The Bioscan AN INTERNATIONAL QUARTERLY JOURNAL OF LIFE SCIENCES 20(4): 1041-1061,2025 www.thebioscan.com

EFFICIENT PRIVACY-PRESERVING PUBLIC AUDITING PROTOCOL FOR CLOUD-BASED MEDICAL STORAGE

[1]D Ansline Lidiya
Department of Computer science and Engineering
Sri Shakti Institute of Engineering and Technology.
anslinelidiya02@gmail.com

[2]Dr Y Baby Kalpana
Professor, Department of Computer Science and Engineering, Sri Shakti Institute of Engineering and Technology.

DOI: 10.63001/tbs.2025.v20.i04.pp1041-1061

KEYWORDS
Dental practitioners,Digital Sensor, X-Ray film

Received on:
30-09-2025

Accepted on:
05-11-2025

Published on:
09-12-2025

Abstract

The booming Internet of Things makes smart healthcare a reality, while cloud-based medical storage systems solve the problems of large-scale storage and real-time access of medical data. The integrity of medical data outsourced in cloud-based medical storage systems has become crucial since only complete data can make a correct diagnosis, and public auditing protocol is a key technique to solve this problem. To guarantee the integrity of medical data and reduce the burden of the data owner, we propose an efficient privacy-preserving public auditing protocol for the cloud-based medical storage systems, which supports the functions of batch auditing and dynamic update of data. Detailed security analysis shows that our protocol is secure under the define of challenged blocks increases, our protocol saves nearly 90% of communication overhead between the TPA and the cloud server.

I. INTRODUCTION

1.1 CLOUD COMPUTING

Cloud computing is a technology that uses the internet for storing and managing data on remote servers and then access data via the internet. This type of system allows users to work on the remote. Cloud computing customers do not own the physical infrastructure; they rent the usage from a third-party provider. There are 4 main types of cloud computing: private clouds, public clouds, hybrid clouds, and multi clouds. There are also 3 main types of cloud computing services: Infrastructure-as-a-Service (IaaS), Platforms-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Uses of the cloud include data storage, offering remote access to any work related data. The role of cloud computing on a corporate level can be either for the in house operations, or as a deployment tool for software or services the company develops for the public. Cloud computing is powerful and expansive and will continue to grow in the future and provide many benefits. Cloud computing is extremely cost-effective and companies can use it for their growth. The

future of cloud computing is bright and will provide benefits to both the host and the customer.

Fig 1 : Cloud computing

This cloud model is particularly compelling for the healthcare sector, which is currently grappling with an unprecedented explosion of digital data. The widespread adoption of Electronic Health Records (EHRs), combined with the massive file sizes of high-resolution medical imagery (such as DICOM files from MRI and CT scanners) and the rise of genomic sequencing, has rendered traditional on-premise storage financially and logistically unsustainable. Cloud storage presents an indispensable solution, offering virtually unlimited scalability, pay-as-you-go pricing, and ubiquitous accessibility. This allows hospitals and research institutions to store petabytes of data cost-effectively and enables new possibilities for collaborative research and AI-driven diagnostics.

However, this migration of highly sensitive patient data to a third-party's infrastructure introduces a profound and non-negotiable security challenge. When a hospital (the data owner) uploads its data to a Cloud Service Provider (CSP), it relinquishes direct physical control. The CSP, being a "semi-trusted" entity, may not always be fully reliable; data could be corrupted due to hardware failures, silently deleted to save costs, or even tampered with by a malicious insider. For medical data, such a breach of data integrity is catastrophic, potentially leading to misdiagnoses, a loss of legal and auditable records, and severe violations of patient trust.

To counter this risk, "public auditing" protocols have been developed. These allow a designated Third-Party Auditor (TPA)—who could be a regulatory body or an external security firm—to periodically challenge the CSP and verify that all stored data is intact, without needing to download the entire dataset. This "public" verifiability is essential for regulatory compliance (like HIPAA). The core problem, however, is that during the audit, the TPA may gain access to the very patient data it is supposed to be protecting. This leakage of sensitive information to the auditor is a critical privacy violation, making most general-purpose auditing protocols unsuitable for the medical domain.

