*Journal of Harbin Engineering University* Vol 44 No. 8
*ISSN: 1006-7043* August 2023

# Secure Data Sharing and Privacy Preservation in AI-Driven Healthcare IoT Networks

**Neha Kulshrestha[1], Prajwal Prafulrao Wadettiwar[2], Mr. Tamil Thendral M[3], Mr. Nazeer Shaik[4], Dr. K. Sivanandam[5], C M Mohana[6]**

[1]Assistant Professor, Department of Computer Science and Information Systems, Shri Ramswaroop Memorial University, Lucknow, UP, India
[2]Department of Economics, Symbiosis School of Economics, Pune, Maharashtra, India.
[3]Assistant Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu, India.
[4]Assistant Professor, Dept. of. CSE, Srinivasa Ramanujan Institute of Technology (Autonomous), Anantapur, Andhra Pradesh, India.
[5]Associate Professor, Department of Electronics and Communication Engineering, M. Kumarasamy College of Engineering, Karur, Tamilnadu, India.
[6]Assistant Professor, Department of Computational Intelligence, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamilnadu, India.

**Abstract**

The healthcare industry has seen a total transformation thanks to the Internet of Things (IoT) networks powered by artificial intelligence (AI). These networks now provide previously unimaginable opportunities for remote monitoring, customized care, and immediate health supervision. However, this quick development has also led to significant worries about the security and privacy of private medical data transferred inside these networks. By using its expertise to enable seamless data flow within Healthcare Monitoring Systems (HMS), cloud computing has the potential to improve healthcare services[1]. In turn, this enables users to access health-related data regardless of location, including patients, physicians, pharmacists, and insurance agents. Security issues, though, make it difficult to integrate cloud computing into HMS. These security issues are caused by a lack of knowledge about data storage and the precise security measures used to protect data privacy. People who struggle with diseases like AIDS or other socially significant illnesses, for example, show considerable aversion to such systems and look for a highly reputable HMS that can securely store such sensitive data[2]. This study proposes a fresh strategy: the use of healthcare monitoring systems on the Aneka Cloud platform. With the help of the internet, this solution makes it possible to store, retrieve, and process patients' Electronic Health Records (EHRs) on the Cloud. Additionally, it rapidly alerts emergency agencies, doctors, and family members in urgent situations. On the mobile Cloud platform, a disease diagnosis functionality for Android is also being developed. This invention makes it easier to diagnose diseases using the symptoms that patients report, and it is especially useful for people who live in distant or underserved areas with little access to medical services.

**Keywords**: Secure data sharing, Privacy preservation, AI-driven healthcare, IoT networks, Encryption techniques, Access control, Data anonymization and Confidentiality.

## 1. Introduction

The field of cloud computing technology has expanded quickly and significantly in the modern environment. Cloud computing essentially offers a service-based approach as opposed to a product-based one. This involves transferring assets, programs, and data through networks or the internet. As a result, from the perspective of the user, there is unrestricted access to network resources and data that transcends geographical restrictions [3]. No matter where they are located in the world, people and resources are connected dynamically through the internet. The Healthcare and Banking sectors, among others, have been persuaded to align with and achieve their key goals by the inherent advantages of cloud computing. Cloud computing has the ability to strengthen services in the healthcare industry by

utilizing its know-how to enable seamless data flow within Healthcare Monitoring Systems (HMS).

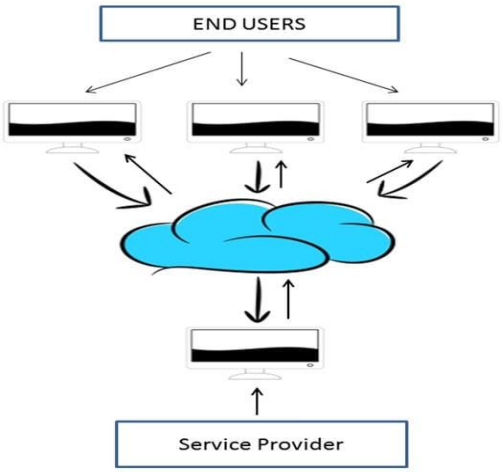



Figure.1: Primary approach of Cloud Computing

This capacity enables a wide range of stakeholders, including patients, doctors, pharmacists, and insurance agents, to easily obtain essential information whenever they need it without being constrained by regional boundaries. Although adoption of cloud computing has been slow at HMS, this is largely because of widespread security worries. The fundamental security problems result from a lack of thorough knowledge about the physical location of data storage, the types of security measures used to protect data privacy, and the effectiveness of these measures in providing strong protection[4]. To give an example, people dealing with serious illnesses like AIDS or other socially significant diseases angrily reject systems that do not ensure the highest level of security for their sensitive data. Their desire centers on a completely reliable healthcare monitoring system that can guarantee the complete security of their personal information.
Network engineers used a cloud-like shape to depict numerous devices and their related networks, giving rise to the word "Cloud" in this context. Figure 1 shows the main illustration of this Cloud network concept.

