuring privacy.

III. FLOW CHART FOR SYSTEM

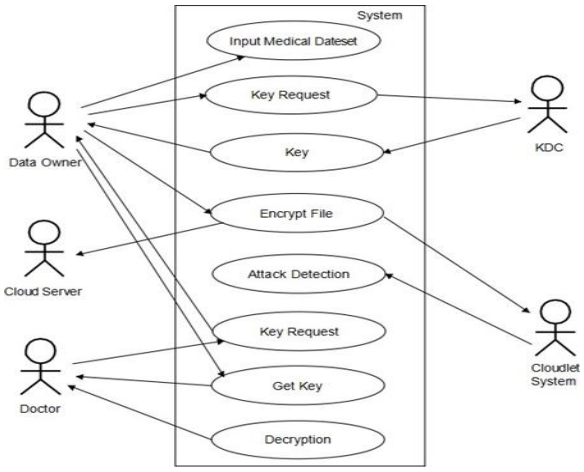

Fig -1: System Flow Chart

II.I. RELATED WORK

Fig -2: Login Page

The data provider login page serves as the gateway for new data providers to upload and encrypt data securely. Through this portal, authorized users gain access to upload their data, which is subsequently encrypted to prevent unauthorized access without the specific encryption key.

Fig -3: KDC Page

The Key Distribution Center generates unique public- private key pairs for specific email IDs of authorized doctors and securely distributes these keys to enable secure access to patient data without intrusion. This process ensures confidentiality, integrity, and authenticity in the healthcare data exchange environment

Fig -4 Medical Staff Login Page

The login page facilitates the key authority request process for medical staff, enabling them to securely receive cryptographic keys from the KDC for decrypting and accessing patient data. This ensures that sensitive medical information is accessed and handled only by authorized personnel, maintaining patient confidentiality and data security.

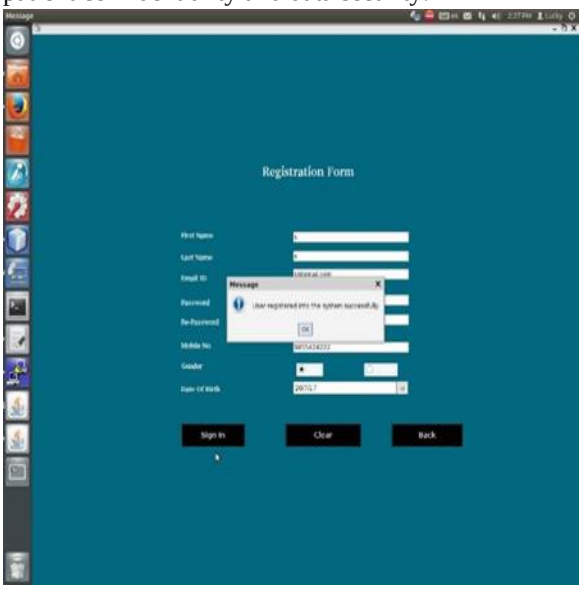

Fig -5: User Registration Form

The registration page allows data owners or doctors to register themselves in the system by providing necessary information. Upon successful registration, a confirmation message is displayed, and the user is ready to access the system using their credentials.

Fig -6: Browse File

The data upload window allows data owners to securely upload their data onto the cloudlet system, ensuring confidentiality, integrity, and access control over the uploaded data.

