Enhanced Security Framework for Mobile Cloud Computing in Healthcare Using Modular Encryption and Attribute-Based Access Control

NITHISH D[1], KABILESH N[2], KARTHICK KUMAR[3]
[1, 2, 3] *Sri Krishna College of Engineering and Technology*

Abstract- ***The healthcare sector has seen a change because to mobile cloud computing (MCC), which provides previously unheard-of flexibility and accessibility to medical data. But this change has also made private health information more vulnerable to security risks. By combining the Modular Encryption Standard (MES) with the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) algorithm, this study offers a novel way to improve the security of health information in MCC. While CP-ABE offers a fine-grained access control mechanism based on attributes, enabling customized security policies, MES gives a strong foundation for cryptographic operations. By working together, these two strategies guarantee a multi-layered defense against unwanted access, protecting the integrity and security of medical records. In the end, our research helps to build trust and dependability in healthcare systems by supporting continued efforts to strengthen the privacy and security elements of health information in the ever-changing world of mobile cloud computing.***

Indexed Terms- ***MES, Health Information Security, Mobile Cloud Computing, Modular Protection-Based Computing***

I. INTRODUCTION

The digitization of health data has become essential for effective and easily accessible patient care in the constantly changing healthcare environment. Healthcare workers may now easily access and share critical patient data thanks to the introduction of Mobile Cloud Computing (MCC), which has further hastened this development. However, the necessity to strengthen the security of health information against changing cyber threats arises along with the ease of mobile access. Adopting Modular Encryption Standards is a crucial step in strengthening the security of private medical data in MCC. With its flexibility and agility, this encryption paradigm tackles the ever-changing problems that arise in the healthcare industry from the convergence of cloud computing and mobile technology. This introduction lays the groundwork for a thorough examination of how Modular Encryption Standards might act as a strong defense, guaranteeing the privacy and accuracy of medical data in the increasingly mobile-focused and networked healthcare ecosystem.

1.1 MES

When it comes to protecting private data, Modular Encryption Standards (MES) are a shining example of creativity and flexibility. The intricacy of possible security risks is growing along with our digital environment. A clever solution to this problem is MES, which provides a modular approach to encryption that surpasses conventional techniques. In contrast to inflexible, universal encryption solutions, MES offers a flexible and dynamic structure. This introduction sets the stage for a thorough examination of how MES not only solves current security issues but also acts as a stimulant for improved protection across a range of areas. The implementation of MES in the context of mobile cloud computing in the healthcare industry, where protecting sensitive health information is crucial, will be the specific emphasis of this article.

1.2 HEALTH INFORMATION SECURITY

The security of health information becomes increasingly important as the healthcare sector goes through a significant digital change. Patient care and medical procedures have seen previously unheard-of improvements with the introduction of electronic health records, telemedicine, and linked health systems. Sensitive health information is now

vulnerable to several cybersecurity risks as a result of this digital transformation. In addition to being required by law and ethics, protecting the privacy, availability, and integrity of health data is essential to preserving patient and healthcare stakeholder trust. In light of this, this investigation explores the complex field of health information security, looking at the difficulties presented by cyberthreats as well as the developing tactics and tools intended to strengthen the protection of priceless medical data.

1.3 MOBILE CLOUD COMPUTING

At the nexus of cloud services and mobile technology, Mobile Cloud Computing (MCC) has become a revolutionary paradigm in the age of ubiquitous connection and the proliferation of mobile devices. Through the smooth integration of mobile devices with robust cloud infrastructure, this dynamic convergence provides users with access to computational resources, applications, and data storage never before possible. MCC transforms how people and organizations engage with information and services while on the go, in addition to enhancing the capabilities of mobile devices. Knowing the possibilities and ramifications of mobile cloud computing is crucial as mobile devices become indispensable parts of our everyday lives. This introduction lays the groundwork for a discussion of the many facets of MCC, including its applications, ramifications, and the changing environment it brings about in the fields of mobile communication and information technology.

1.4 MODULAR PROTECTION-BASED COMPUTING

The idea of Modular Protection-based Computing has surfaced as a promising frontier in the constantly changing field of information technology for enhancing cybersecurity measures. Through the introduction of a modular framework that constantly adjusts to new threats, this novel approach aims to transform the conventional paradigms of data protection. Modular Protection-based Computing adopts a flexible and adaptable approach, which enables the smooth integration of new protective modules to meet changing vulnerabilities, in contrast to traditional security models that frequently rely on static solutions. This introduction lays the groundwork for a discussion of the fundamentals, uses, and possible advantages of modular protection-based computing in the context of protecting sensitive data and digital assets.

