International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V71I10P222

Volume 71 Issue 10, 238-253, October 2023
© 2023 Seventh Sense Research Group®

Original Article

Secure and Privacy-Preserving Storage of E-Healthcare Data in the Cloud: Advanced Data Integrity Measures and Privacy Assurance

G. Dhanalakshmi[1], G. Victo Sudha George[2]

[1,2]Department of Computer Science and Engineering, Dr.M.G.R Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu, India.

[1]Corresponding Author : dhanalakshmi4481@gmail.com

Received: 07 June 2023 Revised: 26 August 2023 Accepted: 02 September 2023 Published: 03 October 2023

***Abstract** - Cloud-based E-Healthcare systems require effective management of both internal and external security risks, which can be addressed through a range of cloud security practices and technologies. However, the need for significant storage capacity raises concerns about data security and cyberattacks. Thus, improving the security levels of cloud-based E-Healthcare systems remains a complex challenge that requires ongoing attention and resources. In this research, a unique method for creating a safe and private cloud storage system for electronic healthcare data is proposed. Moreover, it employs a hybrid cryptography technique that combines symmetric and asymmetric key encryption algorithms to enhance data security and privacy. The system also integrates advanced data integrity measures, including hash functions and checksums, to ensure data authenticity, integrity, and non-repudiation. The proposed system employs a range of trustworthy security measures, including advanced encryption techniques, role-based access control mechanisms, robust data validation utilising hash functions, and admin activity with data access and audit trails to safeguard against unauthorised access and prevent data leakage. The system is deployed in a cloud environment to provide scalable and cost-effective storage solutions for E-Healthcare systems. Experimental results show that the suggested system outperforms alternatives regarding efficiency, security, and privacy. It can help improve the quality of healthcare services by ensuring patient privacy and confidentiality.*

***Keywords** - Cloud security, E-Healthcare systems, Data security, Hybrid cryptography and Access control mechanisms.*

1. Introduction

Cloud data storage has become increasingly popular due to its scalability, cost-effectiveness, and ease of access. However, the convenience of cloud storage comes with the challenge of ensuring data security, which has become a critical issue for cloud service providers. Since it must safeguard the privacy, accuracy, and accessibility of data stored there, cloud data storage security poses a number of issues. Access control measures must be put in place to restrict unauthorized access to the data. At the same time, data encryption provides an additional layer of security by rendering the data unreadable to unauthorized users.

Data backup must be employed to prevent data loss in case of accidental deletion, system failure, or cyber-attacks. Both cloud service providers and clients share responsibilities for ensuring cloud data storage security. Strong passwords, regular system updates, and two-factor authentication are some practices that customers must adopt. Additionally, they must continuously monitor their cloud storage for suspicious activities and ensure that data is encrypted before being uploaded to the cloud.

E-Healthcare, which involves using technology to enhance healthcare services, has numerous advantages, including improved efficiency, cost savings, and better patient outcomes. However, it also raises significant security concerns. Some key security issues in E-Healthcare include data breaches, unauthorized access, malware and viruses, system failures, and patient safety.

Cybercriminals can target electronic health records, leading to identity theft and insurance fraud, while unauthorized access can result in serious privacy breaches. Malware and viruses can infect E-Healthcare systems and disrupt services, while system failures can cause delays in treatment. Patient safety can be compromised if patient data is compromised, leading to misdiagnosis, medication errors, or other serious safety concerns. In order to tackle security issues associated with E-Healthcare systems, implementing strong security measures such as access controls, encryption, firewalls, and periodic software updates is crucial.

1.1. Cloud Service Delivery Models

To address various customer needs, cloud computing offers a spectrum of services. Users can develop and manage their own cloud-based applications within this framework, accessing virtualized computing resources, including servers, storage, and networking.

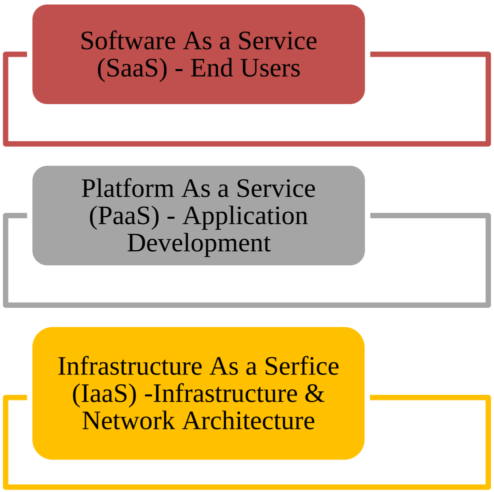

Software As a Service (SaaS) - End Users
Platform As a Service (PaaS) - Application Development
Infrastructure As a Serfice (IaaS) -Infrastructure & Network Architecture

Fig. 1 Cloud service models [2, 3]

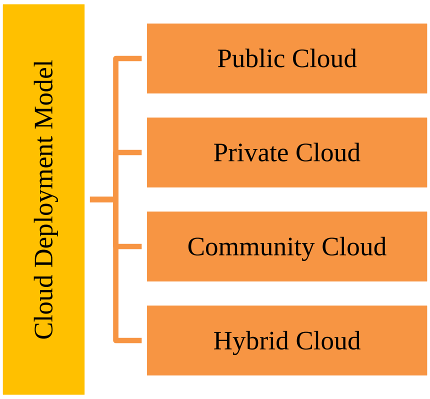


Fig. 2 Cloud deployment models

- Infrastructure as a service offers virtualized computing resources like servers, storage, and networking. Infrastructure as a Service (IaaS) enables users to create and maintain their own applications on the cloud platform.
- Platform as a Service (PaaS) offers a pre-configured platform with development tools, runtime environments, and other services so that applications can be built, deployed, and managed without the requirement for underlying infrastructure management.
- Software as a Service (SaaS) offers ready-to-use software programs available online, eliminating users needing to install and manage the software on their own devices.
- Function as a Service (FaaS) provides a server-less architecture where customers can run small code units in response to events, paying only for the exact amount of resources consumed by the function.
- Container as a Service (CaaS) provides a complete environment for running and managing containerized applications, abstracting away the complexity of infrastructure management.

1.2. Cloud Deployment Models

Incorporates the following the categories cloud deployment model

- Third-party vendors provide public cloud services over the internet and can be accessed by anyone subscribing to the service.
- A private cloud is a cloud delivery design that allows for more control, customization, and security over the cloud environment since just one organization makes use of the cloud infrastructure.
- Combining private and public cloud models, the hybrid cloud helps organizations use both deployment types' advantages while still keeping control over sensitive data and applications.
- A community cloud combines the benefits of a private cloud and is shared by organizations with similar objectives, such as meeting regulatory compliance requirements.
- Multi-cloud deployment involves using various cloud services from different providers to prevent vendor lock-in, enhance redundancy, and leverage specialized services from each provider.

1.3. Cloud Security Risks and Security Policies

1.3.1. Cloud Security Risks

Proper security measures, like encryption and access control, are crucial to stop hackers from stealing data from cloud services. Even people inside the organization with access to cloud systems can be a risk to data security. Not following regulatory requirements can lead to legal and financial problems.

It can be hard for organizations to keep track of data when it is stored and processed off-premise. Cloud provider reliability is very important to ensure data and applications can always be accessed. Using third-party vendors for cloud services can bring extra risks, like security breaches.

1.3.2. Security Policies

Information security's main premise is maintaining information availability, confidentiality, and integrity. Integrity maintains the information's accuracy and unchanged status, while confidentiality ensures that only those with permission can access it. Last but not least, accessibility guarantees rapid, unfettered access to information when needed.

2. Research Methodology

Conducting a literature review is crucial in establishing a strong foundation for expanding knowledge and identifying areas that require further research. The objective of this study is to elucidate the methodology employed for conducting a thorough and comprehensive literature search, which involved using a literature search engine to explore high-quality academic literature databases (including IEEE Xplore, Science Direct, ProQuest, Springer, and Mendeley References online library).

The search criteria were restricted to document titles, and search terms such as "cloud computing," "security," "data storage," "threats," and "attacks" were used to search all databases. Initially, the search produced 86 records, including duplicates.

Table 1. Comparison of different cloud platforms

Cloud Platform	Cost	Scalability	Security	Performance	Available Services
Amazon Web Services (AWS)	• Flexible AWS pricing options • Customizable to specific needs • Costs can escalate quickly	• Easy scalability on cloud • Multiple auto-scaling options • Optimizes performance and cost	• Robust AWS security • Adheres to compliance standards • Ensures data confidentiality and integrity	• High-performance computing • Customizable networking options • Wide range of cloud services	• Compute, storage, databases, and AI. • Analytics, DevOps, security, and more
Microsoft Azure	• Flexible Azure pricing • Pricing can be complex • Pay-as-you-go, reserved, and spot	• Multiple Azure scaling options • Near-unlimited scalability • Optimizes performance and cost	• Strong Azure security • Compliant with regulations • Ensures data confidentiality and integrity	• Customizable Azure networking • Fast computing capabilities • Optimizes performance with tools.	• Compute, storage, networking, databases, AI, IoT, DevOps, security, analytics, and more.
Google Cloud Platform (GCP)	• Competitive Google Cloud pricing • Additional fees for some service • Costs can quickly add up	• Dynamic auto-scaling • Highly scalable infrastructure • Supports growth	• Robust GCP security • Data encryption IAM for user access control • Security key enforcement	• High-performance computing • Fast data processing • Load balancing for optimization Auto scaling and CDN features	• AI/ML services available • Scalable storage solutions • High-speed data transfer • Low-latency fibre network.

