Protecting Individualized Education and Therapy Records Via Two-Tier Integrity Verification in Distributed Educational Systems

Prasanna Guduru[1,*], K. Vijaya Lakshmi[2], Sumit Gupta[3]

[1]Research Scholar, Department of Computer Science, Sri Venkateswara University, Tirupati, Andhra Pradesh, India. Email: prasanna.guduru@gmail.com, Orchid id : 0000-0003-1186-9935

[2]Professor, Department of Computer Science, Sri Venkateswara University, Tirupati, Andhra Pradesh, India. Email: vijayalakshmik4@gmail.com, Orchid id : 0009-0008-7069-8025

[3]Director, R&D Department, DeepCognix AI Labs, Bangalore, Karnataka, India. Email: sumit@deepcognix.com, Orchid id : 0009-0007-4766-3468

*Corresponding Author: Prasanna Guduru, Email: prasanna.guduru@gmail.com

HOW TO CITE:

Prasanna Guduru, K. Vijaya Lakshmi, Sumit Gupta (2026). Protecting Individualized Education and Therapy Records Via Two-Tier Integrity Verification in Distributed Educational Systems. International Journal of Special Education, 41(5s), 386-401.

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors. Open access publication underthe terms and conditions of the Creative CommonsAttribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

ABSTRACT:

As special education and disability support services become more digitized, the use of distributed systems for storing individualized education plans (IEPs), therapy records, behavioral assessments and assistive intervention data has grown. While frameworks currently use encryption and access control, there are threats to data integrity during the data restoration process that are less addressed, including cases of manipulation of data during reconstruction, silent corruption of the ciphertext, and fragment tampering. This corruption can affect the continuity of education as well as disability support services for persons with disabilities. In this paper, the concept of Two-Tier Integrity Verification Unit (IVU) for secure restoration of Distributed Educational Records is proposed. The framework does deterministic cryptographic integrity verification at two points before decrypting. Tier 1 uses a hash function, SHA-256, on each individual piece of ciphertext to prevent corrupt data and unauthorized changes from affecting the storage-node level. Tier 2 verifies the integrity of the reconstructed cipher text, to detect fragment reordering and reconstruction boundary attacks that fragment level verification would not detect. Only if both the verification steps are passed, will the decryption be carried out. Evaluation on a synthetic educational-support dataset showed that the overhead for total IVUs is 43.0 ms for a 10 MB dataset, while detecting tamper is effective. The proposed framework ensures integrity assurance in limited time to minimal duration of restoration, enabling secure and trustworthy management of distributed educational and therapy records of people with disabilities.

Keywords: Educational Data Integrity, Two-Tier Integrity Verification, Individualized Education Plans (IEPs), Secure Data Restoration, Ciphertext Fragment Verification.

1. Introduction

The swift adoption of educational and disability support services has revolutionized the way Individualized Education Plans (IEPs), therapy records, behavior assessments, assistive intervention reports and multidisciplinary learner documentation are managed (Shivashankar & Bakthavatchaalam, 2024). Distributed digital systems are becoming more and more popular for storing and transferring learner data between geographically dispersed settings in rehabilitation facilities, educational institutions, therapists, and special educators. These serve to increase accessibility, to facilitate collaborative planning of intervention, and to provide continuity for educating and intervening with individuals with disabilities. As the reliance on distributed educational infrastructures has grown, however, the security and integrity of sensitive learner information (Sinan et al., 2024) are also becoming serious concerns.

Recent attacks on educational and public-service systems have shown that when records are compromised, there are impacts beyond disruption to the organization. For disability support environments, inaccurate and incorrect educational records could lead to wrong accommodations, discontinue therapy services, assess learners incorrectly, and not provide individual accommodations (Lovett, 2020). Disability support documentation impacts individual instructional plans, allocation of assistive technologies, scheduling of therapies, and decisions about behavior intervention, and differs from traditional academic records. Thus, maintaining the integrity of educational records distributed from one place to another is very important for the provision of continuous and reliable support services for individuals with disabilities.