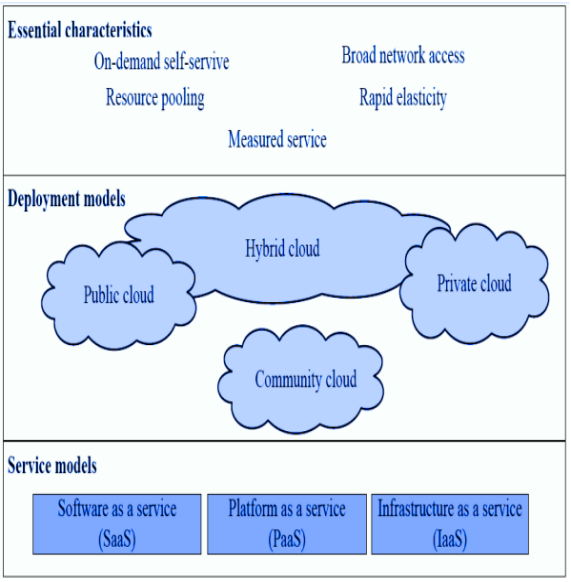



Figure.2: Key components and features in Cloud Computing by NIST

The development of cloud computing is the result of the fusion of numerous preexisting concepts and fresh ideas from various academic fields. These fields include distributed and grid computing, which enables parallel processing capabilities, service-oriented architecture (SOA), which offers a wide range of services, and virtualization, which forms the basis of cloud computing. With a focus on storage and computing services, this paradigm of cloud computing presents a viable computational model for both academics and industry. This strategy shows considerable promise to improve collaboration, scalability, dependability, agility, and availability by moving internal computer and storage infrastructure to remote servers managed via the internet. Figure 2 illustrates how the National Institute of Standards and Technology (NIST) conceptualizes cloud computing[5]. Three service models, four deployment models, and a number of Cloud Computing-specific traits are all included in the NIST framework. A recent change in the healthcare industry has seen the traditional paper-based health records moving toward electronic representations known as Electronic Health Records (EHRs), as seen in Figure 3. EHRs offer a wide range of benefits, including greater care precision, improved documentation techniques, increased efficiency, reduced medication errors, extended accessibility to medical information, increased safety measures,

and more. The Healthcare Monitoring System (HMS), a conceptual framework created to simplify daily operations and activities inside healthcare systems, has arisen in this setting[6]. Clinical processes, administrative duties, patient-related reporting, and other commercial viewpoints are all included in these activities. HMS is built on a foundation of interconnected subsystems that work together to give the best patient care and clinical management possible. Electronic Health Records (EHRs) are continuously collected, archived, and analyzed as part of HMS operations. These records come from a variety of sources, including administrative records kept by the healthcare institution, patient health data gathered during hospital visits, and other outside data sources.

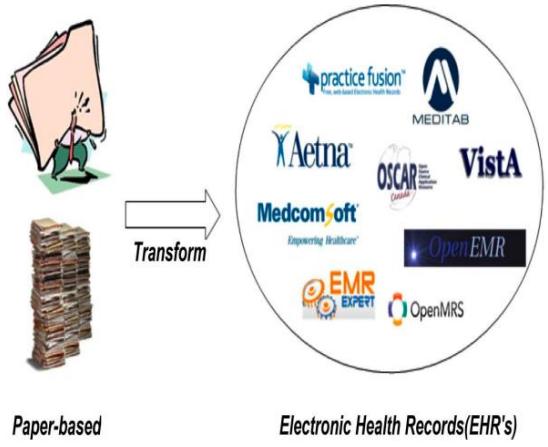



Figure.3: Transforming paper-based health records into Electronic Health Records (EHRs)

Figure 4 shows how the Healthcare Monitoring System (HMS) is laid out. This technology creates a network that links patients, doctors, important parties, and even ambulances. It enables the electronic health records (EHRs) that include patient medical information to be received and analyzed. The HMS updates health statuses and interacts with patients, clinicians, and family members based on the findings of this investigation[7]. The technology rapidly alerts the ambulance in emergency situations, extending the lives of victims. The key function of the Healthcare Monitoring System framework is around the secure management and processing of large amounts of data. Notably, the "Personal Data Protection Act," which was passed in 2018, was introduced by the Center for Internet Society of India (CIS-India). The need of protecting patient EHRs from unwanted access when shared through third-party channels is emphasized by this legislation.