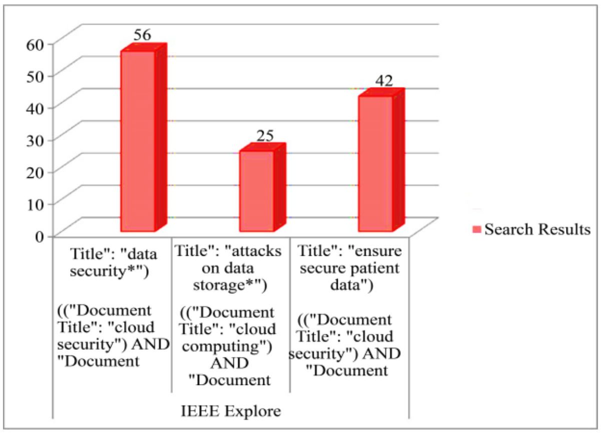


Fig. 3 Search results based on data bases

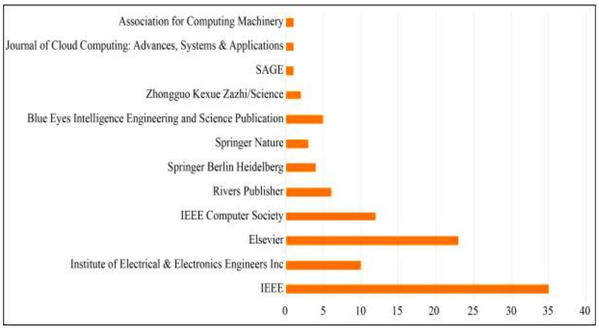


Fig. 4 List of journals on secure cloud storage environment

Figure 3 provides information about search results based on databases, and Figure 4 shows the number of journals. The three stages of the survey cover various challenges, threats, and risks related to cloud storage security that are relevant in the context of cloud computing. Stage 1: involves searching the IEEE Xplore Digital Library, Springer, and Science Direct databases, as well as using keyword searching and the Boolean "+" operator. Stage 2:Mendeley Desktop Software is used to gather references, organize quotes, and create bibliographies while also serving as an academic social network for sharing research ideas. Stage 3: Collecting and evaluating 150 articles using Mendeley References, which were narrowed down to 86 articles focused on data storage security issues, threats, and risks in cloud computing. The Working Model of Literature Survey on Mind Map in Figure 5 provides an overview of the survey, including database details, a list of publishers, and a list of journals to help prepare the survey paper.

3. Related Work

[1] The authors have proposed a secure cloud storage system that employs secure network coding techniques and data dynamics to enhance data security and availability in cloud storage. This system utilizes encryption, network coding, and data redundancy techniques to ensure the confidentiality, integrity, and availability of data in cloud

storage systems. [2] The authors have introduced an improved authentication scheme for remote data access and sharing in cyber-physical-social systems using cloud storage. This scheme incorporates a lightweight mutual authentication protocol that utilizes hash functions and a shared secret key, thereby enhancing the security of cloud-based data access and sharing.

[3] The proposed scheme has been designed to address the security and efficiency issues of existing multi-authority access control schemes, making it a promising solution for secure data storage in IoT applications. [4] The authors have introduced Web Cloud, a web-based cloud storage system that enables secure data sharing across multiple platforms. This system provides strong security guarantees and efficient sharing capabilities, making it a promising solution for secure data storage and sharing in the cloud. [5] The authors propose a novel cloud-based approach for healthcare information systems that ensures secure and efficient storage and retrieval of patient data. This approach is designed to tackle the challenges faced by traditional healthcare information systems and elevate the overall quality of healthcare services.

The authors propose a big data approach for a secure E-Healthcare information system in cloud environments. This system employs access control, encryption, and intrusion detection to ensure patient data confidentiality, integrity, and availability, making it a promising solution for secure healthcare information management. This review evaluates various cryptographic techniques for cloud-based data protection, highlighting their strengths and weaknesses and providing insights into their applicability. It is a valuable resource for researchers and practitioners in the field of cloud security.

[6] A proposed algorithm provides strong security guarantees while requiring fewer computational resources, making it a promising solution for secure data storage and transmission in resource-constrained cloud environments. [7] The authors propose a novel method for enhancing security in sustainable systems in cloud computing by combining encryption and data mining techniques. This method offers improved security and efficiency for cloud-based systems, making it a promising solution for addressing security challenges in sustainable cloud computing.

The authors propose a web-based cloud storage system, Web Cloud, that offers strong security guarantees and efficient sharing capabilities. This system is a promising solution for secure data storage and sharing in the cloud. [8] The authors propose a secure encryption scheme for protecting multimedia data in cloud environments, utilizing a Composite Logistic Sine Map (CLSM) and SHA-256. The scheme offers high security and efficiency, making it a promising solution for secure data storage and transmission in cloud-based multimedia applications. [9] The proposed approach achieves high search efficiency and strong security guarantees, making it suitable for practical cloud storage systems. [10] The authors propose an attribute-based encryption approach that allows for secure and efficient storage, sharing, and retrieval of encrypted data in the cloud. Experimental results show its superiority over other methods.

[11] A cloud-based buyer-seller watermarking protocol (CB-BSWP) is proposed in this paper, utilizing a semi-trusted third party for copy deterrence and privacy preservation. The protocol achieves copy deterrence and privacy preservation without revealing any sensitive information about the buyer or the seller to a third party. [12] An approach for secure and efficient data sharing and search in a cloud-edge collaborative storage system is proposed by the authors. This is done using a combination of attribute-based encryption and searchable encryption techniques, which can be useful for various applications that require secure and efficient data sharing and search in a collaborative cloud-edge environment.

[13] An efficient privacy-preserving certificate-less provable data possession scheme for cloud storage is presented in the article. This ensures data confidentiality and integrity with low communication overhead, making it suitable for practical applications. [14] A shared dynamic data audit scheme that supports anonymous user revocation in cloud storage is introduced by the authors. This ensures the security and privacy of users' data. A novel signature-based aggregate range query protocol enables anonymous user revocation with efficient computation and communication overhead.

[15] The authors suggest a secure image retrieval scheme based on AES, random mapping, and bag-of-words in cloud computing to improve the privacy and efficiency of image retrieval. Experimental results show that the proposed scheme outperforms existing schemes regarding retrieval accuracy and efficiency. [16, 17] A blockchain-based approach to secure storage and access of electronic medical records in the Inter Planetary File System (IPFS) is proposed in this article.

This proposed approach utilizes smart contracts to control access to the stored medical data. It allows patients to permit healthcare providers to access their medical records securely, with improved privacy and authenticity. [18] The authors propose an SGX-based key management framework that provides secure and efficient key management for data-centric networking. The framework can protect sensitive key information from unauthorized access and tampering and support dynamic key management for various data-centric networking applications. [19] The article presents a comprehensive benchmarking study of dynamic, searchable, symmetric encryption schemes for cloud-Internet of Things applications.

It evaluates their performance in terms of query processing time, index size, and communication overhead, identifying the most efficient schemes and highlighting the trade-off between security and efficiency, which can guide the selection of an appropriate scheme based on the specific needs of a cloud-IoT application. [20] The authors present a generic construction of expressive public-key encryption with keyword search from key-policy attribute-based encryption. They also present an efficient scheme over prime-order groups that provides stronger security guarantees and faster search speed compared to existing solutions. [21] The paper proposes a verifiable key-aggregate keyword searchable encryption scheme for secure data sharing in storage. This achieves efficient keyword search and update operations while preserving data confidentiality and privacy. [22]

A secure content-based image retrieval scheme in cloud computing is introduced, ensuring the confidentiality of the query image and search key. This scheme achieves both privacy protection and efficient search performance, using a combination of homomorphic encryption and secure multi-party computation to protect the confidentiality of the query image and search key while using a locality-sensitive hashing technique.

[23] The authors proposed a new decentralized cloud storage security framework that enforces authorization policies on access control decisions made by storage providers. The framework allows for delegated access control decisions and supports secure resource sharing and auditing.

[24] The authors presented an identity-based public auditing scheme for cloud storage systems that utilizes blockchain technology to ensure audit integrity and resist attacks from malicious auditors. The scheme is efficient and provides security and privacy guarantees. [25] This paper presents a privacy-preserving approach for real-time image integrity auditing in cloud storage systems using a blockchain-based arbitration mechanism.

The method reduces computation and communication overheads while providing confidentiality, integrity, and availability guarantees. [26] The paper suggests an Attribute-Based Encryption (ABE) approach for secure storage, sharing, and retrieval of encrypted data in the cloud, focusing on scalability and performance.

The proposed pattern outperforms existing ABE-based approaches in terms of efficiency and security. [27] The authors advised a secure IIoT framework for efficient resource management in smart manufacturing. The framework uses a lightweight encryption algorithm for secure communication and integrates a blockchain-based consensus mechanism for secure data exchange.

[28] This paper recommends a novel Stern-Brocot-based non-repudiation dynamic provable data possession scheme for cloud storage systems. The proposed scheme ensures both data possession and non-repudiation with high efficiency, low computational complexity, and strong security.

[29] The authors introduced Hy-SAIL, a hybrid approach that combines centralized and decentralized storage architectures to address scalability, availability, and integrity challenges in cloud storage systems. This solution improves performance, reduces communication and computation overhead, and enhances security and data redundancy. [30] The authors suggested a lightweight auditing scheme for cloud storage with deduplication and strong privacy protection. The proposed scheme reduces the overhead of cloud storage auditing while improving the security and privacy of data. [31] The authors introduced a lightweight auditing scheme for cloud storage with deduplication support and strong privacy protection.

The proposed scheme achieves efficient and privacy-preserving storage auditing and significantly reduces communication and computation overheads, making it practical for cloud storage systems. [32] This paper proposes a Li-Fi-based security cloud framework integrating Li-Fi technology with cloud computing and cryptography to provide secure and reliable communication for future IT environments. The framework ensures high-speed and secure data communication.