Much effort has been devoted to the use of cryptographic methods for securing data storing systems in the education field and cloud computing. Because of its computational efficiency and proven security features (Upadhyay et al., 2026), symmetric encryption algorithms, like Advanced Encryption Standard (AES) are widely used. Recent works have also enhanced the confidentiality and access control mechanisms using hybrid encryption schemes (Garigipati et al., 2026), blockchain based architecture (Palkar et al., 2026), and distributed cloud security mechanism (Rohollahi et al., 2026). These strategies enhance the protection of data that is restored from distributed storage and assume that the data is structurally safe when restored from the distributed storage, but the approaches are not comprehensive. The assumption is flawed under the distributed model where the records are encrypted and stored at several storage nodes before being decrypted.

With distributed educational storage systems, the fragments of ciphertext can be modified while being stored or retrieved, such as being altered, corrupted, replaced or reordered. In general, existing systems reconstruct and decipher without any effort to validate the integrity of the reconstructed ciphertext independently (Ayare et al., 2025). In this regard, bad encrypted information can still be decrypted and handed over to educators or therapists without any indication that there was a problem. This unchecked corruption can have a negative impact on education decision-making and educational disability services. In this sense, the problem of integrity assurance becomes a key concern, albeit overlooked, in the restoration phase of secure educational data management.

In a distributed system, hash-based verification techniques offer an effective way to prevent unauthorized changes from occurring. The National Institute of Standards and Technology (NIST) has standardized a cryptographic hash function, called SHA-256, which is widely used for integrity verification purposes and is collision resistant (Syed, 2025). Systems can check for data changes without exposing plaintext by recomputing hashes and comparing the results. Although SHA-256 is applicable in a distributed verification, the implementation of fragment level and reconstruction level integrity validation before decryption is still not sufficiently explored in educational data storage systems.

In this paper, we introduce a Two-Tier Integrity Verification Unit (IVU) to fill this gap in order to protect distributed therapy and educational records. The proposed IVU can be used as an independent

verification unit in between data retrieval and decryption. Tier 1 is used to verify each piece of the ciphertext by using SHA-256 to detect fragment substitution and silent corruption attacks. Tier 2 checks the integrity of the reconstructed ciphertext before decryption in order to identify attacks such as attacks on the boundaries for the reconstructed text, and attacks that reorder the fragments. Decryption will be permitted only if both the verifications are passed. Any inconsistencies at either stage will result in a NO restoration.

The proposed framework helps secure and trustworthy handling of distributed educational record for people with disabilities. The key contributions of this work are summarised as follows:

- The Two Tier Integrity Verification Unit (IVU) is intended to be an independent architectural element for the secure restoration of distributed educational and therapy records.
- To mitigate attacks such as fragment substitution, silent corruption, fragment reordering and reconstruction boundary misalignment, a SHA-256-based fragment-level and reconstruction-level verification mechanism is proposed to be performed before decryption.
- The tamper detection capability and computational overhead are evaluated in experimental evaluations that use a synthetic educational-support dataset with IEP and therapy-record structures.
- The existing distributed educational data security methods show weaknesses in two-tier integrity verification for restored encrypted records, which is a non-deterministic process.

The rest of the paper is organized as follows. The literature review and research gap analysis is provided in Section 2. A proposed framework, called IVU (Integrated Vehicle and Urbanization), and the system architecture are described in Section 3. The experimental setup and evaluation methodology are introduced in section 4. The results and comparison of the study are discussed in Section 5. Lastly, Section 6 summarizes the paper and presents future research directions.

