**Educational Administration: Theory and Practice**
2024, 30(5), 13341-13349
ISSN: 2148-2403
https://kuey.net/

**Research Article**

# A Secure Framework For Enhancing Data Privacy And Access Control In Healthcare Cloud Management Systems

Taduri Suneetha[1*], Dr Jai Bhagwan[2]

[1*]Research Scholar, Dept of Computer Science, Monad University, Hapur (India), suneetha@mallareddyuniversity.ac.in
[2]Professor, Dept of Computer Science, Monad University, Hapur (India), shaikarchi@gmail.com

**Citation:** Taduri Suneetha, Dr Jai Bhagwan, (2024), A Secure Framework For Enhancing Data Privacy And Access Control In Healthcare Cloud Management Systems, *Educational Administration: Theory and Practice*, *30*(5), 13341-13349
Doi: 10.53555/kuey.v30i5.5783

**ARTICLEINFO**

**ABSTRACT**

Cloud computing offers a pay-as-you-go model, widely utilized for its cloud storage services by both individuals and businesses to manage data efficiently. Despite its popularity, ensuring data security and privacy remains a significant challenge. This Research paper presents new solutions to enhance cloud computing security. The primary goal is to create a secure cloud environment, benefiting both users and service providers by ensuring safe data processing and delivery. Sectors like business, banking, military, and healthcare are cautious about adopting cloud storage due to security concerns. This research aims to address these concerns and attract more users by providing secure cloud solutions. The first approach introduces the Scalable and Enhanced Key Aggregate Cryptosystem (SEKAC), enhancing healthcare data security through double encryption. This method ensures confidentiality and integrity by securely storing and retrieving medical data, outperforming previous techniques. The second approach employs the Improved Diffie-Hellman Key Exchange Algorithm, which secures data transmission from cloud servers to users. This method enhances security by generating secure keys and facilitates safe key sharing through attribute-based encryption. The third strategy focuses on secure data exchange using advanced data splitting and clustering techniques. The Clustering and Partitioned-based Secured Data Transmission Method, combined with the Enhanced Krill Herd Algorithm and hybrid Elliptic Cryptographic technique, improves data security and efficiency. Overall, this research introduces innovative methods to bolster cloud security, particularly for healthcare, ensuring secure data storage, retrieval, and transmission.

**Keywords-**Cloud Computing Security, Data Privacy, Scalable and Enhanced Key Aggregate Cryptosystem (SEKAC), Diffie-Hellman Key Exchange Algorithm, Data Encryption, Secure Data Transmission

## 1. INTRODUCTION

Medical Informatics, or Health Informatics, focuses on managing health information using various techniques and tools. E-health, a subset of this field, involves electronically storing and providing health services to patients. The healthcare sector increasingly embraces IT, and Hospital Information Systems (HIS) have grown significantly in the past decade (1). HIS functions rely on diverse subsystems from different manufacturers, each with unique specifications and protocols (2). Electronic Health Records (HER), a product of HIS, organize treatment data from various healthcare providers over time. Accessible data enhances healthcare quality and efficiency, but EHRs often need to be segmented based on user needs (3). Despite the benefits, healthcare has been slow to adopt IT solutions, with many physicians still using paper records, leading to inefficiencies and limiting timely, high-quality care (4). Interoperability between HER systems is crucial for efficient workflows and data exchange, but challenges include varying operating systems, programming languages, and hardware (5). Legal, security, and privacy concerns also complicate seamless data transfer. Safeguarding medical data and ensuring patient privacy are paramount, requiring access control, encryption, and measures against unauthorized access (6). Cloud Computing Technology can enhance health services by enabling universal data access and sharing among patients, physicians, and

insurers. However, security concerns about data storage and transmission remain a challenge. Addressing these concerns involves authentication, integrity, and confidentiality measures, ensuring a secure environment for healthcare data (7).

**MAJOR SECURITY ASPECTS TO HER SHARING:** The proliferation of medical data poses significant risks to patient privacy and data security, requiring effective measures to prevent unauthorized access (8). Secure sharing of electronic health records (HER) by health professionals involves addressing key principles: interoperability, privacy, integrity, and accessibility. Interoperability faces challenges from differing languages, protocols, and standards, impacting HER exchange (9). Ensuring universally compatible HER formats is essential. Privacy demands that EHRs are accessed only by authorized individuals, with risks from sharing methods like CDs, portals, and emails (10). Integrity requires accurate and reliable data, but can be compromised by documentation errors and technical issues (11). Accessibility concerns arise as health professionals need patient records across various locations. Adhering to HIPAA regulations is crucial for maintaining privacy, security, and standards for patient information, ensuring patient consent for HER sharing (12).