[33] The authors introduced a DNA cryptography-based encryption technique for securing data storage in the cloud. The method uses DNA sequences as cryptographic keys and genetic operations like splicing and concatenation to generate the keys. [34] This paper proposed a collaborative auditing blockchain framework for cloud storage systems that improves data integrity, accountability, and transparency. The framework ensures confidentiality and privacy by utilizing homomorphic encryption and zero-knowledge proof protocols.

[35] The authors suggested a novel bi-level encrypted multi-cloud secure data management architecture (BE-MCSDMA) for ensuring data confidentiality, integrity, and availability in multi-cloud environments. The proposed architecture employs homomorphic encryption and proxy re-encryption techniques to ensure secure data sharing and access among multiple clouds while preserving user privacy. [36] The authors preferred a secure e-health management system that leverages the integration of IoT and cloud computing technologies.

The system ensures secure and efficient management of health-related data and services while preserving user privacy and confidentiality. [37] The authors recommended a Patients' E-Healthcare Records Management System (PRMS) designed for privacy preservation in third-party cloud platforms. The system ensures that private and confidential user information is maintained while securely storing and managing confidential patient data.

[38] The authors advised an energy-efficient and secure data aggregation scheme for the Internet of Healthcare Things (IoHT) using Fog computing technology. The suggested system (FC-SEEDA) guarantees efficient and secure gathering and aggregating of medical data from diverse IoT.

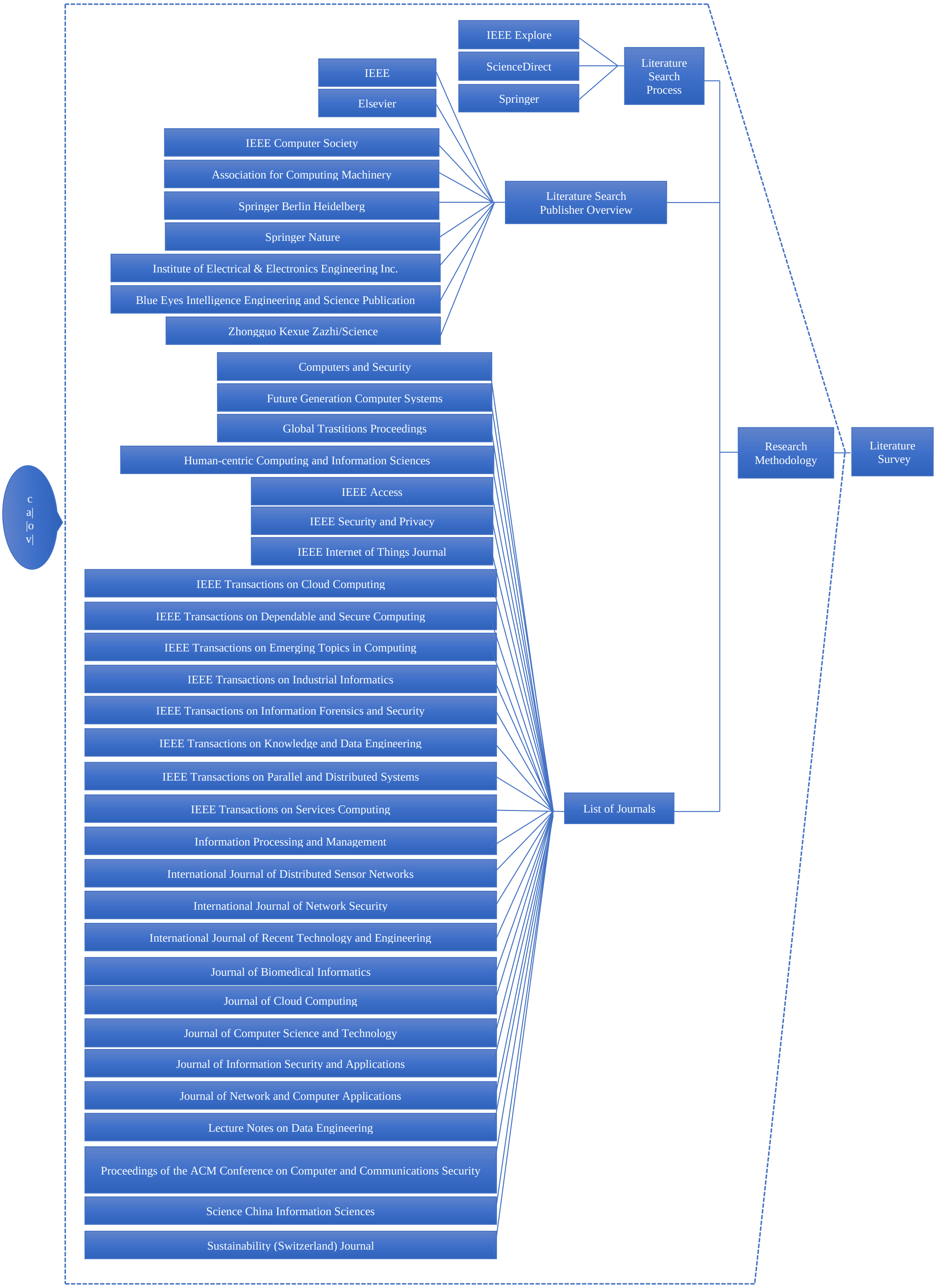

IEEE Explore
ScienceDirect
Springer
Literature Search Process
IEEE
Elsevier
IEEE Computer Society
Association for Computing Machinery
Springer Berlin Heidelberg
Springer Nature
Institute of Electrical & Electronics Engineering Inc.
Blue Eyes Intelligence Engineering and Science Publication
Zhongguo Kexue Zazhi/Science
Literature Search Publisher Overview
Computers and Security
Future Generation Computer Systems
Global Trastitions Proceedings
Human-centric Computing and Information Sciences
IEEE Access
IEEE Security and Privacy
IEEE Internet of Things Journal
IEEE Transactions on Cloud Computing
IEEE Transactions on Dependable and Secure Computing
IEEE Transactions on Emerging Topics in Computing
IEEE Transactions on Industrial Informatics
IEEE Transactions on Information Forensics and Security
IEEE Transactions on Knowledge and Data Engineering
IEEE Transactions on Parallel and Distributed Systems
IEEE Transactions on Services Computing
Information Processing and Management
International Journal of Distributed Sensor Networks
International Journal of Network Security
International Journal of Recent Technology and Engineering
Journal of Biomedical Informatics
Journal of Cloud Computing
Journal of Computer Science and Technology
Journal of Information Security and Applications
Journal of Network and Computer Applications
Lecture Notes on Data Engineering
Proceedings of the ACM Conference on Computer and Communications Security
Science China Information Sciences
Sustainability (Switzerland) Journal
List of Journals
Research Methodology
Literature Survey
c
a|
|o
v|

Fig. 5 Working model of literature survey on mind map tool

3.1. Literature Survey

Table 2. Comparative analysis with main recent research studies

References & Year	Advantages	Limitations
[1] & 2020	Delivers dynamic, efficient, and scalable security solutions for cloud storage.	Involves significant computational and communication overhead.
[2] & 2020	Enables secure and efficient remote data access and sharing with streamlined authentication and authorization processes.	Vulnerable to replay and impersonation attacks.
[3] & 2020	Facilitates secure and efficient multiauthority access control in IoT cloud storage environments.	Scalability may be limited due to the requirement for trusted authorities.
[4] & 2020	Enables secure and efficient cross-platform data sharing through web-based cloud storage using homomorphic encryption.	Due to the high computation overhead involved, this scheme may not be well-suited for large-scale data sharing.
[6] & 2021	Enables secure and energy-efficient transmission of medical data.	Due to resource requirements, it may not be suitable for low-power or limited connectivity environments.
[7] & 2021	Provides dependable and scalable solutions at a reasonable cost.	The discussion is limited to virtualization attacks.
[4] & 2022	Enables efficient, adaptable file sharing with robust data privacy protections.	Requires the establishment of a personal web-based cloud storage solution.
[8] & 2022	Capable of delivering highly secure, scalable, and resilient data solutions.	Photo processing necessitates significant storage space requirements.
[9] & 2020	Provides secure solutions for cloud storage systems.	DFAs can consume larger tables than NFAs.
[10] & 2020	Data owners who have contracted with cloud providers to manage data access and security must be able to do so.	No acceleration strategies exist, and data is costly.
[11] & 2022	Delivers secure multimedia content to users worldwide.	Requires significant storage capacity.
[12] & 2020	Offers a secure solution for data sharing and searching in collaborative storage environments that span the cloud and edge.	The proposed scheme may not be appropriate for large-scale data storage due to its high computational cost.
[13] & 2019	Enables efficient data possession verification in cloud storage environments.	The proposed scheme may not be suitable for scenarios where data requires frequent updates.
[14] & 2019	Delivers secure mechanisms for auditing shared data and storing and accessing EMRs in cloud storage environments through blockchain technology.	More types of audit logs are required.
[15] & 2020	Delivers secure mechanisms for auditing shared data and storing and accessing EMRs in cloud storage environments through blockchain technology.	Additional storage space is necessary.
[18] & 2020	Delivers a secure mechanism for managing keys in data-centric networking environments.	Validation of scalability and effectiveness in various scenarios is necessary.
[19] & 2020	Benchmarking of DSSE schemes is necessary to compare their performance in terms of various metrics such as time and space complexity, search efficiency, and communication overhead.	The study focuses on evaluating and analyzing existing schemes rather than proposing a new scheme.
[20] & 2020	Efficient and adaptable scheme for various applications.	Suggested approach for data encryption is that it may not provide complete protection against certain types of ciphertext attacks.
[21] & 2020	Supports dynamic user revocation and efficient verification.	Assumes the cloud server is honest but curious, leaving the possibility of unauthorized access and manipulation of data.
[22] & 2020	Provides a secure mechanism for ensuring both content privacy and query confidentiality in cloud-based storage and retrieval systems.	Requires significant computational resources and may not be suitable for low-powered devices or systems with limited resources.
[23] & 2020	Provides a comprehensive solution for secure data storage with assured accessibility and confidentiality in a DCS system.	Limited sample size.
[24]&2019	Blockchain technology provides a dependable solution for publicly auditing cloud storage systems, safeguarding against rogue auditors.	Additional storage space is required for effective analysis of the data.