2. Literature Review

Digital technologies have become more popular in the special education and disability support workplace, thus changing the way that individualized education plans (IEPs), therapy reports, behavioral assessment, assistive intervention records, and multidisciplinary learner documentation are managed. Digital records enhance engagement between educator, therapist, psychologist and caregivers; and aid in the continuity of services for individuals with disabilities. As the distributed educational infrastructures gain in importance, however, the confidentiality, accessibility, reliability and integrity of the records are also becoming a concern. Research in special education has always placed a high priority on the importance of IEP and related support documents to ensure that students with disabilities receive legally mandated, individualized and evidence-based educational services (Kouo et al., 2024).

Blackwell and Rossetti emphasized that IEP systems are an integral part of special education and educational planning, and impact teaching and learning, learning accommodations, and resource allocation for millions of students with disabilities (Blackwell et al., 2014). Likewise, the quality and uniformity of IEP documentation has been seen to impact students' educational outcomes and service provision when they have learning disabilities (McKenna et al., 2024). In addition, Kouo et al. (2024) argued for the need for proper and personalised educational record systems to ensure effective provision of related services, as well as statutory systems for supporting individuals with disabilities. These results indicate that information from educational records in special education settings is more than documents of administration, it is an important decision making resource that impacts on the learner's support and intervention..

In recent years, important governance and accountability issues have also emerged in inclusive education systems, with regard to digital records. Oloto and Yeboah developed a conceptual models

of risks to documentation systems in special education and found that the lack of consistency in data practices, reporting requirements, and validation processes do pose significant risks to educational accountability and service reliability (Oloto & Yeboah, 2025). Peters has coined the term "dirty data" about educational records and explained how inaccurate, incomplete or manipulated educational information may negatively impact the marginalized student and the learner with a disability (Peters, 2022). The research also suggested that the issue of educational data integrity is strongly related to fairness and student opportunity, as well as adherence to privacy laws, like FERPA.

Discussing about disability-support and behavioral intervention service delivery, Ahmed and Yuan mentioned that the digital service delivery environments are increasingly relying on electronic communications, cloud-based reports, teletherapy and distributed storage systems (Ahmed & Yuan, 2026). Cavalari et al. (2014) spoke about the increasing integration of electronic records in service provision and supervision and outlined some of the challenges of securely managing digital records in practice and regulations. The study highlighted the need for better integrity assurance and governance for electronic records where the content is critical to the privacy of the individual's behaviour and therapy information, so that it can be better protected from being altered by unauthorized parties or inconsistencies between records.

In the field of special education, quality of accountability and documentation is a major concern, while in the field of technical security research, confidentiality and control of access in distributed digital systems are of major concern. In order to safeguard any sensitive records, they are commonly encrypted using algorithm encryption like AES as it is fast and has proven to be effective. There are a number of studies that suggest innovative hybrid encryption models, blockchain-based architectures and distributed cloud security models for securing electronic records (Rezaeibagha et al., 2015). Fernández-Alemán et al. found that the general research areas that have been studied most in the field of electronic record security systems (ERSS) are access control, authentication and privacy preservation (Fernández-Alemán et al., 2013). Likewise, recent systematic reviews conducted on the security of EHRs highlighted the importance of role based and attribute based access control as frequent solutions to safeguard sensitive distributed data (Cobrado et al., 2024).

The privacy, interoperability and secure distributed data management issues have also been the subject of research in the field of electronic record systems. The authors of Tertulino et al. pointed out several ongoing issues in the field of ensuring privacy and security in electronic record systems while also ensuring system performance and interoperability (Tertulino et al., 2024). Almaghrabi and Bugis also found that as more and more information about services is becoming digital, electronic record systems are becoming more susceptible to unauthorized use and data breaches (Almaghrabi & Bugis, 2022). This research taken as a whole suggests a greater need for improved security of educational records and cybersecurity of therapy records in the digital age.