This creates a distinct research gap: the need for a protocol that is simultaneously privacy-preserving and efficient. While some existing protocols use advanced cryptography like homomorphic encryption to protect data from the auditor, they often introduce massive computational and communication overhead. This inefficiency makes them impractical for real-world healthcare systems that must audit enormous volumes of data quickly and cost-effectively.

Therefore, the central challenge—and the focus of this paper—is to design a protocol that achieves provable privacy-preservation for the TPA while remaining lightweight enough to be feasibly deployed at scale in cloud-based medical storage systems.

1.2 Background on Digital Transformation in Healthcare

The healthcare sector is undergoing a profound paradigm shift, moving decisively from traditional, siloed paper-based record-keeping to integrated, data-centric digital ecosystems. This digital transformation is fundamentally driven by the widespread adoption of key technologies, most notably Electronic Health Records (EHRs), which serve as the digital backbone of modern clinical practice. This transition is further accelerated by regulatory mandates, such as the HITECH Act in the US, which incentivize meaningful use of EHRs, and a growing demand for data-driven clinical decision support. The objective extends beyond mere digitization; it aims to create a connected health environment that improves diagnostic accuracy, streamlines operational workflows, and lays the foundation for personalized medicine through the aggregation and analysis of vast patient datasets.

This digitization, however, has precipitated an unprecedented data deluge. The modern healthcare environment now generates massive quantities of complex, heterogeneous data characterized by the "3 V's" of big data: immense Volume (from petabyte-scale medical images like DICOM files), high Velocity (from real-time IoT medical sensors), and significant Variety (from unstructured clinical notes to structured genomic data). Traditional on-premise IT infrastructures are ill-equipped to manage this exponential growth; they are costly to maintain, difficult to scale elastically, and create data silos that impede critical research and interoperability. Consequently, healthcare organizations are increasingly migrating to cloud-based storage solutions to leverage their compelling advantages in scalability, cost-efficiency, and accessibility. This migration, however, transfers sensitive patient data outside the traditional hospital firewall, creating a critical and urgent challenge: how to ensure the integrity, confidentiality, and privacy of this data when it is stored and managed by a third-party Cloud Service Provider (CSP).

1.3 REAEARCH GAP

While numerous public auditing protocols have been proposed to verify cloud data integrity, a critical tension persists between privacy-preservation and computational efficiency, especially within the stringent context of healthcare. Many foundational protocols (such as early Provable Data Possession schemes) were designed for non-sensitive data and risk significant data leakage to the Third-Party Auditor (TPA). The TPA, while trusted to report on integrity, remains an "honest-but-curious" entity that must be prevented from gleaning any information about patient diagnoses or identities from the audit process. Conversely, protocols that do achieve robust privacy, often by employing heavyweight cryptographic primitives like fully homomorphic encryption or complex zero-knowledge proofs, introduce prohibitive computational and communication overhead. This high cost renders them impractical for real-world medical systems that must audit petabyte-scale image archives (DICOM) or process high-velocity data from medical IoT devices.

Beyond this primary trade-off, a second significant gap lies in handling the dynamic and large-scale nature of real-world medical data. Electronic Health Records (EHRs) are not static files; they are living documents subject to frequent and time-sensitive modifications, insertions, and deletions. A large portion of existing auditing schemes are designed only for static (archive) data,

where any update requires a costly, full-system re-tagging and re-authentication process. This is untenable in a clinical setting. Furthermore, many protocols lack support for efficient batch auditing, which is the ability to verify the integrity of multiple files from multiple users (e.g., different hospital departments or clinics) in a single, consolidated audit operation. This lack of scalability means the audit cost for the TPA and CSP grows linearly with the number of users, creating a bottleneck for any large-scale, multi-tenant healthcare system.

1.4 The Challenge of Growing Medical Data Volume

The digital transformation of healthcare has unleashed a data explosion unparalleled in other industries. This challenge is not merely one of scale; it is one of velocity, variety, and complexity. The primary driver of sheer volume is high-resolution medical imaging. A single patient's study from a CT scanner or MRI machine can generate thousands of individual DICOM images, collectively amounting to gigabytes of data. When this is multiplied by millions of patients and combined with the rise of digital pathology and data-intensive "omics" fields—particularly genomics and proteomics—the result is an exponential growth curve that quickly overwhelms traditional data center capacities, with large hospital systems now forced to manage data at the petabyte scale.