[25] & 2019	It employs a unique arbitration technique to enable real-time photo integrity audits on cloud storage while upholding privacy.	Focused on image files, limiting its applicability to other data types.
[26] & 2020	Allows safe storage, sharing, and retrieval of encrypted cloud data using attribute-based encryption, increasing access control flexibility.	Depends on a trusted authority to oversee the attribute-based access control system, potentially introducing a single point of failure.
[27] & 2020	Proposes a secure and efficient resource management approach for smart manufacturing leveraging the Industrial Internet of Things (IIoT).	One limitation is the lack of description regarding the specific algorithms or methods employed in the framework.
[28] & 2019	Enables users to check the integrity of their cloud-stored data without downloading the entire file.	May not be well-suited for environments with multiple clients or users.
[29] & 2019	Due to its high fault tolerance and efficient data retrieval capabilities, it is well-suited for cloud storage systems.	Demands significant coordination among nodes, potentially resulting in increased system overhead and complexity.
[30] & 2020	Its efficiency and lightweight nature make it well-suited for cloud storage systems.	It may not be suitable for large-scale cloud storage systems.
[32] & 2018	Delivers fast data communication and secure cloud storage capabilities.	It may not be well-suited for environments with low lighting conditions or physical obstructions that hinder light wave transmission.
[33] & 2018	Ensures a high level of data security in cloud storage systems through a robust and secure approach.	DNA cryptography exhibits high computational complexity, which may limit its suitability for real-time systems.
[34] & 2020	Provides a dependable method for safeguarding data integrity in cloud storage systems.	Demands substantial computational resources and poses a challenge due to the high cost of maintaining the blockchain network.
[35] & 2022	Ensures data privacy and security in multi-cloud environments through multi-level encryption and secure data transfer protocols.	Due to the substantial computational requirements and system complexity, maintaining and operating the system can be challenging.
[36] & 2022	Provides a secure and efficient solution for managing e-health data.	Adoption of the solution may be limited in resource-limited settings due to the requirements for substantial resources and expertise.
[37] & 2022	It possesses the capacity to improve both the accessibility and efficiency of healthcare services.	Due to the substantial computational requirements and system complexity, maintaining and operating the system can be challenging.
[38] & 2023	Enables secure and resource-efficient data aggregation, reducing energy consumption and communication overhead in IoT devices.	Limited to small-scale IoT networks, the scalability of the solution requires evaluation.

4. Proposed System

The proposed system aims to enhance the security of E-Healthcare systems in a cloud storage environment. This system incorporates a combination of robust security measures to address concerns related to data protection. Strong encryption is applied to safeguard data and maintain confidentiality. Strict access controls are enforced to allow only authorized data usage, tightly regulating user access. Hash functions are utilized for data validation, ensuring data integrity, and detecting any potential tampering. It also includes admin activity auditing, which monitors and logs administrative actions for added security. By implementing these measures collectively, the proposed system effectively prevents unauthorized access and data leaks, providing a secure cloud storage environment for E-Healthcare data. The focus is on improving the security of cloud computing environments to safeguard healthcare data's confidentiality, integrity, and availability. The ultimate objective is to ensure that patients' sensitive information remains secure and protected. By utilizing this approach, it becomes possible to store and retrieve all electronic medical history data pertaining to a patient, thereby eliminating the need to comb through multiple databases for relevant information. The system's functionality allows both patients and physicians to access and add information to the cloud-based database. It may support cryptographically secure hashing algorithms that provide authentication and data integrity to protect, prevent, and harden data transfer from healthcare providers to cloud storage. Architecture for E-Healthcare clouds with hospital and cloud storage can provide an efficient and secure platform for storing and managing patient data. Here are some points to consider in such an architecture:

- Cloud Storage: Cloud storage can provide a scalable and flexible solution for securely storing large amounts of patient data. Data can be stored in a private cloud, hybrid cloud, or public cloud, depending on the organization's needs and requirements.
- Hospital Network: The hospital network can serve as a gateway between the cloud storage and the hospital's internal systems, allowing for secure data transmission and access.
- Security Measures: To ensure the safety of patient data and safeguard against unauthorized access or cyber-attacks, it is vital to implement robust security measures, including access controls, encryption, firewalls, and intrusion detection systems.
- Interoperability: E-Healthcare clouds should be designed to support interoperability with other healthcare systems and data standards to ensure seamless data exchange and collaboration across different organizations and platforms.
- Analytics and Reporting: E-Healthcare clouds should have tools for analysing and reporting on patient data to enable clinicians to make informed decisions and improve patient outcomes.
- Disaster Recovery: Having a disaster recovery plan in place for cloud storage is crucial to ensure that patient data remains both protected and accessible during any potential disasters or system failures.
- By implementing an architecture for E-Healthcare clouds with hospital and cloud storage, organizations can improve patient data management's efficiency, accuracy, and security.
- While reducing costs and improving patient outcomes. Figure 6 depicts the suggested communication model of E-Healthcare systems. The Communication Model of E-Healthcare systems has the following four entities: Patients, Physicians, nurses, and medicine centres. Patient records are called Electronic Health Records (EHRs), which are kept on the Google Cloud Platform (GCP), a third-party cloud computing platform, and retrieved as needed using a web-based application.
- Let P be the set of patients, where each patient is represented by a unique identifier p_i, where i = 1, 2, ..., n. Let D be the set of doctors, where each doctor is represented by a unique identifier d_j, where j = 1, 2, ..., m. Let C be the set of cloud data centers, where each data center is represented by a unique identifier c_k, where k = 1, 2, ..., p. Let A be the set of associations between patients, doctors, and cloud data centers, where each association is represented by a tuple (p_i, d_j, c_k), indicating that patient p_i's data is stored in cloud data center c_k and is associated with doctor d_j. Then, the set of associations A can be represented in equation format as A = {(p_i, d_j, c_k) | p_i ∈ P, d_j ∈ D, c_k ∈ C}
- In other words, A is the set of all possible combinations of patients, doctors, and cloud data centers. If patient p_i's data is stored in cloud data center c_k and is associated with doctor d_j, then the corresponding tuple (p_i, d_j, c_k) would be included in A. For the purpose of healthcare decision-making and analysis, this representation is used to track patient data, its storage location, and its association with various doctors.
- Incorporating trust and security measures is essential to ensure that data stored in cloud storage is secure and protected. Several security measures can be taken to protect sensitive data, such as patient data stored in a cloud storage system. Firstly, the RSA-CRT algorithm can generate a public and private key pair. Data encryption is done using a public key, which can only be accessed by authorized users possessing the corresponding private key.

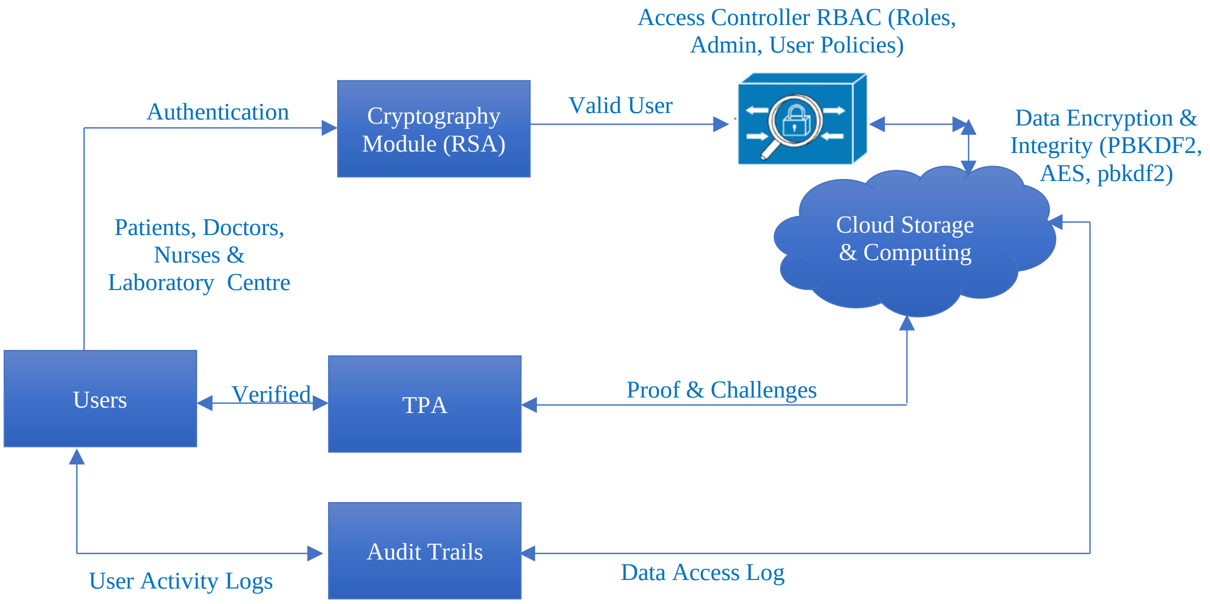

Access Controller RBAC (Roles, Admin, User Policies)
Authentication
Cryptography Module (RSA)
Valid User
Data Encryption & Integrity (PBKDF2, AES, pbkdf2)
Patients, Doctors, Nurses & Laboratory Centre
Cloud Storage & Computing
Users
Verified
TPA
Proof & Challenges
Audit Trails
User Activity Logs
Data Access Log