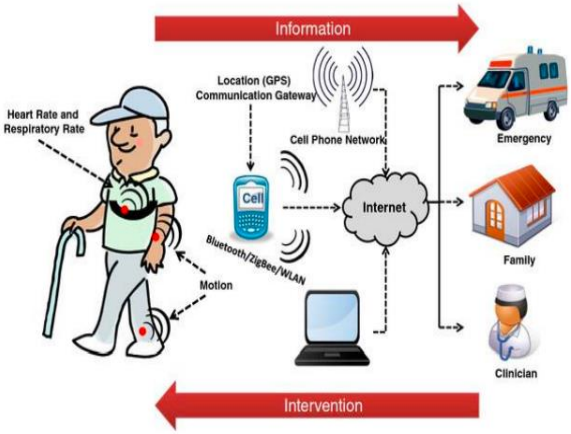



Figure.4: Healthcare Monitoring System architecture

An important development in information technology (IT) is cloud computing. It removes the barriers that prevent customers from accessing information and resources. Users merely need an internet connection to access the world's resources. The pay-as-you-go structure of cloud computing, which lets users only pay for what they use, is a distinctive characteristic. This method provides user-friendly access without requiring knowledge of core processes[8]. In the current environment, the healthcare sector is adopting internet services including websites and telemedicine consultations, similar to other industries. Physical patient visits are still necessary, though. Every day, data is transferred between many players in the healthcare industry, such as patients, physicians, pharmacies, and insurance companies. For instance, online services are the main reason insurance businesses are successful. On the other hand, pharmacies can let clinics know about newly created drugs that might take the place of older ones that are no longer effective or that have side effects. Swift data transfer is essential for providing high-quality medical care, and cloud computing plays a key role in making this happen. By preventing additional fatalities, the transmission of medical innovations has the potential to save many lives. Unrestricted worldwide data distribution is made possible by cloud computing. Healthcare firms use cloud computing to give information access to

stakeholders throughout the world via computers and mobile phones. As a result, they can create a "Cloud Healthcare Monitoring System (CHMS)" to effectively handle the processing, distribution, and collection of health information. For healthcare stakeholders looking for easy access to information and services, the move to cloud computing has proven to be cost-effective. Additionally, healthcare firms can use cloud computing to build an all-encompassing IT platform. This strategy encourages resource sharing between different clinics, cutting expenses and maximizing use. As mentioned in [5], cloud computing facilitates the monitoring and access of patient data. The patient records can now be easily accessed from anywhere in the world, at any time, thanks to this architecture.

## 2. Literature Survey

There is some ambiguity in the literature regarding the definition of Healthcare Monitoring System (HMS). However, the use of information and communication technology (ICT) techniques to meet medical care needs is frequently linked to HMS. ICT connections among important parties, such as clinics, healthcare businesses, and providers, facilitate the operation of HMS. [9] delves into the functions of patients, pharmaceutical experts, and non-medical pharmaceutical experts in the HMS framework's storage and processing of healthcare data. According to the literature, healthcare is viewed as a partnership between patients and medical staff members, including physicians, nurses, and pharmacists. For instance, the Online Health Dictionary (2019) describes healthcare as the service offered to patients by medical professionals in a variety of capacities, such as treatment, illness management, and prevention. Furthermore, [10] shows that HMS involves the sharing of medical data between patients and healthcare professionals, highlighting the importance of healthcare in disease diagnosis, treatment, and prevention, all of which are managed by medical specialists. The financial and social well-being of residents is substantially impacted by the quality of healthcare. Thus, quality, performance, security, and financial viability are among the top priorities for the healthcare system. Given the significant national investment required to deliver high-quality healthcare, addressing economic concerns is essential. Access to healthcare information and prompt disease response may be hampered by the actions of individuals within a country. As a result, it is critical to design adequate and affordable IT policies and infrastructure [3]. The application of IT principles to routine healthcare tasks streamlines procedures and improves healthcare quality.

To enable patient-centric dissemination of Electronic Health Records (EHRs) within a discriminating framework, the authors of [11] developed a centralized authority structure. This distribution is divided into various phases, such as information gathering and security requirements. In the context of access management procedures, the authors created a way to recognize and handle system exceptions. Healthcare providers implemented a centralized EHRs system for storing and accessing patient data within Healthcare Monitoring Systems (HMS). Different healthcare providers may use different EHR systems to serve patients in the setting of a cloud environment. These solutions might not, however, be compatible with cloud computing's granularity level. In [12], the authors identified security constraints unique to cloud-based e-health systems and presented a reference model for sharing data amongst cloud-based EHRs. In this model, the EHRs system was defined using a use case diagram along with pertinent security countermeasures and workable security techniques. [13] presented a patient-focused Digital Rights Management (DRM) strategy that took advantage of patient preferences to address data secrecy concerns involving EHRs that were outsourced to the Cloud. This strategy attempted to restrict outsourced data access by authorized users and ensure data confidentiality from Cloud Service Providers (CSPs). These [14] methods, however, fall short in their ability to enable fine-grained access control. Kilic et al. developed a plan to share EHRs among different eHealth Centres via a peer-to-peer network [15] to get over this restriction. Super-peers were utilized in this system to represent the eHealth Centres, allowing for message coordination and accommodating metadata used by various centres. It's crucial to remember that this method

is not cloud-based. For EHRs on the Cloud, [16] developed a novel design utilizing Attribute-Based Encryption (ABE) in the search for privacy-preserving techniques. They separated the system into distinct security areas, each of which controlled access for a certain subset of users, in order to address key sharing challenges. This strategy restricted access to only a certain group of people based on their viewpoints on the pertinent subject.