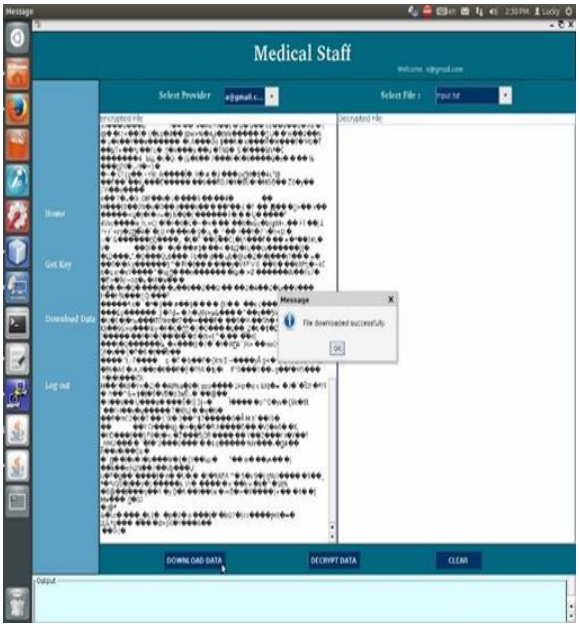

Fig -7: Download File

After receiving the keys from the KDC, authorized users can securely download and decrypt files using their private keys, ensuring confidentiality and integrity of the data throughout the process.

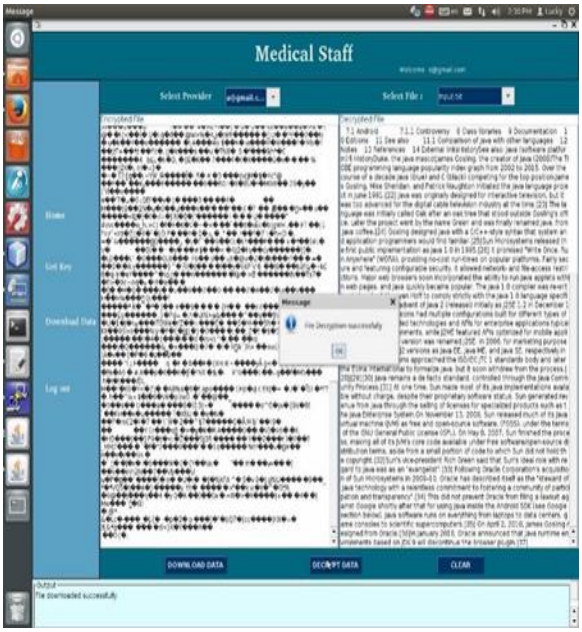

Fig -8: Decrypt File

Medical staff can select the provider and file to be decrypted, initiating the decryption and download processes securely through the system interface. This ensures efficient access to patient data while maintaining confidentiality and compliance with security protocols.

Fig -9: Attack Found

If an unauthorized user attempts to access the data, the system detects the unauthorized access attempt and displays an "attack found" message to alert system administrators or security personnel. This prompts immediate investigation and response to mitigate the attack and prevent further unauthorized access.

III. CONCLUSION AND FUTURE SCOPE

This proposed system is a secure cloudlet-based information sharing framework that operates on an encrypted data format. The Key Distribution Center (KDC) facilitates encryption by providing encryption algorithms to customers or data owners. When sharing data, if an attack occurs, the cloudlet system employs a collaborative intrusion detection system (IDS) technique to prevent it. The system's implementation demonstrates its enhanced security and reliability, while also saving time and memory resources.

REFERENCES

[1]. M. Quwaider and Y. Jararweh, “Cloudlet-based efficient data collection in wireless body area networks,” Simulation Modelling Practice andTheory, vol. 50,pp. 57–71, 2015./

[2]. R. Zhang and L. Liu, “Security models and requirements for healthcare application clouds,” in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on. IEEE, 2010, pp. 268–275.

[3]. K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, “Deypos: Deduplicatable dynamic proof of storage for multi-user environments,”2016.

[4]. N. Cao," Privacy-preserving multi-keyword ranked search over encrypted cloud data", INFOCOM, 2011 Proceedings IEEE, IEEE, (2011).

[5]. Min Chen, Yongfeng Qian, Jing Chen, Kai Hwang, Shiwen Mao, Long Hu, “Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing”, IEEE Transactions on Cloud Computing, 2016.

[6]. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy- preserving multi-keyword ranked search over encrypted cloud data,” Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.