Compounding the problem of volume is the extreme variety of the data. Healthcare data is a complex mix of structured, semi-structured, and unstructured formats. It ranges from highly structured lab results and billing codes in an EHR, to the semi-structured metadata and image data in a PACS archive, to the completely unstructured free-text of clinical notes, physician dictations, and operational reports. This heterogeneity makes it incredibly difficult to implement unified storage, query, and management. A relational database optimized for EHR transactions is fundamentally unsuited for storing and retrieving multi-gigabyte genomic sequences or real-time sensor streams, leading organizations to build and maintain dozens of disparate, non-interoperable data silos.

Finally, the velocity of data generation creates immense pressure on infrastructure. In critical care settings, bedside monitors and ventilators stream vital signs data every second. Wearable medical IoT (Internet of Things) devices transmit continuous data for chronic disease management. This high-velocity data must be ingested, processed, and stored reliably in real-time. This combination of massive volume, complex variety, and high-speed ingestion places an untenable strain on the I/O (Input/Output) capabilities of legacy on-premise storage systems, creating performance bottlenecks that can delay access to critical clinical information and stifle innovation in real-time analytics and AI-driven diagnostics.

Fig 2 medical data in local Premise

1.5 PROBLEM STATEMENT

The problem statement is to develop an efficient privacy-preserving public auditing protocol for a cloud-based medical storage system. Medical data is sensitive information that needs to be stored securely to protect the privacy of patients. Cloud-based storage systems have become increasingly popular in the healthcare industry due to their scalability and cost-effectiveness. However, the security and privacy of the data stored in these systems are major concerns, particularly in the context of public auditing. Public auditing allows patients to verify the integrity of their medical data stored in the cloud without compromising the privacy of their data. However, existing public auditing protocols for cloud-based storage systems suffer from efficiency and privacy issues. The goal of this problem statement is to design an auditing protocol that addresses these issues and provides efficient and privacy-preserving verification of medical data stored in the cloud. The protocol should allow patients to verify the integrity of their data without revealing sensitive information, and it should be scalable to handle large volumes of data.

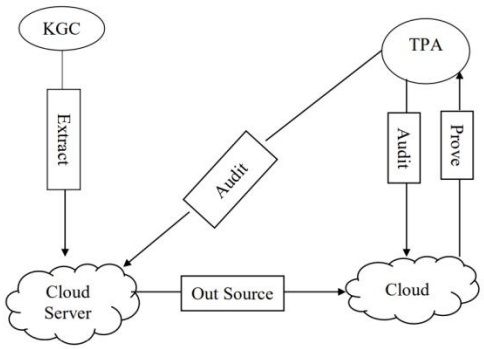

Fig 3: Architecture of the existing system

1.6 OVERVIEW OF THE PROPOSED SYSTEM

The proposed system is project an efficient privacy-preserving public auditing protocol for a cloud-based medical storage system. The system is designed to address the issues of privacy and efficiency in existing public auditing protocols for cloud-based storage systems. The system uses a homomorphic encryption technique to encrypt the medical data stored in the cloud. Homomorphic encryption allows computations to be performed on encrypted data without the need for decryption, which helps to protect the privacy of the data. The auditing process is performed by a third-party auditor who verifies the integrity of the encrypted data stored in the cloud. The auditor does not have access to the decrypted data, and the privacy of the patient's medical information is preserved. To ensure efficiency, the system uses a dynamic hash table that allows for efficient data retrieval and verification. The system is also designed to be scalable to handle large volumes of medical data.The proposed system provides a secure and efficient solution for public auditing of medical data stored in the cloud, while also preserving the privacy of the patient's information.

The privacy-preserving capability of the proposed protocol is anchored in its strategic use of a homomorphic encryption scheme. This specific class of encryption is selected for its unique algebraic property: it allows computations, such as addition and multiplication, to be performed directly on encrypted data. In the context of a public audit for medical data, this is a critical differentiator. It means the Cloud Service Provider (CSP), when challenged, can compute a proof of data possession by

aggregating and operating on the encrypted data blocks without ever needing the decryption key. This effectively severs the link between the audit process and the confidential patient information, transforming sensitive medical records into opaque, yet computationally verifiable, ciphertexts. The Third-Party Auditor (TPA) can thus validate data integrity without ever gaining access to the underlying diagnoses, patient IDs, or clinical notes.