Electronic Health Records (EHRs) can be stored on the cloud and managed by healthcare providers and patients, which is a promising development. However, this decision raises a number of security issues, including how to keep EHRs in the Cloud accessible, shareable, processed, and stored securely. There may also be difficulties with key generation (key escrow), user revocation, and forward/backward secrecy. Despite its advantages, cloud computing poses special risks to the security and privacy of medical data in real time [17]. Numerous techniques have been introduced to deal with these problems. In the beginning, [18] presented an Identity-Based Encryption (IBE) method in which users can only decode data provided they had the corresponding identities. The authors subsequently moved on to Fuzz-IBE (also known as Attribute-Based Encryption or ABE), which restricts access to users who meet certain attribute conditions by encrypting and decrypting data using attributes set by the owner. To address simple attribute overlap scenarios, tree-based ABE systems like Key-Aggregate ABE (KA-ABE) and Ciphertext-Policy ABE (CP-ABE) were more frequently developed. DARPA implemented searchable encryption to solve privacy and security issues for EHRs stored on remote systems. This method achieves symmetric key encryption using a Secure Index (SI) with a searchable feature. Documents and keywords are contained in the SI, a data structure. If the user has access to the corresponding trapdoor, it only returns documents that match certain keywords. Only when the user possesses the secret key is the trapdoor capable of being generated. Patient Controlled Encryption (PCE) is a concept that is introduced in [19]. Medical information is organized in a tree format and encrypted using the patient's private key in PCE. This approach starts off by using a fixed hierarchy symmetric key PCE. The authors then expanded on this strategy to incorporate public symmetric key PCEs with both a fixed hierarchy and a flexible hierarchy. The idea of public key PCE obtained from pairings was also introduced in [19]. By addressing issues like access control, key management, and user-controlled encryption, these techniques and strategies aim to improve the security and privacy of EHRs in Cloud Computing environments. A Key Generation Authority (KGA) has been used in a number of earlier cryptographic methods to generate user keys from a master key. This method poses issues with key escrow, as the KGA, as a third-party server, might generate user keys for unlawful data access. To solve this problem, [20] proposed an identity-based search method that allows the KGA to share sensitive keys without being aware of user identities. When user IDs match attributes, this method works well with attribute-based encryption (ABE). This plan, however, is not appropriate for ABE for a number of reasons. First off, user attribute access must be controlled by extra security policies because user attributes are hidden from both the general public and the KGA. Additionally, because the KGA randomly distributes keys based on attribute sets, problems like attribute collision come up. It becomes difficult for the KGA to maintain consistency of random user key elements despite changes in attribute sets. Electronic Health Records (EHRs) in the Cloud have also been advocated for protection using non-cryptographic techniques. These techniques frequently make use of policy-based validation architecture, giving patients access to control rules. Some strategies incorporate cryptographic methods, such as the verification of digital signatures. In particular, [20] established the Data Capture and Auto Identification Reference (DACAR) principle to solve concerns with diverse health services' safety, integrity, confidentiality, and synthesis. The DACAR uses service-oriented architecture (SoA) to manage service applications while deploying and storing EHRs on private and public clouds. A low level addressing security and secrecy, a center level addressing permission specifications, and a top level addressing data verification services make up the three tiers of the DACAR design. A broker-

based permission technique for the targeted dissemination of EHRs from various Cloud Healthcare Monitoring Systems (CHMSs) was also given in [21]. In order to manage shared EHRs across several Clouds and create implicit composite EHRs, this system implements an EHRs collector. A policy administrator is in charge of specification upkeep and access control implementation. In order to combine numerous EHRs from diverse healthcare providers, this composite EHR system was created. However, when there are numerous healthcare providers involved, the complexity of access control strategies and architectures might provide difficulties.

## 3. Secure Architecture for Healthcare

The improvement of a patient's quality of life and longevity during an emergency greatly depends on prompt, effective access to health information [9], which makes a substantial contribution to dependable medical support. Healthcare services could be improved because to the scalability and security that cloud computing provides for cloud resources. But a crucial query surfaces: how secure is the outsourcing of medical data? Many people wonder if they should trust outside parties with their medical information.