**HEALTHCARE MONITORING SYSTEM;** Electronic Health Records (EHRs) transform physical patient records into digital format, enhancing documentation, cost-effectiveness, efficiency, data access, and safety (13). Healthcare systems gather various reports, including administrative, clinical, and patient data, from multiple sources. A Healthcare Monitoring System connects physicians, patients, staff, and ambulance services, ensuring real-time health status updates and emergency responses (14).

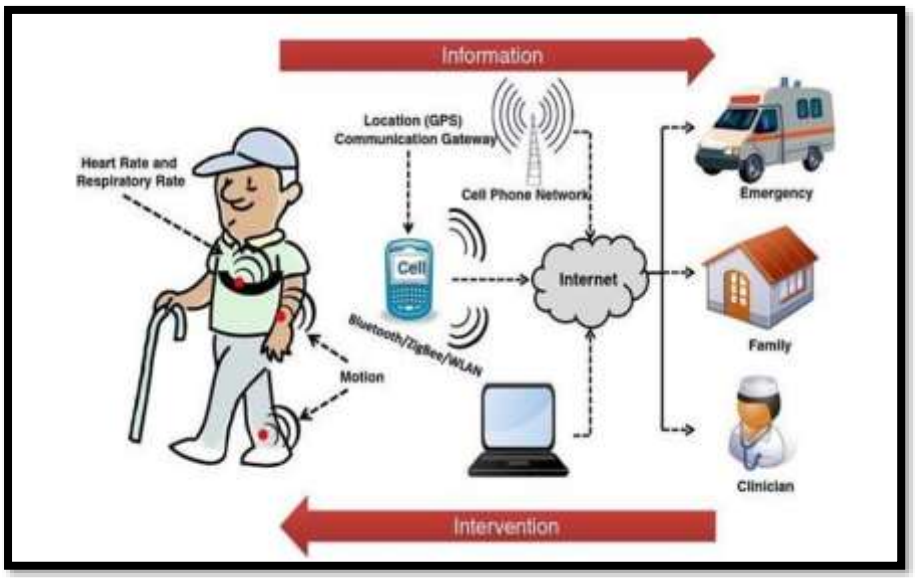


**FIGURE 1 HEALTHCARE MONITORING SYSTEM**

CLOUD STORAGE SERVICES: Cloud storage services offer public, private, or hybrid models, each with unique considerations like investment, data volume, and security (15, 16). Users must weigh factors such as performance, access patterns, and location to choose the best model (17). Public clouds provide shared servers managed by service providers, while private clouds offer dedicated infrastructure (18). Storage providers offer various pricing models, including fixed fees and metered usage, to accommodate different needs (19). The pay-per-use model allows flexible resource allocation, ensuring scalability to meet changing demands (20). Overall, cloud storage services continue to evolve, offering expanded options and flexibility for users (21).

Security Issues in Cloud Storage: Cloud computing integrates informatics to enhance productivity and information management (16). However, concerns about security and compliance hinder its adoption (15). Protecting private data and ensuring legal compliance are crucial (22). Users must ensure security, confidentiality, and accessibility in third-party data storage services (23). Virtualization is a key security tactic, protecting against user attacks. However, not all resources are virtualized flawlessly (20). Pioneering Internet services must prevent security breaches (21). Users depend on contracts and legal measures to safeguard against provider misconduct (22). Overall, managing security features like authenticity, privacy, and access control is vital for reliable cloud storage services (23).

SECURE DATA SHARING IN CLOUD COMPUTING: Secure data sharing in cloud computing faces significant security and privacy risks (23). Users are wary due to vulnerabilities in critical business and IT systems (19). Cloud providers' access to stored data poses threats of theft and resale to third parties (22). Safe data sharing entails identifying authorized individuals, granting access without owner intervention, and encrypting data to thwart unauthorized access (24). However, user revocation poses computational

challenges, burdening data owners (23). Implementing this solution at scale, especially for critical data, presents logistical hurdles (20). Addressing these complexities is crucial for realizing secure data sharing in cloud computing (15).