Fig. 6 Communication model of E-Healthcare systems

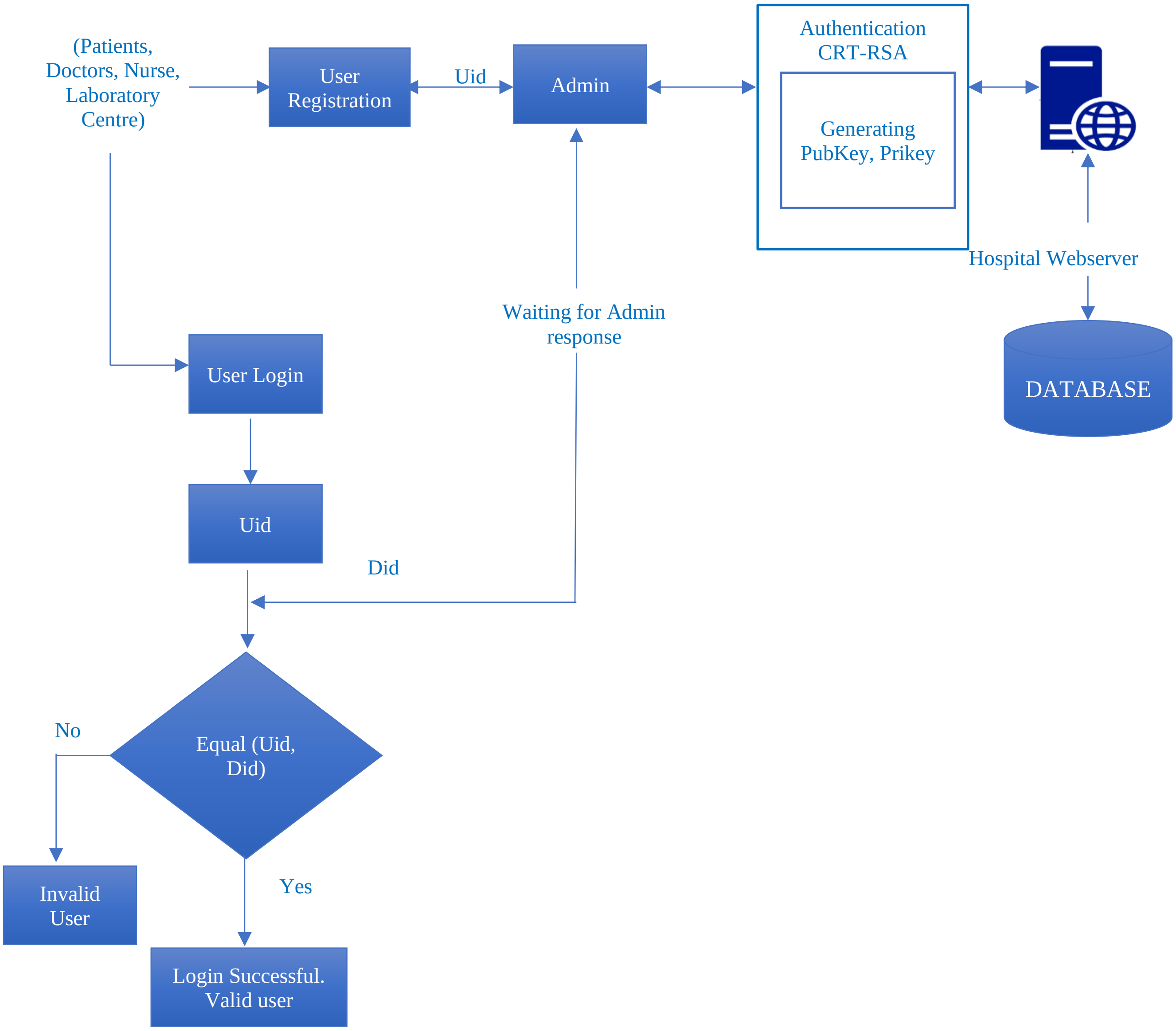

(Patients, Doctors, Nurse, Laboratory Centre)
User Registration
Uid
Admin
Authentication CRT-RSA
Generating PubKey, Prikey
Hospital Webserver
DATABASE
Waiting for Admin response
User Login
Uid
Did
Equal (Uid, Did)
No
Invalid User
Yes
Login Successful. Valid user

Fig. 7 User authentication

- Secondly, role-based access control can be implemented, ensuring only authorized users with the correct permissions can access the data. Thirdly, AES - 256 with PBKDF2 can be used to validate the data and generate a secure hash of the password using Modified SHA 512. Lastly, audit trails can be implemented to track changes and access to the data, providing a record of who accessed the data and what changes were made. These measures work together to ensure patient data remains secure and only authorized users can access it in a cloud storage environment.

4.1. User Authentication

Various techniques can be employed to guarantee the security of patient data in E-Healthcare systems. User authentication has been strengthened by integrating traditional RSA with the Chinese Remainder Theorem (CRT). This has been done to address the factorization problem of traditional RSA and speed up computation when using 3 digits of 5 large prime numbers.

4.2. Access Control

In cloud-based storage systems for e-health, Role Based Access Control (RBAC) is a helpful tool for controlling who has access to patient data. RBAC works by assigning roles to individuals and groups based on their duties and privileges, which helps to limit unauthorized access and enforce compliance requirements. RBAC provides scalability and auditability benefits, making it useful for managing large systems and tracking user behaviour. In an e-health system, RBAC involves managing access to resources, such as patient data, based on user roles and privileges. A user is an individual or entity that requires access to a resource, while a role defines what a user can or cannot do in the system. The resource is the object or data the user is attempting to access, and the operation is the action the user is attempting to perform on the resource. Authorization is the process of determining whether a user has the appropriate privileges to access a resource, while policies are the rules and guidelines used to determine access to resources. To guarantee that only authorised users have access to patient data and that data security and privacy are always maintained, the administration manages roles, privileges, and access control in the system. Administrators can lower the risk of data breaches and unauthorised access by using RBAC to guarantee that only authorised users can access patient data. RBAC can also help with compliance and security audits.

An illustration of Role Based Access Control (RBAC) in an E-Healthcare System can be seen in the code above. Users are given roles and permissions in RBAC according to their responsibilities and rights. The code defines three roles: doctor, nurse, and receptionist, and assigns permissions to them based on their responsibilities. Users are then assigned roles, and access to resources is defined using policies. In this case, the resource is patient data, and the policies define which operations are allowed or denied for each role. Finally, the "authorize" function checks whether a user has the appropriate permissions to access a resource based on their role and the policies defined. This assists in maintaining data security and privacy and ensuring that only authorised users have access to patient data.

Table 3. User's roles and responsibilities

Define roles and permissions	Define users and assign roles	Authorize user to access resources based on their role and permissions

role doctor {
permission READ_PATIENT_DATA;
permission EDIT_PATIENT_DATA;
permission ADD_PATIENT_DATA;
permission DELETE_PATIENT_DATA;}
role nurse {
permission READ_PATIENT_DATA;
permission EDIT_PATIENT_DATA;
permission ADD_PATIENT_DATA;}
role receptionist {
permission READ_PATIENT_DATA;
permission ADD_PATIENT_DATA;}
	user doctorA
	{ role doctor; }
	user nurseB {
	role nurse ;}
	user receptionistC {
	role receptionist;
	}
	// Define resource and access policies
	resource patient_data operation read {
	allow: doctor, nurse, receptionist;
	deny: all;}
	operation edit {
	allow: doctor, nurse;
	deny: all; }
	operation adds {
	allow: doctor, nurse, receptionist;
	deny: all; }
	operation delete { allow: doctor; deny: all; }}
		function authorize(user, operation, resource) {
		if (user.role.permissions contains operation and resource.operation.allow contains user. role) {
		return "Access granted";
		} else {
		return "Access denied";}}