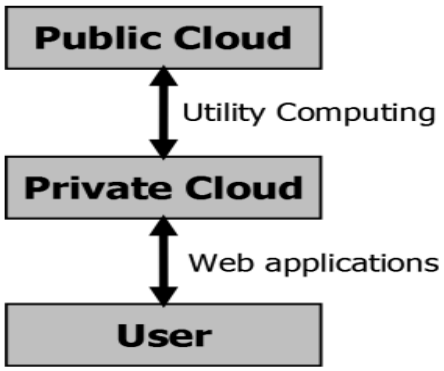



Figure.5: Cloud service model

This includes a variety of healthcare data that is kept on external servers, such as medical records, family history, insurance information, and associated knowledge. This practice raises issues regarding possible illegal access and exploitation of private data. Significant difficulties arise from the complexities of protecting healthcare data when it is shared and outsourced in a cloud setting. Many experts have focused their attention in recent years on understanding the privacy concerns of medical data kept on remote servers. Despite these efforts, there is still a glaring void in the comprehensive examination of technical-level privacy issues relating to healthcare data. The preservation of Electronic Health Records (EHRs) in cyberspace is a significant challenge that necessitates creative solutions to solve security and privacy concerns.It is obvious that a well-structured architecture and protocols must be developed right away to solve privacy and security issues while managing healthcare data on external servers. This study explores a safe architecture framework using Cloud service design principles to address privacy concerns, as seen in Figure 5. The core Cloud service model serves as the foundation for the suggested design. Together with public Cloud providers like Amazon or Google, Software as a Service (SaaS) companies offer a private Cloud architecture. Users can use internet-capable gadgets in this configuration to store and access their health-related data [6]. Users who use internet-connected devices boost data transmission. In this architectural design, extensive data processing duties are first handled by the private Cloud before the processed data is subsequently stored in the public Cloud. This method offers consumers a simple and secure way to handle their health information on Cloud servers while simultaneously enhancing security. In addition to ensuring higher security for users' health information, this structure makes it easier to engage with healthcare information on internet-enabled devices.

## 4. Proposed Model

Figure.6 shows the preferred system design, which includes a number of operational entities. The assigned controller, which is located within the private Cloud and plays a crucial part, is a key component of this system. This controller processes the data and creates an encrypted Index when a user desires to store their data on a remote server. Users and the private Cloud communicate with one another across a secure network that is made possible by a firewall. Users' keys and access policies are kept in the key store. These access techniques are used when a user is unable to access their data in an emergency because their device has been lost or isn't working properly. On the other hand, the

Untrusted controller is semi-trusted because it is a part of the public Cloud. In light of this, only cipher text data may be processed. Trapdoors are used for search operations that utilize search patterns from the unreliable controller. This strategy makes sure that the Cloud data is safe and that misuse is avoided. In the cloud, files are kept in encrypted form for data storage. The assigned controller processes a group of documents (D) to produce an Index (I), which is then saved as ciphertext. The Medical Emergency Service (MES), which is tasked with connecting a doctor who can aid in an emergency, also plays a part in the system. Data access is dependent on user attributes in an Attribute-dependent Encryption (ABE) scheme, providing users access to data only if they comply with the established access regulations. Patients can define shared access strategies based on user traits in the proposed design, facilitating data access in an emergency. Based on the patient's access policy, the private Cloud and MES can both give emergency data access. Figure.6's network architecture depicts the interactions that are made possible by both public and private networks. The Personal Area Network (PAN), a private network, uses technologies like Bluetooth and Wi-Fi networks whereas the public network includes the Internet. The design encourages the usage of all internet-enabled devices to upload health data to the private Cloud, enabling secure and readily available healthcare data management even while data privacy within the personal area network is not a main priority.