Creating a patient-centric online healthcare system connecting hospitals, clinics, doctors, insurers, pharmacies, and labs demands meticulous planning (19). Automated health services and electronic record management are increasingly adopted, requiring significant investment and training (18). Future needs center on seamless access to health records anytime, anywhere (17). Integrating diverse formats and platforms into a unified framework precedes ensuring secure data availability across networks (16). Challenges include integrating disparate data sources, ensuring data availability while upholding security, and implementing robust measures to safeguard Electronic Health Records (HER) (20). Prompt and cautious action is crucial to prevent inappropriate disclosure of sensitive health data in a shareable, interoperable environment (21).

The pay-per-use model in cloud computing tailors services to users' needs, notably in cloud storage (18). Security concerns prompt research into secure data handling, crucial for protecting private information (22). Cloud's popularity among medical researchers necessitates secure data storage for accurate analysis and predictions (15). However, current methods face challenges like increased processing overhead and content manipulation risks (20). Objectives include implementing robust encryption methods, enhancing data sharing, and ensuring secure storage access (24). Innovations like SEKAC, IDHKE, CPSDTM, and Honey-Encryption aim to bolster security and optimize cloud resources, promising efficient, secure data exchange with fine-grained access control in public clouds (23).

## 2. LITERATURE REVIEW

Choudhury et al. (2011) propose an innovative user authentication model for cloud settings, replacing traditional methods with a robust approach. Users authenticate by inserting a smart card, entering their credentials, and receiving a one-time key on their mobile device. This method ensures mutual authentication, identity management, and session key agreement. Cloud computing's dispersed nature raises security concerns, but strong authentication prevents unauthorized access. Users can change passwords at will, ensuring flexibility. Security analysis confirms the effectiveness of this approach, offering a solid foundation for cloud security.

A secure fine-grained access control technique called outsourced attribute-based access control has been presented by Li et al. (2013). It makes use of two organizations: Key Generation Cloud Service Provider (KGCSP) and Decryption Cloud Service Provider (DCSP). The key delivery by authority attribute is outsourced to the KGCSP entity. Fractional decoding of encrypted messages is handled by the DCSP. In doing so, effective key decryption and nose epage of confidential data are achieved.

Tang et al. (2013) presented collaborative access control properties. Agility, homogeneity, centralized facilities, and outsourcing trust are among them. A multitenancy authorization formal system was used with an Authorization as a Service (AaaS) approach. The technique even aids in fine-grained trust replicas managerial control. A straightforward solution that contributes to cloud trust is the cryptographic role in integrating trust based on access control.

According to Ayad et al. (2014), a cloud-based storage system that facilitates the outsourcing of dynamic data is envisaged, in which the owner will have the ability to access and archive the data kept by the cloud service provider. Their program enables authorized users to ensure that users are receiving the most recent version of the outsourced data.

According to Jianghong Wei et al. (2018), a multi-authority CPABE scheme can be built with the following features: (1) each attribute authority can independently issue secret keys for users, negating the need for a fully trusted central authority; (2) each attribute authority can dynamically remove any user from its domain, preventing that user from accessing data that has been outsourced in the future; Finally, the updating of secret keys and ciphertext is carried out in a public manner. Third-party cloud servers have the ability to update the encrypted data from the current time period to the next one so that the revoked users cannot access the previously available data.

For data communication, Shashi Mehrotra Seth and Rajan Mishra (2019) employed a comparative technical examination of encryption techniques. In order to evaluate the encryption algorithm, this article examined its performance in terms of calculation time, memory utilization, and output bytes. Abdul Elminaam et al. (2020) offer the overall performance of symmetrical encryption algorithms such AES, DES and 3DES, RC2, Blowfish, and RC6. A comparison of various algorithm parameters, including data block sizes, data kinds, electric battery usage, distinct key sizes, and encryption/decryption speeds, has been conducted for these encryption methods.