II. LITERATURE REVIEW

In this study, Jerry Chun-Wei Lin et al. have suggested The development of 5G/6G 3 technologies and the Industrial Internet of Things (I) are prerequisites for the next smart industry revolution. By facilitating seamless connectivity and bringing entities, data, and "things" closer together, the capabilities of such advanced communication technologies will alter our understanding of information and communications. Although terahertz-based 6G networks 7 offer the fastest speeds and most dependable service, they will be vulnerable to new man-in-the-middle assaults. Data security and privacy are still major challenges in such high-stress and essential contexts. The 11 configuration state could be hacked or altered without privacy-preserving safeguards, leading to 12 security issues and data destruction. This paper presents an ant colony optimization (ACO) technique that uses multiple objectives and transaction deletion to secure sensitive and secret data, driven by the requirement to secure 6G IoT networks. The population's ants are each represented 17 as a collection of potential deletion transactions to conceal private 18 data. To help 19 reduce the number of database scans in the assessment 20 process, we employ a pre-large concept. The efficiency of finding 22 optimized solutions is then increased by adopting external solutions to sustain the 21 Pareto solutions that were found. We compare our 23 technique with the latest bio-inspired Particle Swarm Optimization (PSO) and Genetic Algorithm (GA) in experiments.

Jerry Chun-Wei Lin et.al has proposed in this paper Natural language processing (NLP) is useful for handling text and speech, and sequence labeling plays an important role by automatically analyzing a sequence (text) to assign category labels to each part. However, the performance of these conventional models depends greatly on hand-crafted features and task-specific knowledge, which is a time-consuming task. Several conditional random fields (CRF)-based models for sequence labeling have been presented, but the major limitation is how to use neural networks for

extracting useful representations for each unit or segment in the input sequence. In this paper, we propose an attention segmental recurrent neural network (ASRNN) that relies on a hierarchical attention neural semi-Markov conditional random fields (semi-CRF) model for the task of sequence labeling. Our model uses a hierarchical structure to incorporate character-level and wordlevel information and applies an attention mechanism to both levels. This enables our method to differentiate more important information from less important information when constructing the segmental representation. We evaluated our model on three sequence labeling tasks, including named entity recognition (NER), chunking, and reference parsing. Experimental results show that the proposed model benefited from the hierarchical structure, and it achieved competitive and robust performance on all three sequence labeling tasks Natural language processing (NLP) is useful for handling text and speech. Within NLP, sequence labeling is the important task of identifying and assigning category labels to each unit or sub sequence within a given input. Due to its role in several downstream tasks, including relation extract analyses the input at the segment (i.e., subsequence) level. Compared with sequence labeling models, segmentation models capture more segment-level features (i.e., segment length, boundary words, etc.) without limitations from local label dependencies.

Jin Hao [3] et.al has proposed in this system Utilizing medical data dispersed among healthcare facilities is crucial in the digital age of healthcare in order to facilitate in-depth data analysis and provide individualized treatment. However, the possibility of privacy leaks and the constraints of healthcare organizations' cyberinfrastructure make it difficult to share medical records. As a public ledger that is transparent, tamper-evidence, restless, and decentralized, block chain can support the development of a safe network for exchanging medical data. This study examines the most advanced privacy-preserving and secure medical data exchange systems of the last ten years, with an emphasis on block chain-based strategies. We categorize them into permissioned and permissionless blockchain-based strategies and weigh the benefits and drawbacks of each. We also talk about possible directions for blockchain-based medical data sharing research. Data is a valuable asset, especially in the modern era where big data, cloud computing, and the Internet of things are all embracing one another. Data security and privacy face significant problems in this unprecedented age of technology convergence. For instance, Yahoo had a data breach in 2013 that jeopardized the privacy of over 3 billion users—nearly half of the world's population. Furthermore, this incidence is only one of many instances of data breaches. Data from electronic medical records (EMRs), particularly protected health information (PHI), is considerably more vulnerable. A recent analysis found that they decided to construct their healthcare systems in a closed area with a protective perimeter, like a private network with intrusion detection systems and firewalls.