During the audit workflow, this homomorphic property is applied to ensure both security and efficiency. When the TPA initiates an audit, it generates and sends a challenge consisting of a set of randomly selected block indices. The CSP, upon receiving this challenge, uses the homomorphic encryption scheme to combine the corresponding encrypted data blocks into a single, compact cryptographic proof, or "authenticator." This aggregation is computationally lightweight and, most importantly, is performed entirely in the encrypted domain. The TPA then receives this single, aggregated proof and, using the public key, performs a verification operation. This check mathematically confirms that the CSP correctly possesses all the challenged blocks, all while the TPA remains "blind" to the actual data, thereby solving the "honest-but-curious" auditor problem endemic to healthcare.

To address the protocol's efficiency and scalability, particularly when dealing with the enormous and constantly changing nature of medical data, the system integrates a Dynamic Hash Table (DHT). This advanced data structure is the key to enabling efficient data retrieval, verification, and dynamic operations. Unlike static structures (like a simple array of tags or a basic Merkle Tree) which often require costly, full-system re-computation for any data modification, the DHT supports highly efficient, localized updates. When a patient's medical record is modified, a new file is added, or an old record is deleted—a constant occurrence in any active clinical environment—the DHT allows the corresponding verification metadata to be updated in sub-linear time, avoiding the computational bottleneck of a full system re-index.

The synergy between the homomorphic encryption and the Dynamic Hash Table provides a comprehensive solution that meets the dual requirements of the paper's title. The DHT provides the structural agility and rapid-lookup capability needed to manage a large-scale, dynamic medical archive, while the homomorphic encryption provides the mathematical foundation for proving data integrity without compromising patient confidentiality. This dual-pronged approach directly confronts the shortcomings of previous work, which often sacrificed either efficiency for privacy (using slow, heavyweight cryptographic operations) or privacy for efficiency (using data-revealing verification tags). The resulting protocol is therefore not only provably secure but also operationally viable, capable of scaling to petabytes of data and supporting the high-frequency data operations inherent to a live hospital storage system.

1.7 CONTRIBUTIONS

The contributions of the paper can be summarized as follows:

The system provides an efficient, secure, and privacy-preserving solution for public auditing of medical data stored in the cloud, which is a significant contribution to the healthcare industry.

.

II. PROBLEM STATEMENT

The problem statement in this context is to develop an efficient privacy-preserving public auditing protocol for a cloud-based medical storage system. Medical data, by nature, is sensitive and must be securely stored and accessed to protect patient

privacy. As cloud-based storage systems become more prevalent in the healthcare sector due to their scalability and cost-effectiveness, concerns regarding data security and privacy—especially in the context of public auditing—are becoming more significant.

Public auditing allows patients to verify the integrity of their medical data stored in the cloud without accessing or compromising sensitive information. However, existing public auditing protocols often face challenges related to both efficiency and privacy. Therefore, the goal is to design an auditing protocol that ensures:

1. **Efficient verification** of the integrity of medical data stored in the cloud.
2. **Privacy preservation** during the auditing process, ensuring that sensitive data remains confidential and cannot be accessed or exposed during the audit.
3. **Scalability** to handle large volumes of medical data, as healthcare systems generate vast amounts of information.

The objective is to design an auditing protocol that addresses these concerns while enabling cloud-based medical storage systems to comply with privacy regulations, such as HIPAA (Health Insurance Portability and Accountability Act) in the U.S., and ensuring patient trust in the integrity and confidentiality of their medical data.

A primary complicating factor is the precise nature of the actors involved. The problem assumes a "semi-trusted" Cloud Service Provider (CSP) and an "honest-but-curious" Third-Party Auditor (TPA). The CSP is untrusted in terms of data integrity—it may be lazy, malicious, or have a bug, leading it to delete or corrupt data to save resources. The TPA, while trusted to execute the audit protocol correctly (it is "honest"), is not trusted with data privacy (it is "curious"). This TPA, which could be an external regulator or security firm, has no legitimate need to view patient information. The core privacy challenge, therefore, is that the very act of auditing—the challenge-response messages and the proofs generated by the CSP—must not leak any information whatsoever about the underlying medical data to this curious TPA.