Using open-source technologies like Kubernates and Jupyterhub, which tend to be suitably upgraded as cloud computing security, a novel architecture is proposed (C. Chu et al. 2016). According to Kuo-Hsuan et al. (2017), a computationally comprehensive hybrid-based health care system framework based on attribute encryption is suggested for scalable, cost-effective patient access to personal records, health information, and medical records. The Picture Archiving and Communication System (PACS) uses a general convolutional neural network (CNN) to validate data in order to improve patient report information that was previously

kept on a different database server in order to determine similarities. By studying the characteristics of past experiences, intelligent agents may categorize patient photos and build a platform for data analysis that paves the way for intelligent health care solutions. To securely communicate data with other institutions in an effective manner, it is possible to generate the loaded data using multiple internal servers (Dixit et al. 2018).
Zhenfei Zhang et al. (2020) recommend reaction attacks against full homomorphic approaches for safeguarding outsourced computation. We can store the associated secret key of the system by using this attack, which is mostly based on the user's response to the output given by the cloud. Although homomorphic encryption algorithms appear to be a promising option, there are certain drawbacks when utilizing them in cloud computing. Here, a good message attack is employed in opposition to all completely homomorphic encryption schemes. During this assault, a malevolent cloud can obtain the messages by examining the user's answer. One of this strategy's main benefits is that it can retrieve the message from a malicious cloud utilizing a completely homomorphic system that explains dependability under outsourced computation conditions. The disadvantages of cloud computing include that it comes with certain issues, is quite expensive, and does not provide enough for the user.
Since it is widely supported and simple to integrate with a variety of apps on multiple platforms, the Public Key Infrastructure is used in the majority of grid-based implementations (Lim K et al. 2016). Identity-Based Encryption functions as a public key encryption method where a public key is substituted for an arbitrary string, like an email address or phone number. A master secret's power is typically embodied in the private key produced by a private key generator (Vijayakumar P et al. 2016). Through this interference, messages can be encrypted and signatures verified by everyone, even after public features and public key "strings" have been distributed without prior key distribution.
Due to the convergence of wireless and forthcoming mobile technologies, which is an emerging communication key on mobile-multicast keys management, multi-group-based services can coexist on a single network for proliferation (M. G. Gouda et al. 2018). Group Key Management (GKM) keys can be inefficient in multicast group setups because they require overhead rekeying in order to improve. With an established GKM, secure group communication may be made by merely coughing on a single group service (X. Zou et al. 2016). When servicing a multiple group network via a homogeneous or heterogeneous network, overhead arises from low rekey transmission. A wireless network can accommodate both one and more movement members if it joins a group network. The slot based multiple GKM strategy for a multiple multicast group was proposed in this research (T. T. Mapoka et al. 2015). This work discusses the different types of key management problems for multicast communication sessions (Z. Zhou et al. 2017).

## 3. SCALABLE AND ENHANCED KEYAGGREGATECRYPTOSYSTEM FOR CIHMS

This section elucidates the proposed systems architecture catering to healthcare organizations' data management via WBAN. SEKAC offers scalability and vast data storage from sensor inputs, crucial for secure communication in healthcare. An intelligent health monitoring system is pivotal for cloud security, depicted in the architecture diagram featuring cloud storage, patients, healthcare organizations, and the Healthcare Insurance Authority. Patient data, acquired through WBAN, undergoes double encryption, augmented by ciphertext id, enhancing security. Double encryption thwarts traceability, with semi-functional and regular keys used for encryption. Decryption, facilitated by semi-functional and aggregated keys, enables healthcare organizations to provide prescriptions securely, encrypted similarly for patients' receipt.