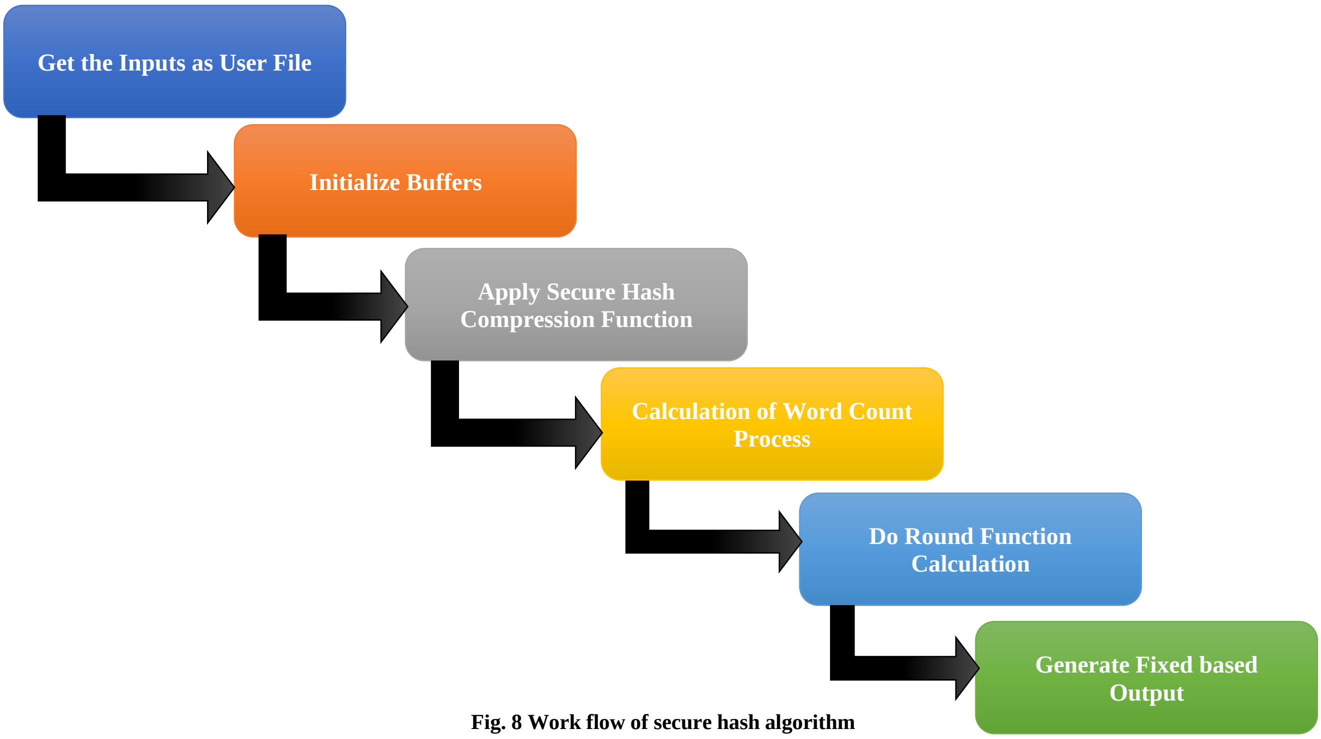

Get the Inputs as User File
Initialize Buffers
Apply Secure Hash Compression Function
Calculation of Word Count Process
Do Round Function Calculation
Generate Fixed based Output

Fig. 8 Work flow of secure hash algorithm

4.3. Data Validation

Data validation is crucial for secure cloud storage. It ensures that data is accurate, complete, and consistent, reducing the risks associated with storing sensitive information. This helps to ensure that patients' data remains secure and reliable over time. By preventing data corruption, ensuring data accuracy, protecting against unauthorised access, and enforcing regulatory standards, it can help assure secure data storage in cloud storage.

This study suggested PBKDF2 with the AES algorithm and SHA 512 as an improved data integrity solution for E-Healthcare systems on public cloud platforms. The proposed solution includes three main components: data integrity verification, data recovery, and a secure communication protocol. The solution is based on a combination of cryptographic techniques, including hashing, key derivation, and encryption. The solution was tested using cloud-based E-Healthcare systems, and the experimental results were analysed.

Using PBKDF2 with the AES algorithm and Modified SHA 512 provided an improved data integrity solution for E-Healthcare systems on the public cloud platform. The proposed solution includes three main components: data integrity verification, data recovery, and secure communication protocol. The solution is based on a combination of cryptographic techniques, including hashing, key derivation, and encryption.

The well-known secure hash technique (SHA-512) is frequently employed for creating keys. This study introduces a modified SHA-512 that improves security by altering how constants are combined in each round. This modification increases unpredictability and prevents attackers from taking advantage of fixed values and variable mixing; a modification incorporating the secret key into round operations and fortifying the algorithm against assaults on known values is a part of this change. The effectiveness of the redesigned method is also evaluated in the study. The experimental findings using a Java tool demonstrate shorter execution times and better defence against brute-force and rainbow table assaults. SHA-512 is a widely used cryptographic hash algorithm that can process input messages of any length and produce a fixed-length hash value or digest 512 bits (64 bytes).

The last 128 bits of the input message are set aside for modulo 2128 of the original input message, and the input message is padded with a certain amount of bits to ensure that its length is a multiple of 1024. The padding bits start out with 1 and then a string of 0s to reach the necessary length. Thus, L = l + p + 128 is the total length of the input to SHA-512, which is then divided into N = L/1024 equal-sized blocks of 1024 bits each. During each cycle, it updates the initialization vectors and represents the resulting SHA-512 hash value as Ht.

4.4. Audit Trails

Audit trails are a crucial tool for e-health cloud-based storage systems to track and monitor user activity and access to patient data. They can help ensure compliance with regulations like HIPAA and prevent unauthorized access to sensitive patient information. Audit trails record and track user activity, including who accessed what data, when, and from where. They can identify potential security breaches or violations of policies and procedures and detect anomalies or suspicious behaviour. By reviewing and analyzing audit trails regularly, administrators can take corrective actions to prevent data breaches and ensure data integrity and confidentiality.

An algorithm for enhancing data integrity Using PBKDF2 with AES algorithm and Modified SHA 512		
Input: Pass the input and data to be safeguarded. **Output:** encrypted data ← $eData$, message digest← md, $RetrievedData$ ←rData,ComputedDigest← cDigest		
1.		Create a function name as secureData with 2 arguments of data, passphrase.
2.	**a.** **b.**	Generate a derived key using PBKDF2. Assign PBKDF2(passphrase) as dKey
3.	**a.** **b.**	Encrypt the data using the derived key and a secure encryption algorithm like AES-256. Assign AES256Encrypt(data, dKey) as $eData$
4.	**a.** **b.** **c.**	Compute a SHA-512 hash of the encrypted data Assign SHA512(eData) as mDigest Return the encrypted data as eData and message digest as mDigest
Now, Consider encrypted data as input for the next step. **Input:** encrypted data, message digest, passphrase **Output**: decrypted data		
1.	**a.**	Create a function name as rData with 3 arguments of eData, mDigest, with a passphrase.
2.	**a.** **b.**	Generate a derived key using PBKDF2. Assign PBKDF2 with one argument of passphrase as dKey
3.	**a.** **b.**	Compute a SHA-512 hash of the decrypted data Assign SHA512(AES256Decrypt(eData, dKey)) as cDigest
4.	**a.** **b.** **c.**	Compare the computed hash with the stored hash. Check if cDigest is equal to mDigest, then return the decrypted data asAES256Decrypt(eData, dKey) Else, the data has been tampered with.

The following steps are taken to ensure user activity:

1. Initialize an audit log to store user activity and access to patient data.
2. For every user action:
   a. Check if the user is authorized to perform the action on the patient data.
   b. Log the action in the audit log, including the user ID (Uid), timestamp (Ts), action performed, and additional details.
   c. If the action was unauthorized, alert the administrator and revoke the user's access if necessary.
3. Regularly review and analyze the audit log for potential security breaches or policy violations.
4. If necessary, take corrective actions, such as revoking access to certain data or tightening security controls.
5. Maintain the audit log and keep track of any potential problems to ensure the integrity and confidentiality of patient data.

5. Experimental Result Analysis

The proposed solution for ensuring data integrity, confidentiality, and availability in E-Healthcare systems on public cloud platforms has been proven effective through experimental results. Sensitive patient information stored and processed in the E-Healthcare systems is successfully protected from unauthorized access, tampering, or corruption. This solution can be easily integrated into existing E-Healthcare systems on public cloud platforms and customized to satisfy the unique security demands of various healthcare organizations. It has been emphasized how crucial it is to have a strong, safe, and error-tolerant system since the beginning of cloud computing infrastructure growth. The integrity of patient data saved on the Google Cloud Platform is guaranteed and assessed using various secure hashing techniques.