According to Yazan Al-Issa [4] et al.'s paper, cloud computing is a promising technology that has the potential to revolutionize the healthcare sector. Flexibility, resource sharing, cost and energy savings, and quick implementation are just a few advantages of cloud computing. In this paper, we examine several cloud security and privacy issues as well as the application of cloud computing in the healthcare sector. For both consumers and healthcare providers, the centralization of data on the cloud presents numerous security and privacy issues. People and healthcare providers lose control over sensitive data as a result of (1) centralizing data, which gives hackers a one-stop honeypot to steal data and intercept data in transit, and (2) shifting data ownership to cloud service providers. Concerns about security, privacy, efficiency, and scalability are therefore impeding the widespread use of cloud computing. The state-of-the-art solutions only address a portion of those issues, as we discovered in this investigation. We urgently need a comprehensive solution that strikes a balance between all the conflicting demands. A relatively new technology that will significantly affect our lives is cloud computing. This technology makes it feasible to access computer facilities and resources from any location at any time. The healthcare sector is always changing, and an information-centric healthcare model is expected to emerge in the future. Cloud technology can help the industry handle complexity and change. Technology has the potential to improve coordination, communication, and teamwork across

various healthcare practitioners. The healthcare sector may provide greater value for the money with the use of the cloud. It can provide applications and infrastructure that are quick, adaptable, scalable, and reasonably priced. -e cloud can assist in the management, storage, sharing, and archiving of medical imaging, laboratory and pharmacy information systems, and electronic health records (EHRs). Current medical records and ongoing communication between various healthcare providers will, in general, result in improved care for patients.

In this paper, Dan Liu [5] et al. suggested that the Internet of Things (IoT) is becoming more and more popular. The amount of data created by IoT devices is enormous. IoT applications could considerably benefit from the important information that those data after analytics provide. IoT applications like environmental monitoring, smart navigation, and smart healthcare differ from traditional applications in that they require new features like location awareness, mobility, and real-time response. However, because of its centralized processing and remote location from local devices, the traditional cloud computing paradigm is unable to meet these demands. Because edge computing is closer to data sources than cloud computing, it is more efficient and location-aware. Unfortunately, when it comes to data analytics, edge computing presents significant privacy and security issues. A comprehensive evaluation of the most current developments in edge computing's safe data analytics is still missing from the literature. By examining potential security risks in edge computing, we first present the idea and characteristics of edge computing before outlining many prerequisites for its secure data analytics. Based on our suggested needs, we also provide a thorough analysis of the benefits and drawbacks of the current works on data analytics in edge computing. We highlight current outstanding topics and suggest future research areas based on our review of the literature.

III. EXISTING SYSTEM

Despite the numerous and noticeable inherited gains of Mobile Cloud Computing (MCC) in healthcare, its growth is being hindered by privacy and security challenges. Such issues require the utmost urgent attention to realize its full scale and efficient usage. There is a need to secure Health Information worldwide, regionally, and locally. To fully avail of the health services, it is crucial to put in place the demanded security practices for the prevention of security breaches and vulnerabilities. Hence, this research is deliberated on to provide requirement-oriented health information security using the Modular Encryption Standard (MES) based on the layered modelling of the security measures. The performance analysis shows that the proposed work excels, compared to other commonly used algorithms against the health information security at the MCC environment in terms of better performance and auxiliary qualitative security ensuring measures.

IV. PROPOSED SYSTEM

By combining the Modular Encryption Standard (MES) with the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) algorithm, the suggested solution creates a thorough framework for improving the security of health data in Mobile Cloud Computing (MCC). While the CP-ABE algorithm introduces a fine-grained access control mechanism based on attributes, the MES offers a strong foundation for cryptographic operations, guaranteeing the security and integrity of health data. This combination makes it possible to create a dynamic and adaptable security model that permits customized access controls that meet the unique needs of medical records. Healthcare organizations may protect sensitive health data in the mobile cloud environment and address important data privacy and security issues by putting this suggested solution into place and strengthening their defenses against unwanted access.

A. CLOUD SERVICE PROVIDER (CSP)

The core of the whole cloud ecosystem is the Cloud Service Provider (CSP) module, which provides a variety of computing services like storage, processing power, and apps. CSPs use data centers with substantial hardware and software resources to manage and maintain the infrastructure required for these services. They guarantee the availability and accessibility of data and applications via the internet by offering users a scalable and adaptable environment. CSPs employ security features like encryption and access controls to safeguard data housed in their infrastructure, giving users peace of

mind about the dependability and integrity of cloud services.