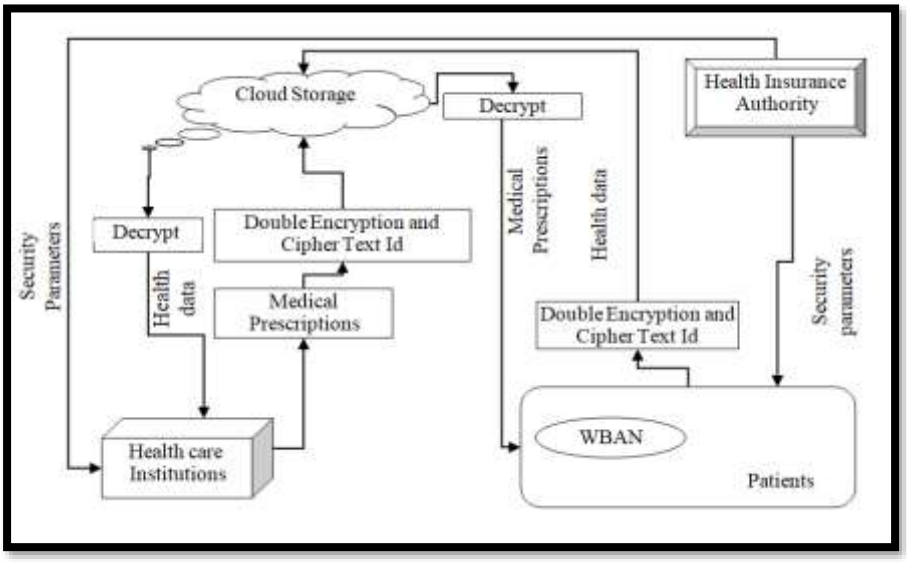


**FIGURE 2. IMPROVED CLOUD BASED INTELLIGENT HEALTH CARE MONITORING**

### 3.1. ALGORITHM FOR SEKAC IN CIHMS

1. Information from WBAN about the patient is given as input
2. Pi sends data to S
3. The host sends data to the ECC
4. The number of Ciphertext classes is set.
5. A certain number of ciphertext classes are sent to Pi by S.
6. From HIA, Pi gets MS, SK, and NK.
7. HD has been protected by Pi
8. The symbol HD stands for Encrypt 1 (NK, HD).
9. SC_HD is the same as Encrypt 2(SK, her, N□ - Hdi).
10. Extract (KS) is the same as
11. The data is protected and kept in the cloud.
12. Health care institutions decrypt data
13. HD is the same as Decrypt(S▬·_HD, her, KS, AK)
14. Health care institutions decrypt data and write down orders.
15. N✦_MP is the same as Encrypt 1 (NK, MP).
16. S✦_MP is the same as Encrypt 2(SK, her, N✦_MP).
17. Extract (KS) is the same as
18. Health care institutions encrypt data, and that data is kept in the cloud.
19. DataPiis was decrypted.
20. MP is the same as Decrypt(S✦_MP, her, KS, AK)
21. Pi gets orders for medicines

SEKAC algorithm in CIHMS employs WBAN for patient health data collection, encrypted and stored in the cloud. Dual encryption with ciphertext classes enhances security. Combining ciphertext IDs yields aggregate keys, sent to healthcare groups for data access via email. Decryption with combined keys enables access to medical prescriptions securely stored in the cloud for patients.

## 4. RESULTS and Discussion

This study compares experimental data from proposed and existing methodologies for cloud storage security. The BDSVCS technique uses class identification and public key encryption. The authors developed a privacy-preserving auditing framework with efficient, secure dynamic data operations. Enhancements include bidirectional authentication, statistical analysis, and improved load distribution, reducing client computational burden. An error response method was also introduced, demonstrating proficient error handling with lower overhead costs. The paper proposes Scalable and SEKAC methods for securing healthcare information, comparing their performance in terms of resource utilization, user satisfaction, integrity, and confidentiality.

**4.1. Confidentiality Comparison:** Confidentiality pertains to safeguarding information against unauthorized access. Put simply, only individuals with proper authorization can obtain entry to confidential information. Confidentiality is quantified by the percentage of unauthorized users who are able to access the data.

**TABLE 1 CONFIDENTIALITY COMPARISON VALUES**

| **Confidentiality (%)** | | | |
|---|---|---|---|
| **Delegation ratio (%)** | **KAC** | **BDSVCS** | **SEKAC** |
| 0.1 | 15.1 | 25.2 | 27 |
| 0.2 | 25 | 38 | 41 |
| 0.3 | 32 | 44 | 46.8 |
| 0.4 | 45 | 58 | 62.5 |
| 0.5 | 50 | 69 | 72 |
| 0.6 | 62 | 78 | 79.8 |
| 0.7 | 75 | 80 | 83.4 |
| 0.8 | 84 | 87 | 89.6 |
| 0.9 | 88 | 96 | 98 |