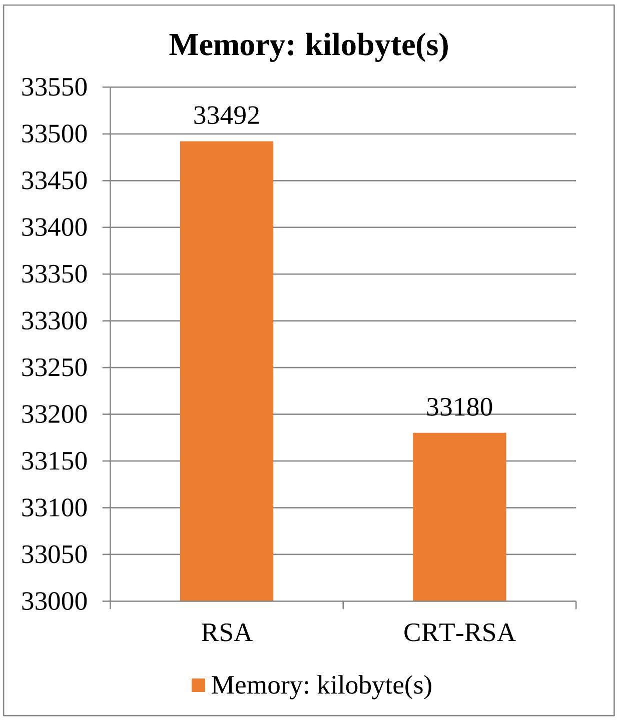


Fig. 9 Shows the memory space (KB) of RSA and CRT-RSA

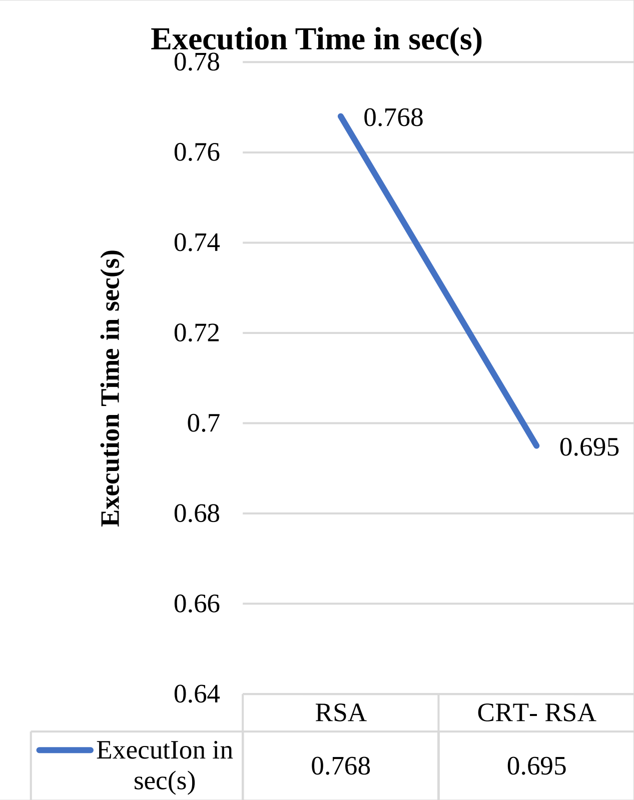


Fig. 10 Shows the execution time (s) of RSA and CRT-RSA

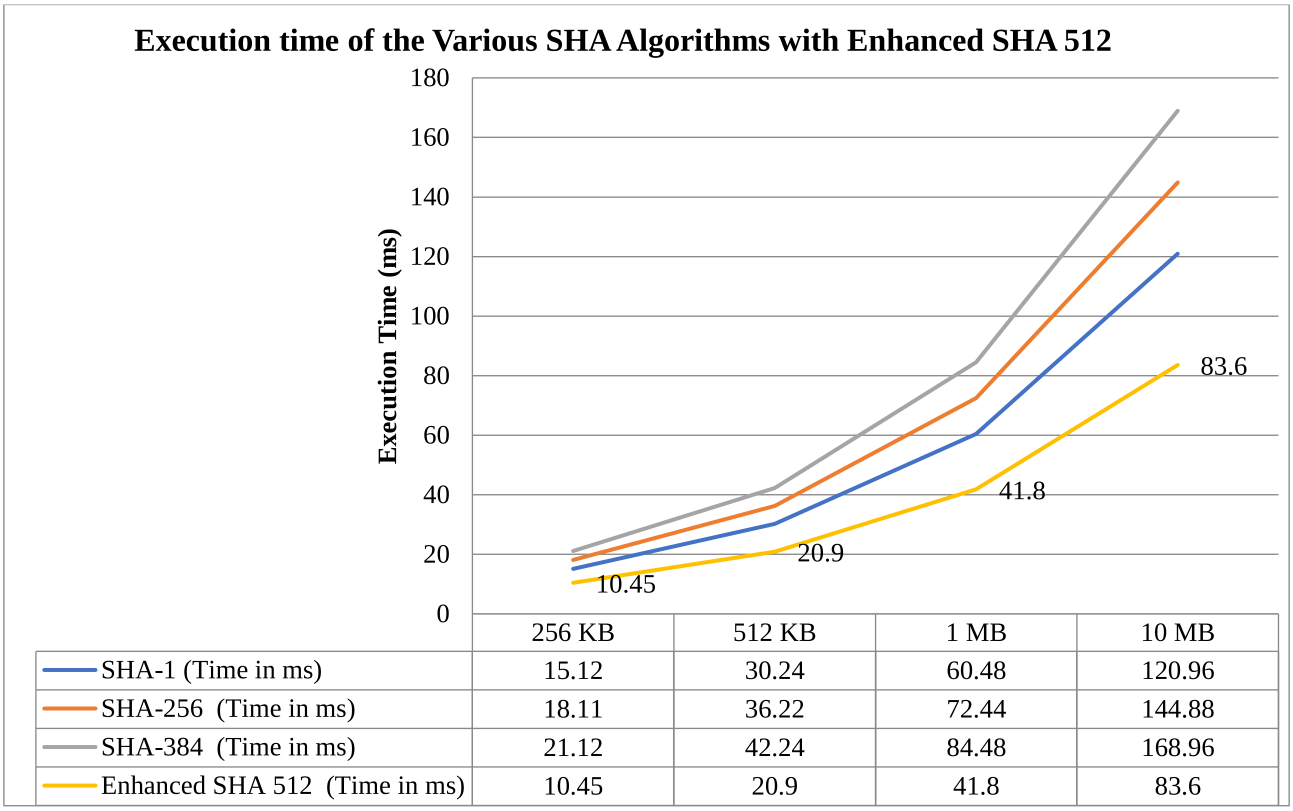
The execution result of the input used in various Secure Hash methods can be seen in the image below.

Table 4 illustrates the time taken to generate hash codes for the current and proposed systems. Based on the table, the proposed method typically generates hash codes within 10.45 to 83.6 milliseconds for data ranging from 256 KB to 10 MB. In contrast, the hash time for existing methods is significantly different from the proposed method. To resist tampering, a method must provide a short compaction time and be more reliable.

However, due to using a more secure hashing algorithm, the proposed method remains faster and more efficient than existing methods. Figure 8 depicts the generation times of the current and proposed systems, which demonstrate that the proposed method generates hash codes faster and provides a highly secure hash code that is resistant to attacks

Table 4. Execution time of various SHA Algorithms with Proposed System

File size		**256 KB**	**512 KB**	**1 MB**	**10 MB**
SHA-1	**Time (ms)**	15.12	30.24	60.48	120.96
SHA-256		18.11	36.22	72.44	144.88
SHA-384		21.12	42.24	84.48	168.96
Enhanced SHA 512		10.45	20.9	41.8	83.6



	256 KB	512 KB	1 MB	10 MB
SHA-1 (Time in ms)	15.12	30.24	60.48	120.96
SHA-256 (Time in ms)	18.11	36.22	72.44	144.88
SHA-384 (Time in ms)	21.12	42.24	84.48	168.96
Enhanced SHA 512 (Time in ms)	10.45	20.9	41.8	83.6

Fig. 11 Execution Times (ms) of the current and proposed systems

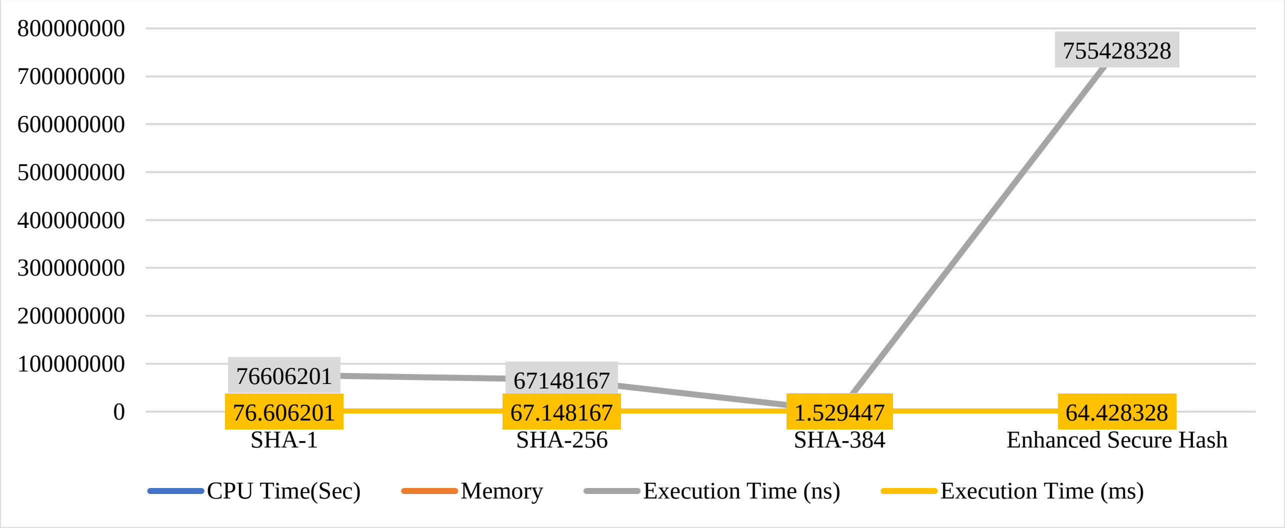


Fig. 12 Performance of security levels

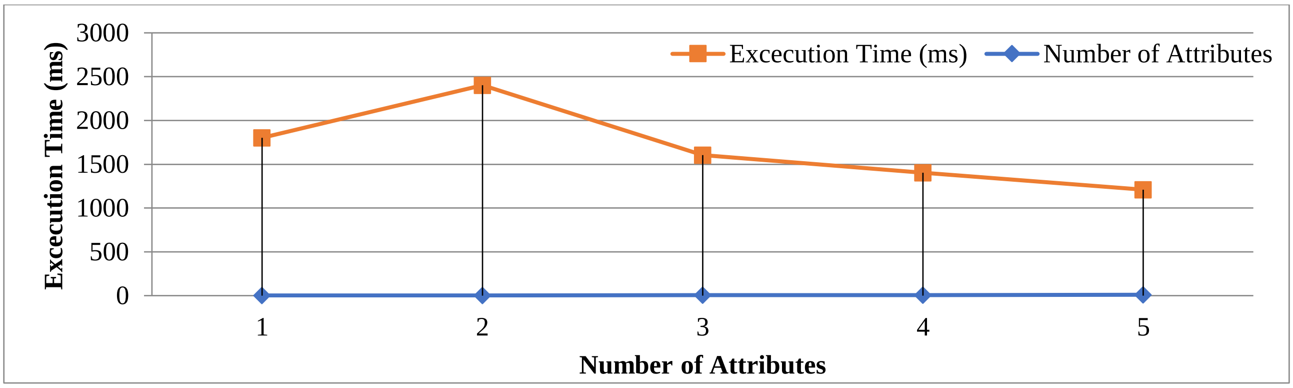


Fig. 13 Execution time of role based access control with various attributes model

6. Conclusion

The high security and secrecy we offer for the patient's personal data is the primary cause of this abrupt transition, which is why the E-Healthcare system is currently expanding very quickly in this era. This proposed system is enhanced to an open software form with requirements like data saving to the cloud and offering external security using cryptography algorithms. This functionality, which is currently available as an online application that we plan to convert to free software and which will primarily be utilized for hospital administrations while also identifying security concerns and holes in the healthcare system, is currently available. Cloud computing still has to be enhanced to secure medical data better and provide secure platforms.