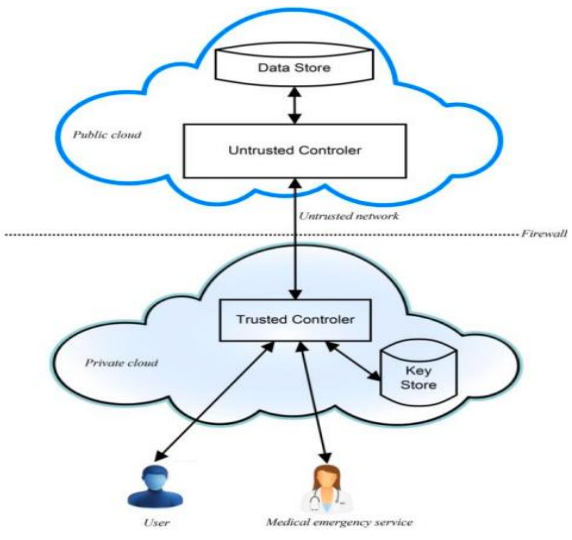



Figure.6: Cloud Computing system architecture

Cloud service companies are typically regarded as semi-honest. Although they normally behave honestly, there are times when they might secretly work with unauthorized people or invaders to carry out malicious deeds. Through the execution of illegitimate requests, this may cause harm to data owners. Cloud providers frequently disguise their operations as protocol compliance in order to appear to be behaving legally and profitably. In the suggested concept, a private Cloud runs behind the protection of a firewall and is completely reliable for managing computations involving healthcare data. The public Cloud, on the other hand, is precise but observant, as was previously mentioned. As a result, all data processing must take place in ciphertext form, and data stored in the Cloud must be encrypted. Here, it is assumed that the channel of communication between users and the private Cloud is a reliable network that provides for its security. The public Cloud and private Cloud's communication channel, however, cannot be trusted. This could result in data leakage, which poses a risk for the exchange of sensitive data. As a result, the Medical Emergency Service (MES) is given the authority to access data for therapeutic purposes in urgent circumstances. The MES is given permission to access data even if they do not have the required permissions since they believe the data owner is unable to grant access because of the emergency. In conclusion, even though cloud service providers are mostly reliable, there may be occasions where collaboration results in unlawful behavior. In order to provide data confidentiality and secure emergency data access, the architecture handles security problems by encrypting data and processing it in ciphertext form with different trusted and untrusted communication channels.

## 5. Security Analysis

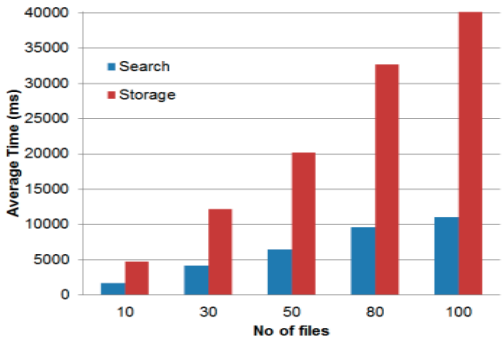
Six storage policies are included in the suggested system architecture to improve data security. First off, shared material that is encrypted cannot be accessed by unauthorized individuals. Second, because file identifiers take the form of numbers, it is difficult to determine file information or ownership. Thirdly, since several sets of files contain the same keyword, redundancy in linked

lists makes it difficult for hackers to find pertinent files. Fourthly, because all transactions take place within the private Cloud environment, user identities are kept anonymous in the public Cloud. Fifthly, the random storing of files prohibits unauthorized users from creating links between current and past keyword searches. Last but not least, the search mechanism is quite effective. It makes use of trapdoors to ensure that sensitive information is kept hidden and also makes use of a hash table to increase search efficiency. Attribute-Based Encryption (ABE) can be used in emergencies to create fine-grained access control. Only when the access policy of the data owner is honored by the Medical Emergency Service (MES) can access be granted. The access method is kept in a private cloud, making it easier to obtain all necessary data. ABE avoids the usage of resource-intensive techniques, and the access policy process is simple. A role-based login system can be used to get around situations when MES has trouble verifying the user's qualities. Data files can be easily transferred from mobile devices to the private Cloud, where they are converted to an encrypted format and then stored in the public Cloud. This strategy is thought to be quite useful. The proposed solution is highly viable and will continue to function normally unless the private Cloud is compromised. It may be said that the private Cloud has high criteria for correctness and integrity, which makes the entire system incredibly durable.

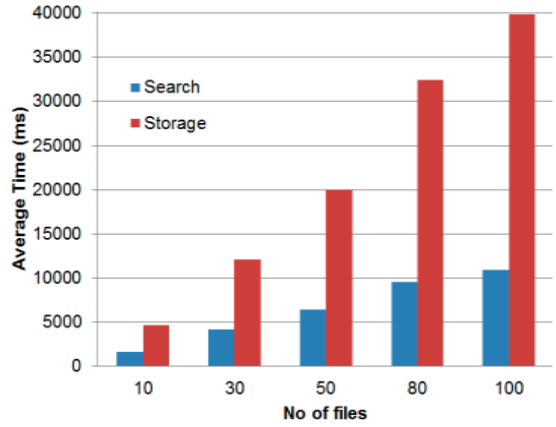
The Medical Emergency Service (MES) will access data in emergency scenarios depending on the user-defined criteria provided at registration. In the event that the user's personal device is misplaced, stolen, or otherwise not in compliance with the requirements at any given time, the MES will permit emergency access. Attribute-Based Encryption (ABE) approaches suitable for emergency access scenarios have been developed in a few prior studies [22]. These methods do have certain drawbacks, though. It becomes difficult to apply access permissions to each file separately, for instance, if a user allows emergency access under a file-based access permissions scheme. A more streamlined strategy is suggested to address these issues: implementing a general ABE access policy to all files. In this architecture, a common access policy is used instead of requiring individuals to individually encrypt their data using ABE. The private Cloud is where these access policies are kept. Based on user-defined access policies, both the private Cloud and MES will make it easier to access emergency data. A problem occurs, though, when someone asserts certain characteristics, as the MES might not be able to verify such assertions. A role-based login system can be used to solve this problem [20]. Users log in using their assigned roles, enabling the MES to quickly confirm and keep track of the actions of the right user. This strategy improves the precision and dependability of emergency access validation, making sure that only authorized individuals can access sensitive information in urgent circumstances.