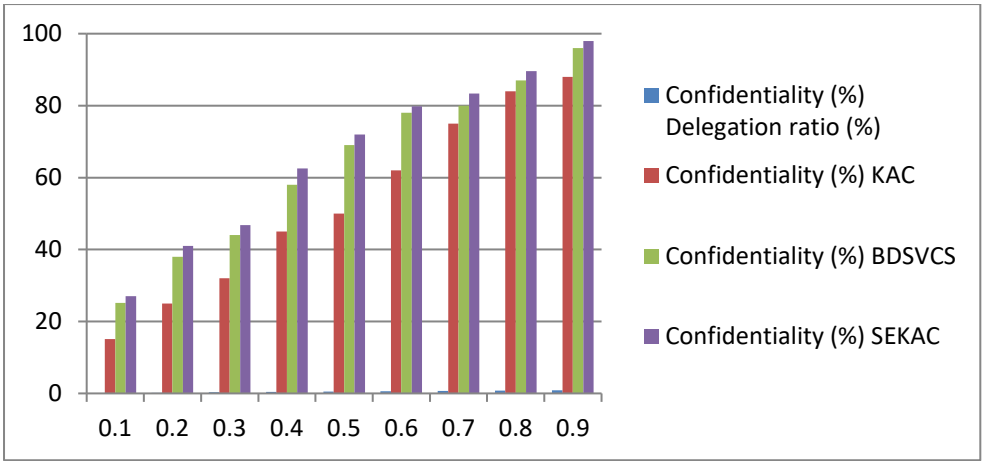


**Figure 3 Comparison Confidentiality with KAC, BDSVCS, SEKAC**

The table provides a performance comparison of existing BDSVCS and KAC in terms of confidentiality, as well as the proposed SEKAC. The suggested SEKAC produces 98% of the integrity with a delegation ratio of 0.9, while BDSVCS produces 96% and KAC produces 88%. This study compares the performance of existing BDSVCS and KAC methods with the proposed SEKAC method in terms of confidentiality. The plot shows the delegation ratio on the X-axis and confidentiality on the Y-axis. The delegation ratio is the ratio of surrogated cipher text classes to the total cipher text class. BDSVCS and KAC use public key cryptosystems, encrypting messages with a class identifier and a public key. The proposed SEKAC technique uses dual encryption and a class identifier, resulting in significantly higher confidentiality. SEKAC shows a 4.3% increase in confidentiality over BDSVCS and a 26% increase over KAC.

**4.2. Integrity Comparison:** Integrity pertains to guaranteeing the veracity of information, meaning that the information remains unaltered and originates from a legitimate source.

**TABLE 2 INTEGRITY COMPARISON VALUES**

| Integrity (%) | | | |
|---|---|---|---|
| **Delegation ratio (%)** | **KAC** | **BDSVCS** | **SEKAC** |
| 0.1 | 15.6 | 21.4 | 23.5 |
| 0.2 | 22.9 | 27.5 | 29 |
| 0.3 | 32.5 | 38.4 | 39 |
| 0.4 | 42.1 | 45.9 | 47 |
| 0.5 | 51.3 | 54.9 | 58 |
| 0.6 | 62.3 | 68.3 | 69.8 |
| 0.7 | 72.3 | 78.3 | 79.2 |
| 0.8 | 85.2 | 88.3 | 89.5 |
| 0.9 | 92.3 | 95.8 | 97.2 |

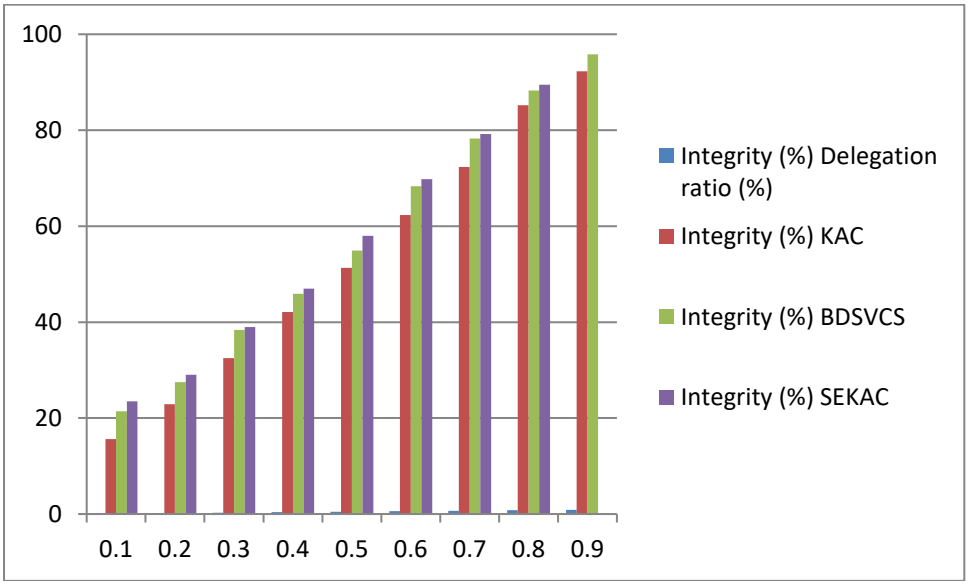


**Figure 4 Comparison Integrity with KAC, BDSVCS, SEKAC**

The proposed SEKAC technique encrypts messages using a class identifier of cipher text and a dual encryption approach. The suggested SEKAC method demonstrates a significantly higher level of integrity compared to existing methods, as seen by the experimental findings. There is a 2.58% improvement in integrity compared to BDSVCS, and an 11.68% increase in integrity compared to KAC techniques.