The proposed solution provides a reliable and secure protection mechanism for sensitive patient information stored and processed in E-Healthcare systems. The solution contributes to the advancement of E-Healthcare Information Systems and provides insights for healthcare organizations in adopting secure and reliable cloud-based solutions.

Further research can explore the application of the proposed solution to other cloud-based systems beyond the E-Healthcare systems. This method used and described in this study is very straightforward and is based on user acceptability. More security and automation for users were provided by the approach of secure hash algorithms discussed and implemented using a Java tool on the Google Cloud Platform. The testing results demonstrate that secure hash algorithms offer the best security for password protection against all attacks. This intern will improve security by bolstering defences against a variety of threats.

Abbreviations

IAM	-	Identity Access Management
HSBC	-	Hongkong and Shanghai Banking Corporation Limited
EC2	-	Elastic Compute Cloud
SSE	-	Searchable symmetric encryption
HE	-	Homomorphic Encryption
TPA	-	Third Party Auditor
IBPA	-	Identity-Based Public Auditing
ABSE	-	Attribute-based Searchable Encryption

References

[1] Binanda Sengupta, Akanksha Dixit, and Sushmita Ruj, “Secure Cloud Storage with Data Dynamics Using Secure Network Coding Techniques,” *IEEE Transactions on Cloud Computing*, vol. 10, no. 3, pp. 2090-2101, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Zahid Ghaffar et al., “An Improved Authentication Scheme for Remote Data Access and Sharing over Cloud Storage in Cyber-Physical-Social-Systems,” *IEEE Access*, vol. 8, pp. 47144-47160, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Shuming Xiong et al., “SEM-ACSIT: Secure and Efficient Multiauthority Access Control for IoT Cloud Storage,” *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2914-2927, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Shuzhou Sun et al., “WebCloud: Web-Based Cloud Storage for Secure Data Sharing across Platforms,” *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 1871-1884, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] R. Jeena et al., “A Novel Approach for Healthcare Information System using Cloud,” *International Journal of Recent Technology and Engineering*, vol. 9, no. 6, pp. 189-191, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Fursan Thabit et al., “A New Lightweight Cryptographic Algorithm for Enhancing Data Security in Cloud Computing,” *Global Transitions Proceedings*, vol. 2, no. 1, pp. 91-99, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Qian He, and Hong He, “A Novel Method to Enhance Sustainable Systems Security in Cloud Computing Based on the Combination of Encryption and Data Mining,” *Sustainability*, vol. 13, no. 1, p. 101, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Rajiv Ranjan Suman, Bhaskar Mondal, and Tarni Mandal, “A Secure Encryption Scheme Using a Composite Logistic Sine Map (CLSM) and SHA-256,” *Multimedia Tools and Applications*, vol. 81, pp. 27089-27110, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Yang Yang et al., “Efficient Regular Language Search for Secure Cloud Storage,” *IEEE Transactions on Cloud Computing*, vol. 8, no. 3, pp. 805-818, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Miguel Morales-Sandoval et al., “Attribute-Based Encryption Approach for Storage, Sharing and Retrieval of Encrypted Data in the Cloud,” *IEEE Access*, vol. 8, pp. 170101-170116, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] Ashwani Kumar, “A Cloud-Based Buyer-Seller Watermarking Protocol (CB-BSWP) Using Semi-Trusted Third Party for Copy Deterrence and Privacy-Preserving,” *Multimedia Tools and Applications*, vol. 81, pp. 21417-21448, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Ye Tao, Peng Xu, and Hai Jin, “Secure Data Sharing and Search for Cloud-Edge-Collaborative Storage,” *IEEE Access*, vol. 8, pp. 15963-15972, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] Yang Ming, and Wenchang Shi, “Efficient Privacy-Preserving Certificateless Provable Data Possession Scheme for Cloud Storage,” *IEEE Access*, vol. 7, pp. 122091-122105, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] Yinghui Zhang et al., “Shared Dynamic Data Audit Supporting Anonymous User Revocation in Cloud Storage,’ *IEEE Access*, vol. 7, pp. 113832-113843, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] Hua Wang et al., “An AES-Based Secure Image Retrieval Scheme Using Random Mapping and BOW in Cloud Computing,” *IEEE Access*, vol. 8, pp. 61138-61147, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Rashmi V. Bhat, and Shruti H. Hegde, “A Survey on Applications of Blockchain in Healthcare Sector,” *International Journal of Recent Engineering Science*, vol. 7, no. 3, pp. 36-39, 2020. [Google Scholar] [Publisher Link]

[17] Jin Sun et al., “Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS,” *IEEE Access*, vol. 8, pp. 59389-59401, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[18] Minkyung Park et al., “An SGX-Based Key Management Framework for Data Centric Networking,” *IEEE Access*, vol. 8, pp. 45198-45210, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Yen-Wu Ti et al., “Benchmarking Dynamic Searchable Symmetric Encryption Scheme for Cloud-Internet of Things Applications,” *IEEE Access*, vol. 8, pp. 1715-1732, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20] Chen Shen, Yang Lu, and Jiguo Li, “Expressive Public-Key Encryption with Keyword Search: Generic Construction from KP-ABE and an Efficient Scheme Over Prime-Order Groups,” *IEEE Access*, vol. 8, pp. 93-103, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] Xuqi Wang, Xiangguo Cheng, and Yu Xie, “Efficient Verifiable Key-Aggregate Keyword Searchable Encryption for Data Sharing in Outsourcing Storage,” *IEEE Access*, vol. 8, pp. 11732-11742, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[22] Jung-Shian Li et al., “Secure Content-Based Image Retrieval in the Cloud with Key Confidentiality,” *IEEE Access*, vol. 8, pp. 114940-114952, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] Enrico Bacis et al., “Securing Resources in Decentralized Cloud Storage,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 286-298, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[24] Jingting Xue et al., “Identity-Based Public Auditing for Cloud Storage Systems against Malicious Auditors via Blockchain,” *Science China Information Sciences*, vol. 62, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[25] Xin Tang et al., “Efficient Real-Time Integrity Auditing with Privacy-Preserving Arbitration for Images in Cloud Storage System,” *IEEE Access*, vol. 7, pp. 33009-33023, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[26] Miguel Morales-Sandoval et al., “Attribute-Based Encryption Approach for Storage, Sharing and Retrieval of Encrypted Data in the Cloud,” *IEEE Access*, vol. 8, pp. 170101-170116, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[27] Khaled Ali Abuhasel, and Mohammad Ayoub Khan, “A Secure Industrial Internet of Things (IIoT) Framework for Resource Management in Smart Manufacturing,” *IEEE Access*, vol. 8, pp. 117354-117364, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[28] Junfeng Tian, Guo Ruifang, and Xuan Jing, “Stern-Brocot-Based Non-Repudiation Dynamic Provable Data Possession,” *IEEE Access*, vol. 7, pp. 96686-96694, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[29] Dino Macedo Amaral et al., “Hy-SAIL: Hyper-Scalability, Availability and Integrity Layer for Cloud Storage Systems,” *IEEE Access*, vol. 7, pp. 90082-90093, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[30] Wenting Shen, Ye Su, and Rong Hao, “Lightweight Cloud Storage Auditing with Deduplication Supporting Strong Privacy Protection,” *IEEE Access*, vol. 8, pp. 44359-44372, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[31] Junfeng Tian, and Xuan Jing, “A Lightweight Secure Auditing Scheme for Shared Data in Cloud Storage,” *IEEE Access*, vol. 7, pp. 68071-68082, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[32] Pradip Kumar Sharma et al., “Li-Fi based on Security Cloud Framework for Future IT environment,” *Human-centric Computing and Information Sciences*, vol. 8, no. 23, pp. 1-13, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[33] Sreeja Cherillath Sukumaran, and Misbahuddin Mohammed, “DNA Cryptography for Secure Data Storage in Cloud,” *International Journal of Network Security*, vol. 20, no. 3, pp. 447-454, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[34] Pei Huang et al., “A Collaborative Auditing Blockchain for Trustworthy Data Integrity in Cloud Storage System,” *IEEE Access*, vol. 8, pp. 94780-94794, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[35] Damisetti Veerabhadrarao, G. Apparao, and S. Anuradha, “BE-MCSDMA: BI-Level Encrypted Multi-Cloud Secure Data Management Architecture,” *Journal of Theoretical and Applied Information Technology*, vol. 100, no. 23, 2022. [Google Scholar] [Publisher Link]

[36] Butpheng Chanapha, Kuo-Hui Yeh, and Jia-Li Hou, “A Secure IoT and Cloud Computing-Enabled e-Health Management System,” *Security and Communication Networks*, vol. 2022, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[37] Kirtirajsinh Zala et al., “PRMS: Design and Development of Patients' E-Healthcare Records Management System for Privacy Preservation in Third Party Cloud Platforms,” *IEEE Access*, vol. 10, pp. 85777-85791, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[38] Chinmay Chakraborty et al., “FC-SEEDA: fog Computing-Based Secure and Energy Efficient Data Aggregation Scheme for Internet of Healthcare Things,” *Neural Computing and Applications*, pp. 1-17, 2023. [CrossRef] [Google Scholar] [Publisher Link]