## 6. Results and Discussion

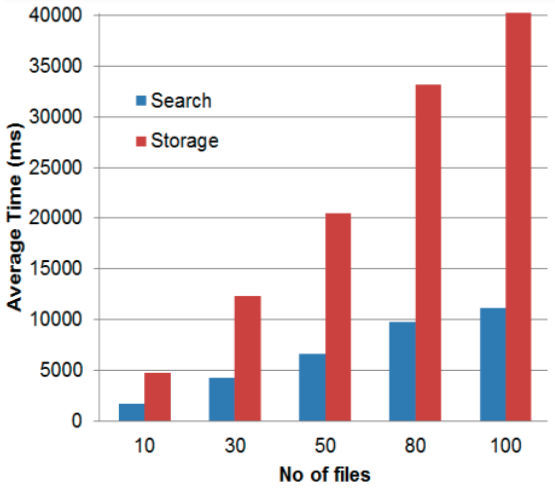
The Aneka Cloud platform is used to implement the private Cloud. Mobile devices such the Samsung Galaxy Grand 2, Lenovo K3 Note, and Apple iPhone 5 were tested, primarily in a 2G network environment, to validate the proposed architecture. At first, experiments on files of equal size were used to gauge storage performance. For instance, the times required to store 10 files and one hundred keywords were 4500ms, 4478ms, and 4569ms, respectively. Additionally, the examination was broadened to include 30, 50, 80, and 100 files, among other figures. The benchmark results of this extended analysis for thirty, fifty, and one hundred files, respectively, are shown in Figures 7(a), 7(b), and 7(c). These benchmark results give information on the efficiency and scalability of the suggested design and aid in evaluating the storage performance of the system in various circumstances.




(a)




(b)




(c)

Figure 7 illustrates the performance results The processing times for storage and search activities are shown in Figure 7 as an illustration of the performance outcomes from the implementation. The following devices were used to do these operations: a) the Samsung Galaxy Grand 2; b) the Lenovo K3 Note; and c) the Apple iPhone 5. The provided information makes it possible to compare the reaction times of various devices and network connectivity possibilities. When working with data that has been outsourced, the suggested system design guarantees the protection of the data against unauthorized users. Users can only decrypt ciphertext using the proposed system's attribute-based encryption (ABE) if they have the necessary attributes. The system also uses immediate attribute revocation, which makes sure that users who are kicked out of a group can't access any plaintext that's related to that group. Re-encrypting the ciphertext with revised attribute group access regulations does this, thereby preventing users with access privileges that have been revoked from viewing the data. A two-authority key generation approach is used to protect against potential attacks from both the Cloud server and the Key Generation Authority (KGA). This system makes guarantee that no single authority may independently produce a secret key. Users who request a key from the Cloud server and KGA each obtain their own unique key. The secrecy of Electronic Health Records (EHRs) stored on the Cloud server is improved when the user combines these keys to create their own key. The test results also show how the suggested design's response times compare across communication channels, notably 4G and Wi-Fi. The network bandwidth is the main factor affecting how well storage and search activities function. According to the findings, the suggested design is very effective, with the private Cloud mostly handling the processing demand. Through a personal area network, users may easily send their data to the private Cloud, which will handle the necessary tasks and safely upload the data index to the public Cloud. Overall, the proposed architecture is proved to be successful, especially when taking the communication routes' bandwidth into account.

## 7. Conclusion

In order to provide secure storage and retrieval of health records from the public Cloud, the proposed system introduces a secure architecture that makes use of a private Cloud. Integrating numerous traits, including unlinkability and anonymity, results in privacy. Additionally, the design makes sure that search patterns are hidden, preventing the release of critical data unless the private Cloud is reliable. In emergency situations, the Medical Emergency Service (MES) is essential for gaining access to information via role-based authentication and attribute-based encryption (ABE). A set of tests that highlight the system's performance in terms of storing and retrieving data show off its effectiveness. It's crucial to recognize certain potential problems with the suggested system, though. Key escrow issues could potentially arise if only one key generation authority is used. on this situation, the key generation authority might produce user keys without the user's input, giving it potential access to unencrypted data

kept on the Cloud. The security and privacy of the healthcare monitoring system are seriously threatened by this predicament. User revocation is yet another crucial problem that the Healthcare Monitoring System (HMS) needs to address. For a variety of reasons, patients may need to withdraw access permits from particular users. This revocation process should be safe and easy to complete without impairing the access rights of other users or jeopardizing data privacy. Conclusion: Even though the suggested system offers promising options for managing and accessing secure healthcare data, it's crucial to carefully analyze and address potential problems like key escrow and user revocation to guarantee the system's overall effectiveness and integrity.