**4.3. Level of User Satisfaction** and **Resource Utilization Rate:** User satisfaction with cloud resources is determined by the quality of service (QoS), assessed both objectively and subjectively. Users provide subjective feedback post-usage, while enhanced procedures employ objective methods. High alignment between resource capabilities and user demands results in high satisfaction. In this study, SEKAC reached 80% user satisfaction after two iterations and nearly 90% after four. SEKAC assigns user preferences to clusters based on resource needs, improving user satisfaction through continuous feedback. Resource utilization is defined as the ratio of allocated to available resources, crucial for CPU performance and cloud provider profit. Compared to BDSVCS and KAC, SEKAC shows higher resource usage, efficiently allocating high-demand users to proficient resources. CIHMS enhances patient record security using the Smart SEKAC system, employing dual encryption for robust data protection. The SEKAC approach demonstrates superior security, integrity, confidentiality, and scalability over BDSVCS and KAC.

## 5. CONCLUSION

Private clouds are highly susceptible to computational security issues, particularly in ensuring secure data sharing. This study focuses on protecting private cloud content from various threats to maintain a secure and privacy-conscious environment, especially in healthcare settings where patient information is stored. The research findings indicate that the proposed strategy significantly improves outcomes.

The CIHMS (Cloud-based Integrated Health Management System) benefits from SEKAC technology, which enhances security through dual encryption, using both a standard and a partially functional key. Decryption involves an aggregate and a semi-functional key. Cipher text classes grow with data volume, making the system scalable. Experimental results show that SEKAC outperforms previous methods like KAC and BDSVCS in confidentiality, scalability, and reliability. The platform ensures secure key distribution via the Improved Diffie-Hellman Key Exchange Algorithm, enhancing security through random prime numbers, master secret keys, and parameter values. The attribute-based encryption mechanism is updated for better access control. Data sharing is secure and reliable, crucial for protecting healthcare data. Double clustering partitions cloud data, followed by clustering these partitions to enhance security. Data is encrypted using the Hybrid Elliptic Cryptographic technique, offering robust security. Experimental findings for CPSDTM, compared to IDHKE and SEKAC, show superior performance in secrecy, integrity, and scalability. CPSDTM achieves 3.96% higher confidentiality over IDHKE and 8.46% over SEKAC. It also shows improved integrity and user satisfaction, highlighting its effectiveness in secure data sharing.

The study aims to address security concerns in sharing Electronic Health Records (EHRs) in healthcare settings. It proposes a framework for maintaining HER confidentiality and privacy, preventing unauthorized access. The research focuses on static determination of secure HER sharing among healthcare units, whether homogeneous within a hospital or heterogeneous between different hospitals. A literature review identified current models and standards for health record exchange, revealing a need for customization and user-specific modeling for interoperability. A real-time study explored challenges in implementing HER security, finding that increased confidentiality can impact availability. The study emphasizes the importance of access control techniques and authorizations. Different access controls were evaluated using the Fuzzy TOPSIS methodology, identifying the ABAC (Attribute-Based Access Control) model as the most suitable for healthcare environments. ABAC allows flexible access control based on user and resource attributes. Policies in ABAC use XACML for adaptability and expandability.

The proposed framework herheres the Hierarchy Similarity Analyser (HSA) algorithm to provide secure Access to sensitive health records across organizations. HER refines access control policies and assigns security levels based on hierarchical distances. The framework manages user hierarchy differences and includes an Authorization method for controlling access. The framework was implemented and tested in various scenarios to demonstrate robustness. It effectively refines access control regulations, limiting data access to authorized users. Testing in both homogeneous and heterogeneous healthcare settings showed successful rule matching and conflict resolution, enhancing data sharing without compromising confidentiality and privacy. In conclusion, the proposed framework offers a viable solution for securely sharing sensitive health records across different healthcare organizations. It combines the benefits of centralized and decentralized data storage approaches, ensuring secure, efficient, and privacy-conscious HER sharing.