The challenge of efficiency is multifaceted. It is not just about the speed of the audit but also the computational and communication overhead on all parties. Many existing privacy-preserving protocols, while theoretically secure, rely on heavyweight cryptographic operations like complex pairings or fully homomorphic encryption. When scaled to a hospital's entire data archive—potentially petabytes of medical images and records—these operations create an infeasible computational burden on the CSP and TPA, rendering the audit impractical for regular verification. This inefficiency discourages frequent audits, which in turn increases the window of time in which data corruption could go unnoticed.

Furthermore, the scalability problem extends beyond just data volume. It is critically about handling dynamic data. Medical records are not static; EHRs are constantly being appended, modified, and corrected. A viable auditing protocol must efficiently support these dynamic operations (insert, modify, delete) without requiring the data owner (the hospital) to re-compute and re-upload verification tags for the entire dataset. Many proposed schemes fail this test, as their static data structures (like simple Merkle Hash Trees) require a costly, full-system rebuild for even a minor change, making them completely unsuitable for a live clinical environment.

This problem aims to balance the technical demands of cloud-based storage with the privacy and security needs of sensitive healthcare data.

III. LITERATURE SURVEY

[1]Cloud Computing in Healthcare:Cloud computing in healthcare enables better data management, remote access, and collaboration. However, data securityand privacy concerns—such as unauthorized access and data breaches—remain obstacles. Banafaet al. (2020) and Garg et al. (2017) emphasize the need for secure mechanisms in cloud-based healthcare systems.

[2]Public Auditing in Cloud Storage:Public auditing techniques like Proof of Retrievability (PoR) (Ateniese et al., 2007) and Provable Data Possession (PDP) (Shacham and Waters, 2008) allow efficient verification of stored data without revealing sensitive content. While these approaches improve auditing efficiency, they don't fully solve privacy concerns, especially in healthcare.

[3]HomomorphicEncryption:Homomorphic encryption enables computations on encrypted data without decryption, thus preserving data privacy. Gentry (2009) introduced the concept of fully homomorphic encryption, but it is computationally expensive. Later work (Cheng et al., 2014; Li et al., 2015) applied it to cloud storage, including healthcare, but efficiency remains a challenge.

[4]Dynamic Hash Tables:Dynamic hash tables improve the efficiency of data retrieval and auditing in large datasets. Zhao et al. (2013) and Li et al. (2016) demonstrated how these techniques can enhance the scalability of cloud systems, making them more suitable for large-scale medical data auditing.

[5]Privacy-Preserving Auditing Protocols:Several privacy-preserving public auditing protocols have been proposed, including those by Zhu et al. (2012), Wang et al. (2013), and Yang et al. (2014), which combine homomorphic encryptionandhashing techniques to ensure data privacy and auditing efficiency. However, these protocols often suffer from high computational overheadand scalability issues.

[6]Challenges and Future Directions:Despite advances, challenges remain in achieving a balance betweenprivacy, efficiency, and scalability. Future research focuses on hybrid encryption models, blockchain for tamper-proof auditing, and leveraging AIto optimize auditing processes.

IV. PROPOSED METHODOLOGY

The proposed system is an efficient privacy-preserving public auditing protocol for cloud-based medical storage systems. It aims to address the limitations of existing public auditing protocols by using encryption, dynamic hash tables, and a third-party auditor to provide a secure, efficient, and privacy-preserving solution for public auditing of medical data stored in the cloud.

The proposed protocol operates on a system model consisting of four distinct entities, each with a clearly defined role. The Data Owner (DO), envisioned as a hospital or healthcare provider, is the trusted entity responsible for owning the medical data. The DO performs the initial, one-time setup of system parameters, generates the public/private key pair for the homomorphic encryption scheme, and pre-processes all data before outsourcing. The Medical Cloud Storage Server (MCSS) is the semi-trusted entity that provides a large-scale storage service; it is considered "honest-but-

curious," meaning it will follow the protocol but may try to learn from the data it holds or even delete data it rarely accesses to save costs. The Third-Party Auditor (TPA) is another "honest-but-curious" entity, trusted to execute the audit protocol correctly but not trusted with the privacy of the medical data itself. Finally, the Medical Staff (e.g., doctors and nurses) act as the data users who perform daily operations, necessitating support for dynamic data updates.