**References**

1. S. M. Karunarathne, N. Saxena and M. K. Khan, "Security and Privacy in IoT Smart Healthcare," in *IEEE Internet Computing*, vol. 25, no. 4, pp. 37-48, 1 July-Aug. 2021, doi: 10.1109/MIC.2021.3051675.
2. S. S. Gopalan, A. Raza and W. Almobaideen, "IoT Security in Healthcare using AI: A Survey," *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, Sharjah, United Arab Emirates, 2021, pp. 1-6, doi: 10.1109/ICCSPA49915.2021.9385711.
3. G. Srivastava, J. Crichigno and S. Dhar, "A Light and Secure Healthcare Blockchain for IoT Medical Devices," *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, Edmonton, AB, Canada, 2019, pp. 1-5, doi: 10.1109/CCECE.2019.8861593.
4. A. AlSunbul and W. M. Elmedany, "Blockchain-based IoT security in healthcare," *4th Smart Cities Symposium (SCS 2021)*, Online Conference, Bahrain, 2021, pp. 531-536, doi: 10.1049/icp.2022.0396.
5. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain and K. -S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," in *IEEE Access*, vol. 3, pp. 678-708, 2015, doi: 10.1109/ACCESS.2015.2437951.
6. A. Yogeshwar and S. Kamalakkannan, "Healthcare Domain in IoT with Blockchain Based Security- A Researcher's Perspectives," *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, 2021, pp. 1-9, doi: 10.1109/ICICCS51141.2021.9432198.
7. E. Fazeldehkordi, O. Owe and J. Noll, "Security and Privacy in IoT Systems: A Case Study of Healthcare Products," *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, Oslo, Norway, 2019, pp. 1-8, doi: 10.1109/ISMICT.2019.8743971.
8. S. Ahmed, Z. Subah and M. Z. Ali, "Cryptographic Data Security for IoT Healthcare in 5G and Beyond Networks," *2022 IEEE Sensors*, Dallas, TX, USA, 2022, pp. 1-4, doi: 10.1109/SENSORS52175.2022.9967208.
9. S. B. Baker, W. Xiang and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," in *IEEE Access*, vol. 5, pp. 26521-26544, 2017, doi: 10.1109/ACCESS.2017.2775180.
10. P. Kamble and A. Gawade, "Digitalization of Healthcare with IoT and Cryptographic Encryption against DOS Attacks," *2019 International Conference on contemporary Computing and Informatics (IC3I)*, Singapore, 2019, pp. 69-73, doi: 10.1109/IC3I46837.2019.9055531.
11. Y. A. Qadri, A. Nauman, Y. Bin Zikria, A. V. Vasilakos and S. W. Kim, "The future of healthcare Internet of Things: A survey of emerging technologies", *IEEE Commun. Surv. Tut.*, vol. 22, no. 2, pp. 1121-1167, Apr.–Jun. 2020.
12. M. Burhan, R. A. Rehman, B. Khan and B. S. Kim, "IoT elements layered architectures and security issues: A comprehensive survey", *Sensors (Switzerland)*, vol. 18, no. 9, pp. 1-37, 2018.

13. M. A. Sahi et al., "Privacy preservation in e-Healthcare environments: State of the art and future directions", *IEEE Access*, vol. 6, pp. 464-478, 2017.
14. S. Challa et al., "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks", *Comput. Elect. Eng.*, vol. 69, pp. 534-554, 2018.
15. S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu and A. V. Vasilakos, "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems", *Futur. Gener. Comput. Syst.*, vol. 108, pp. 1267-1286, 2020.
16. Y. Yang, X. Liu, R. H. Deng and Y. Li, "Lightweight sharable and traceable secure mobile health system", *IEEE Trans. Dependable Secur. Comput.*, vol. 17, no. 1, pp. 78-91, Jan./Feb. 2020.
17. Y. Yang, X. Zheng, W. Guo, X. Liu and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system", *Inf. Sci.*, vol. 479, pp. 567-592, 2019.
18. F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges", *IEEE Commun. Surv. Tuts*, vol. 22, no. 3, pp. 1686-1721, Jul.–Sep. 2020.
19. T T Chhowa, M A Rahman, A K Paul and R Ahmmed, "A Narrative Analysis on Deep Learning in IoT based Medical Big Data Analysis with Future Perspectives", *2nd Int. Conf. Electr. Comput. Commun. Eng. ECCE 2019*, pp. 1-6, 2019.
20. A Strielkina, O Illiashenko, M Zhydenko and D Uzun, "Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment", *Proc. 2018 IEEE 9th Int. Conf. Dependable Syst. Serv. Technol. DESSERT 2018*, pp. 67-73, 2018.
21. M Jayalakshmi and V Gomathi, "Pervasive health monitoring through video-based activity information integrated with sensor-cloud oriented context-aware decision support system", *Multimed. Tools Appl.*, 2018.
22. M Saadeh, A Sleit, K E Sabri and W Almobaideen, "Hierarchical architecture and protocol for mobile object authentication in the context of IoT smart cities", *J. Netw. Comput. Appl.*, vol. 121, pp. 1-19, 2018.