## 6. Future Work

Future work should focus on several key areas to enhance the current cloud security framework. Evaluating various quality of service (QoS) metrics is crucial to improving the cloud architecture's implementation. Ensuring job security remains a priority, especially when service providers may compromise key generators; thus, maintaining robust security measures is essential. Implementing an authentication mechanism will further enhance privacy assurance, while incorporating additional optimization approaches will ensure optimal and reliable resource selection for secure storage. Emphasizing key generation security can significantly bolster the study's overall protection levels. Analyzing various cloud threats will provide insights into the complexity and resilience of the proposed research. Simplifying the key generation process with an anonymity-based access control technique can facilitate real-time data collaboration within teams, granting access based on positions and reducing production time. Expanding the framework to process not only textual data but also photographs and scanned reports will meet the comprehensive needs of healthcare providers. Moreover, integrating health data sharing through cloud computing can support the scalability and portability of electronic health records (EHRs) across different healthcare systems. Exploring the mobile app industry is essential to offer health practitioners secure and controlled data access. Ultimately, adapting the framework to manage larger and more intricate hierarchies will ensure its applicability in diverse and complex healthcare environments.

## References:


1. Alotaibi, Y. K., & Federico, F. (2017). The impact of health information technology on patient safety. Saudi Medical Journal, 38(12), 1173-1180.
2. Coiera, E. (2015). Guide to health informatics. CRC Press.
3. Murphy, A. R., et al. (2016). User perceptions and the adoption of electronic health records in healthcare. Journal of Health Informatics, 12(3), 210-223.
4. Landi, H., et al. (2022). Current trends and future outlook for digital health and artificial intelligence in healthcare. Journal of Healthcare Informatics Research.
5. Bates, D. W., Lee, J., Seger, D. L., & Sheikh, A. (2018). The Impact of Health Information Technology on Patient Safety. In Health IT and Patient Safety (pp. 17-31). Springer, Cham.
6. Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: promise and potential. Health Information Science and Systems, 2(1), 3.
7. McCarthy, C., Eastman, D., & Garrett, N. (2020). Cloud computing in healthcare: Balancing efficiency and security. Journal of Cloud Computing, 9(1), 17-31.
8. Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. Journal of Medical Systems, 41(8), 127.
9. Keenan, M., Nguyen, H., Srinivasan, A., & Fladger, A. (2013). EHR usability: Moving beyond usability testing. Journal of the American Medical Informatics Association, 20(e1), e93-e94.
10. Adler-Milstein, J., & Jha, A. K. (2017). HITECH Act Drove Large Gains in Hospital Electronic Health Record Adoption. Health Affairs, 36(8), 1416-1422.
11. Sittig, D. F., & Singh, H. (2010). A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. BMJ Quality & Safety, 19(Suppl 3), i68-i74.
12. OCR (Office for Civil Rights). (2013). Summary of the HIPAA privacy rule. U.S. Department of Health & Human Services.
13. Jones, S. S., Rudin, R. S., Perry, T., & Shekelle, P. G. (2014). Health information technology: an updated systematic review with a focus on meaningful use. Annals of Internal Medicine, 160(1), 48-54.
14. Dinesen, B., Nonnecke, B., Lindeman, D., Toft, E., Kidholm, K., Jethwani, K., ... & Nesbitt, T. (2016). Personalized telehealth in the future: a global research agenda. Journal of Medical Internet Research, 18(3), e53.
15. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. NIST Special Publication, 800(145), 7.
16. Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: issues and challenges. In 2010 24th IEEE International Conference on Advanced Information Networking and Applications (pp. 27-33). IEEE.
17. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.
18. Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), 599-616.
19. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.
20. Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 8(6), 24-31.
21. Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. In 2009 IEEE International Conference on Cloud Computing (pp. 109-116). IEEE.

22. Pearson, S., & Benameur, A. (2010, November). Privacy, security and trust issues arising from cloud computing. In 2010 IEEE Second International Conference on Cloud Computing Technology and Science (pp. 693-702). IEEE.
23. Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2012). Toward secure and dependable storage services in cloud computing. IEEE transactions on Services Computing, 5(2), 220-232.
24. Zhu, X., & Xiong, L. (2013). Secure and efficient distributed aggregate computation via a lightweight hybrid approach. In Proceedings of the 2013 ACM SIGMOD international conference on Management of data (pp. 203-214).