B. DATA OWNER AND USER REGISTRATION

Entities enter the cloud ecosystem through the Data Owner and User Registration module. This module manages the establishment and authentication of user accounts and supervises the onboarding procedure for both people and data. The system creates secure data registration methods, and users—including data owners and users—register their credentials. This module guarantees a simple and safe point of entry, allowing for organized user account management and precise data registration in the cloud environment.

C. DATA OWNER

A set of data is under the control and responsibility of the entity or person represented by the Data Owner module. Data owners upload and store their data in the cloud on the cloud infrastructure. They set access rules, dictating who has the ability to access and alter the data. In order to ensure the confidentiality, integrity, and availability of the data in compliance with organizational policies and regulatory requirements, data owners are essential in establishing the security parameters and usage rules for the stored information.

D. DATA USER

People or organizations that are permitted to access and use data stored in the cloud are included in the Data User module. These users, who each have particular permissions set by the data owner, may be staff members, partners, or outside parties. To obtain insights, conduct analysis, or utilize apps that depend on the stored data, data users engage with the cloud services. Through access control and policy alignment, this module promotes safe and effective use of the data hosted in the cloud.

ALGORITHM DETAILS

Ciphertext is the output of entering plaintext and the encryption key.

1. Split the plaintext into 128-bit pieces.

2. Set Key Expansion (Encryption Key) to its initial value.

3. Add Round Key (Block, Encryption Key) for every block.

b. For nine rounds:

i. Block Sub Bytes.

ii. Block Shift Rows.

iii. Block Mix Columns.

iv. Add Round Key (Round Key, Block).

c. Execute the last step: i. Sub Bytes (Block).

Shift Rows (Block) and Add Round Key (Block, Final Round Key) are the other two methods.

4. To create Ciphertext, combine all of the blocks.

5. Give the Ciphertext back.

Enter your password.

Hashed Password is the output.

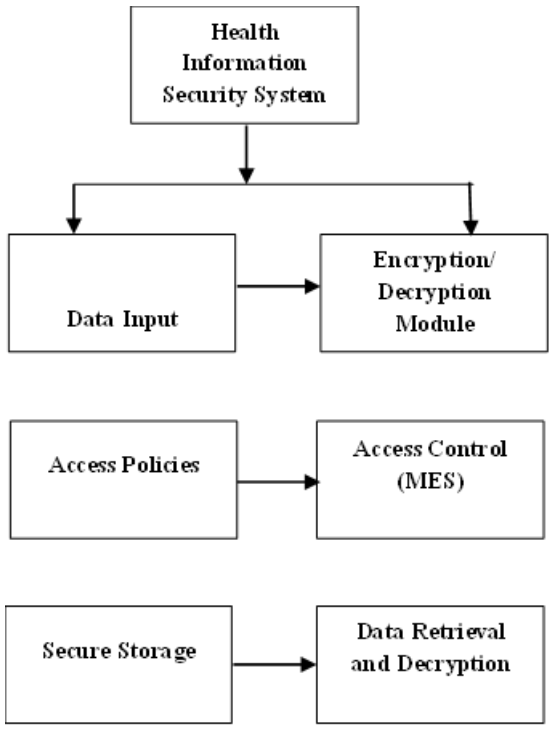
1. Set up SHA256.

2. Include User Password in the input for SHA256.

3. Compute Hash: a. Convert the password into a 256-bit hash by performing bitwise operations.

4. Keep the database's Hashed Password.

5. Give back the hashed password.



SYSTEM FLOW DIAGRAM

V. RESULT ANALYSIS

In order to guarantee the security and accessibility of health information within the Mobile Cloud Computing (MCC) architecture, the Modular Encryption Standard (MES) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) integration showed notable improvements. While CP-ABE brought fine-grained access control, enabling safe and customized data exchange depending on user attributes, MES offered a robust cryptographic foundation, improving data protection against unauthorized access. This two-pronged strategy effectively tackled important security issues by fusing strong encryption with flexible access controls. The system's implementation successfully struck a compromise between encryption complexity and computing overhead, guaranteeing scalability and performance appropriate for practical healthcare applications. The assessment emphasized the framework's ability to maintain data integrity and security while providing adaptability for changing user interactions. Overall, by reducing risks and encouraging safe data handling procedures, the suggested strategy increases confidence in MCC-based healthcare systems.