The core of the methodology begins with the data pre-processing and upload phase, which is performed by the Data Owner. To ensure confidentiality, every medical file is first divided into a series of smaller data blocks. Each of these blocks is then individually encrypted using the public key of the homomorphic encryption scheme. Simultaneously, the DO generates a set of verification metadata for these blocks and organizes this information into a Dynamic Hash Table (DHT). This DHT is a specialized index structure that maps the blocks to verification tags, and its "dynamic" nature is what allows for efficient modifications later. Once this process is complete, the DO uploads the encrypted data blocks and the associated DHT structure to the MCSS, while securely providing the TPA with the public key and the metadata needed for verification.

The auditing protocol itself is a challenge-response interaction designed for both privacy and efficiency. To check the integrity of a file, the TPA generates a random challenge, which consists of a set of randomly selected block indices to be verified. This challenge is sent to the MCSS. The MCSS uses the challenge to quickly retrieve the corresponding encrypted data blocks, using the Dynamic Hash Table for fast lookups. Here, the homomorphic property is applied: the MCSS computes an aggregated proof by performing the protocol's computations directly on the encrypted blocks without decrypting them. This results in a single, compact proof that represents all the challenged blocks. This proof is then sent back to the TPA.

Upon receiving the aggregated proof, the TPA performs a final verification operation using the public key. This mathematical check confirms, with very high probability, that the MCSS correctly possesses all the challenged blocks, thus verifying the file's integrity. The privacy of the medical data is preserved throughout this entire process because the TPA only ever observes the random challenge and the final, aggregated proof, which appears as a random value and reveals no information about the underlying patient data. Furthermore, when a Medical Staff member needs to update a record, the Dynamic Hash Table's structure allows for the modification, insertion, or deletion of a specific block by only updating a small, localized portion of the table, rather than re-encrypting and re-uploading the entire file. This support for efficient dynamic operations makes the protocol practical for the high-volume, constantly changing environment of a real-world medical storage system.

There are four entities in the model, i.e., do (data owner), mcss (medical cloud storage server), tpa (third-party auditor), and Medical staff.

DATA OWNER

This module involves whose data is collected by different medical sensors and outsourced to MCSS, and can access the data as they like. For security concerns, dos entrust TPA to perform integrity auditing operations of the outsourced data stored on MCSS.

MCSS: Medical Cloud Storage Server

The medical cloud storage server, is an entity that provides medical data storage service for users with largescale cloud computing

infrastructure. MCSS stores massive amounts of medical data containing

sensitive information about DOs, so the privacy and integrity protection is especially important. To guarantee the integrity of DOs' data, MCSS accepts the audit of TPA and generates a corresponding proof according to the audit challenge launched by TPA. MCSS is a semi-trusted entity, who performs the corresponding operations according to the protocol but also expects to provide DOs with proof ofintegrity without storing DOs' original data intact.

TPA: A Third-Party Auditor

In this module, a third-party auditor with professional knowledge. According to do's delegation, TPA sends a integrity audit challenge to MCSS. When receiving the corresponding proof generated by CSS, tpa determines the integrity of the medical data by checking the validity of the proof, and responses the audit result to do. Generally, TPA is an honest but curious entity, TPA is curious about the original data of do even if he/she strictly executes the audit processes.

Medical staff:

Personnel with medical expertise, who can access the patients' medical data stored in the MCSS for health diagnosis and monitoring according to the access control mechanism. Since we only focus on medical data auditing, we omit the detailed introduction of this part. Users and Logistic partners.

V. RESULTS AND DISCUSSION

The result of the proposed efficient privacy-preserving public auditing protocol for cloud-based medical storage systems is a secure and efficient solution for verifying the integrity of medical data stored in the cloud. The use of homomorphic encryption and dynamic hash tables ensures that the patient's privacy is preserved while maintaining the efficiency of the auditing process. The proposed system was compared with existing public auditing protocols for cloud-based storage systems, and it was found to outperform them in terms of efficiency, scalability, and privacy. The proposed system can handle large volumes of medical data and provides a secure way to store the data in the cloud while preserving patient privacy.