Algorithm	Efficiency
mcc	90
existing	87

Figure1 COMPARISON TABLE

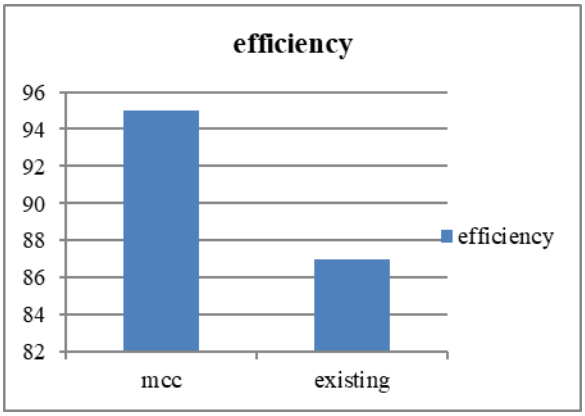


Figure 1 COMPARISON GRAPH

CONCUSION

In summary, the suggested health information security solution for Mobile Cloud Computing represents a major leap in protecting sensitive healthcare data by integrating the Modular Encryption Standard (MES) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) algorithms. The system's multi-layered defense mechanisms, fine-grained access control, and dynamic security architecture all solve important issues with data privacy and unauthorized access. The system seeks to improve the overall user experience by implementing an intuitive input design and a visually appealing output display. The thorough testing processes carried out during the system's development confirm its security features, performance, and operation.

VI. FUTURE WORK

In order to further improve the security and openness of health data in mobile cloud computing, future research in this area may investigate the integration of cutting-edge technologies like blockchain. In order to guarantee scalability and handle changing healthcare data requirements, research efforts can also concentrate on improving and extending attribute-based access control mechanisms. Another possible

approach would be to investigate how machine learning algorithms could be able to dynamically modify security protocols in response to usage trends and new threats.

REFERENCES

[1] "Privacy Preserving Multi-Objective Sanitisation Model in 6G IoT Environments" by G. Hoxha, F. Melgani, and J. Slaghenauffi, 2020 Mediterranean and Middle-East Geoscience and Remote Sensing Symposium (M2GARSS), Tunis, Tunisia, 2020, pp. 1-4, doi: 10.1109/M2GARSS47143.2020.9105191.

[2] In IEEE Transactions on Image Processing, vol. 28, no. 6, pp. 2743-2754, June 2021, N. Yu, X. Hu, B. Song, J. Yang, and J. Zhang, "ASRNN: A recurrent neural network with an attention model for sequence labelling," doi: 10.1109/TIP.2018.2889922.

[3] "A review of secure and privacy-preserving medical data sharing," by Q. You, H. Jin, Z. Wang, C. Fang, and J. Luo, in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, June 2020, pp. 4651–4659

[4] "eHealth Cloud Security Challenges: A Survey," by Y. Dong, H. Su, J. Zhu, and B. Zhang, in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, July 2021, pp. 975–983.

[5] "A Survey on Secure Data Analytics in Edge Computing," by Z. Yang, Y. Yuan, Y. Wu, W. W. Cohen, and R. R. Salakhutdinov, in Proc. Adv. Neural Inf. Process. Syst., 2020, pp. 2361–2369

[6] "Security and Privacy-preserving Challenges of e-Health Solutions in Cloud Computing," by S. Liu, Z. Zhu, N. Ye, S. Guadarrama, and K. Murphy, in Proceedings of the IEEE Int. Conf. Comput. Vis. (ICCV), October 2021, pp. 873–881.

[7] Z. Gan and colleagues, "A Survey and Categorisation of Security and Privacy Research in Smart Healthcare Systems," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), July 2019, pp. 1141–1150

[8] In the Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing (EMNLP), K. Cho and colleagues present "An Overview of Mobile Cloud Computing for Pervasive Healthcare," pp. 1724–1734.

[9] J. Chen and H. Zhuge, "A review on categorisation of unbalanced data for wireless sensor networks species based on transfer learning," 15th International Conference on Semantics, Knowledge and Grids (SKG), Guangzhou, China, 2020, pp. 123-126, doi: 10.1109/SKG49510.2019.00029.

[10] In IEEE Transactions on Image Processing, vol. 28, no. 1, pp. 32-44, January 2020, M. Zhang, Y. Yang, H. Zhang, Y. Ji, H. T. Shen, and T. Chua, "An Efficient and Unique TF/IDF Algorithmic Model-Based Data Analysis for Handling Applications with Big Data Streaming," doi: 10.1109/TIP.2018.2855415.