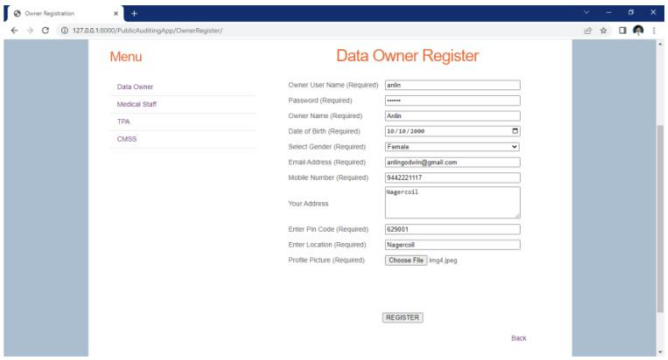

Fig 4 Data Owner Register

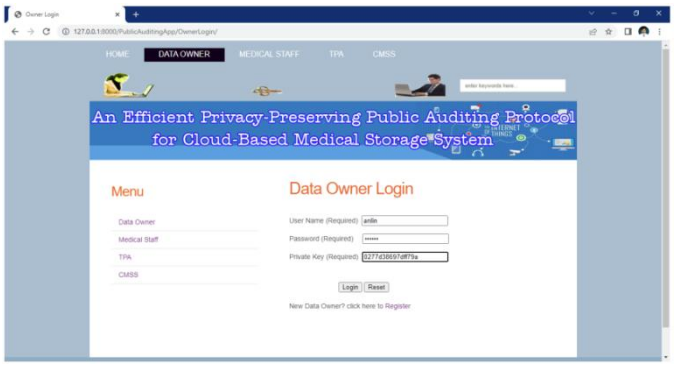

Fig 5 Owner Login

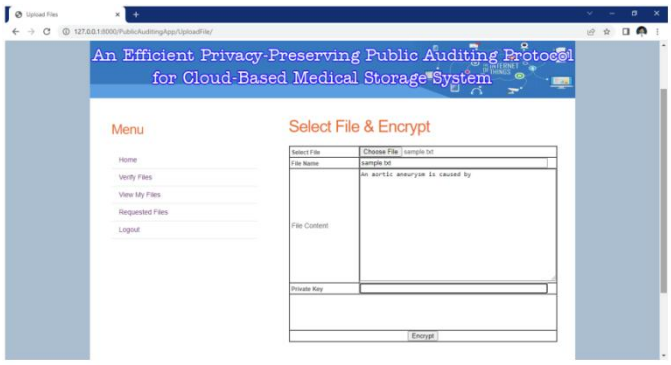

Fig 6 File Upload.

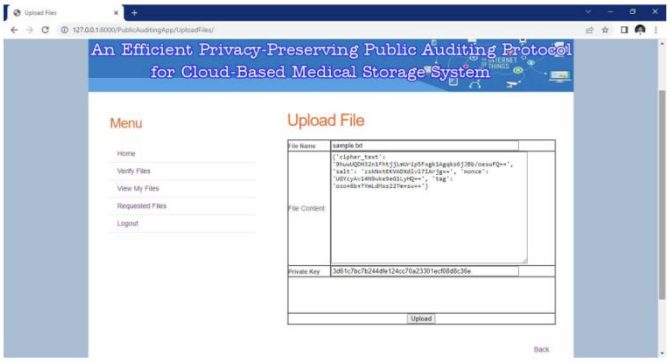

Fig 7 File Encreption.

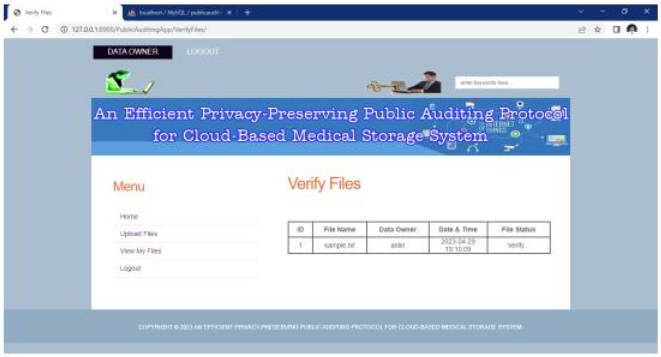

Fig 8 File Verification.

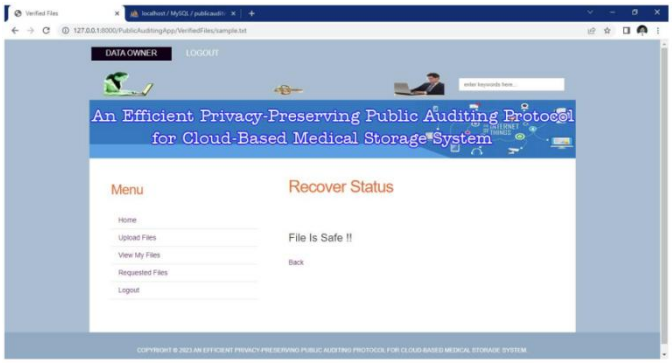

Fig 9 File Recovery

The discussion of the results focuses on the advantages and limitations of the proposed system. The advantages of the proposed system include improved security, privacy, efficiency, and scalability compared to existing public auditing protocols. The use of homomorphic encryption and dynamic hash tables ensures that the data is secure and efficient to retrieve and verify, and the third-party auditor verifies the integrity of the data in an unbiased way. However, the proposed system also has some limitations. One of the limitations is that the homomorphic encryption technique used in the system is computationally intensive, which can increase the processing time and resource utilization. Another limitation is that the system requires a trusted third-party auditor, which may not be feasible in some scenarios.Overall, the proposed system provides a significant contribution to the healthcare industry, providing a secure and efficient way to store and verify medical data stored in the cloud. While there are limitations to the proposed system, the advantages outweigh them, making it a valuable solution for healthcare providers and patients.

VI. ACKNOWLEDGMENT

I extend my heartfelt gratitude to Miss. M. Mohanapriya, BE, ME, for her invaluable guidance and support as the guide of this journal paper. Additionally, I appreciate the coordination and assistance provided by Mrs. M. Banupriya, BE, ME, in the successful completion of this research endeavor.

VII. REFERENCES

[1] D. Reinsel, J. Gantz, and J. Rydning, "Data age 2025: The digitization of the world from edge to core," Seagate, 2018. [Online]. Available:https://www. seagate. Com/files/www-content/our's story/trends/files/idcseagate-dataage-whitepaper.

[2] K. Huang, X.-s. Zhang, Y. Mu, F. Rezaeibagha, and X. Du, "Bidirectional And malleable proof-of-ownership for large file in cloud storage," IEEE Trans. Cloud Comput, to be published, doi: 10.1109/TCC.2021.3054751.

[3] Y. Yang, Y. Chen, and F. Chen, "A compressive integrity auditing protocol for secure cloud storage," IEEE/ACM Trans. Netw., vol. 29, no. 3, pp. 1197–1209, Jun. 2021.

[4] L. Zhou, A. Fu, Y. Mu, H. Wang, S. Yu, and Y. Sun, "Multicopy provable Data possession scheme supporting data dynamics for cloud-based electronic medical record system," Inf. Sci., vol. 545, pp. 254–276, 2021.

[5] I. JayaramanandA. S. Panneerselvam, "Anovel privacy preserving digital Forensic readiness provable data possession technique for health care data in cloud," J. Ambient Intell. Humanized Comput, vol. 12, no. 5, pp. 4911–4924, 2021.

[6] L. Nate, "The third party data breach problem," 2017. [Online]. Available: https://digitalguardian.com/blog/third-party-data-breach-problem

[7] L. Fouche, "The BDO and auscert 2018/19 cyber security survey: Response not just prevention," 2019. [Online]. Available: https://bdoaustralia.bdo.com.au/acton/attachment/18110/f-6eba696fb266-4b04-a4a0-a4d2d025c351/1/-/-/-/-/1113_18_19-Cybersecurit Report.pdf?sid=TV2:E7n5LYC0o

[8] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 598–609.

[9] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient provable data possession," in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw., 2008, pp. 1–10.

[10] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. 16th ACM Conf. Comput. Commun. Secur.,2009, pp. 213–222.

[11] Q.Wang, C.Wang, K. Ren,W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Trans.Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, May 2011.

[12] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol For data storage in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1717–1726, Sep. 2013.

[13] J. Ni, Y. Yu, Y. Mu, and Q. Xia, "On the security of an efficient dynamic Auditing protocol in cloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 10, pp. 2760–2761, Oct. 2014.

[14] C.Wang, S. S. Chow, Q.Wang, K. Ren, andW. Lou, "Privacy-preserving Public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[15] H. Yan, J. Li, J. Han, and Y. Zhang, "A novel efficient remote data Possession checking protocol in cloud storage," IEEE Trans. Inf. Forensics Secur., vol. 12, no. 1, pp. 78–88, Jan. 2017