This has been of special significance when encrypted information is spread out and stored at various locations. Current security systems typically leave it to the system to detect that the data that is retrieved from distributed storage is structurally correct, and they do not assume that the data will be structurally correct in the event of recovery. In distributed systems, however, this is not always true because the ciphertext may get corrupted, substituted, reordered or even structurally changed, during storage and retrieval. Data integrity is also a key requirement with electronic record systems as inaccurate or incomplete records could affect the quality of services and service reliability (Vimalachandran et al., 2018). Although there has been concern around these issues, most of the existing research work concentrates mainly on the issues of confidentiality, privacy and access management, but not on the verification of deterministic integrity before decryption.

The management of secure educational and therapy records is now even more complicated, due to the use of advanced distributed systems and deep learning record infrastructures. The past few years

have witnessed a growing trend toward distributed electronic record systems (Xie et al., 2021) and deep representation learning, which increasingly make use of a set of digital data sources that are fragmented and heterogeneous. These technologies can enhance scalability and intelligent use of the data, but can also expose the end user to unnoticed corruption, reconstruction issues, and integrity problems that can occur throughout a distributed restoration process.

There is some common thread throughout the literature reviewed. The importance of learner documentation that is reliable, individualized and accurate is a key focus of research in the special education field, whereas technical security research is primarily focused on security for access to and confidentiality of the learner. But practically little work has been focused on the verification of integrity of the records in the context of educational and therapy records restoration in a distributed manner. Most current methods do not have the ability to perform a pre-decryption check that can validate the correctness of each individual block of ciphertext, and/or the reconstructed ciphertext, without relying on the decryption process itself, before restoration is allowed.

Hence, there is a large research gap in making the integration of distributed educational record systems and independent two-tier cryptographic integrity verification process. This work is aimed to fill this gap and introduces a Two-Tier Integrity Verification Unit (IVU) in distributed education and therapy-record systems (EDTRS). The proposed framework does as much as two-way verification of the integrity of the fragments, as well as of the reconstruction, before decrypting the record and rejecting corrupted or manipulated records, before they are even delivered to the educator, therapist, or disability-support professional.

3. Proposed IVU Design

3.1 System Overview

The proposed plan has three stages. Phase I is a set up of system parameters that helps generate an encryption key with AES-256. Phase II is for data owner operations, such as making data pseudonymous, encrypting the data, creating a master hash, dividing the data into fragments, hashing each fragment, storing the fragments across a provider and a DHT network and assigning an SDO lifecycle. In Phase III implements the distributed storage layer and the Integrity Verification Unit (IVU). The IVU is a contribution, a two-level verification phase that is placed between the retrieving phase and the decrypting phase. As shown in Fig.1, proposed IVU-Based Secure Distributed Medical Data Storage Framework is presented.

The Integrity Verification Unit is a part that works on its own. It is isolated from sections of the system. IVU does not provide any information to the encryption part, the access control part or the storage management part. The Integrity Verification Unit has the ability to make sure the encrypted text that needs to be decrypted as exactly the same as the encrypted text that was recorded at the end of Phase II. The task of Integrity Verification Unit checks the encrypted text to make sure it is correct or not and to provide encrypted text's safe and has not been changed. The supporting infrastructure is tied to Phases I and II.

3.2 Phase I and Phase II: Supporting Infrastructure

3.2.1 Key Generation and Encryption

AES 256 bit is used to generate a key that is used by SCPRNG in accordance with NIST SP 800-133 Rev. 2 (National Institute of Standards and Technology, 2023) to secure medical records, while 256 bit AES CBC is used to secure the encryption with a randomly generated 128-bit initialization vector.

$$C = AES - 256 - CBC(P, K, IV)$$

where:

- P = plaintext medical record
- K = 256-bit encryption key
- IV = 128-bit initialization vector
- C = generated ciphertext

For its known security and NIST standardization (National Institute of Standards and Technology, 2023), AES-256-CBC was chosen as the supporting encryption element. The encryption part is infrastructure that facilitates the IVU. The

proposed IVU-based secure distributed medical data storage architecture is shown in Fig 1.

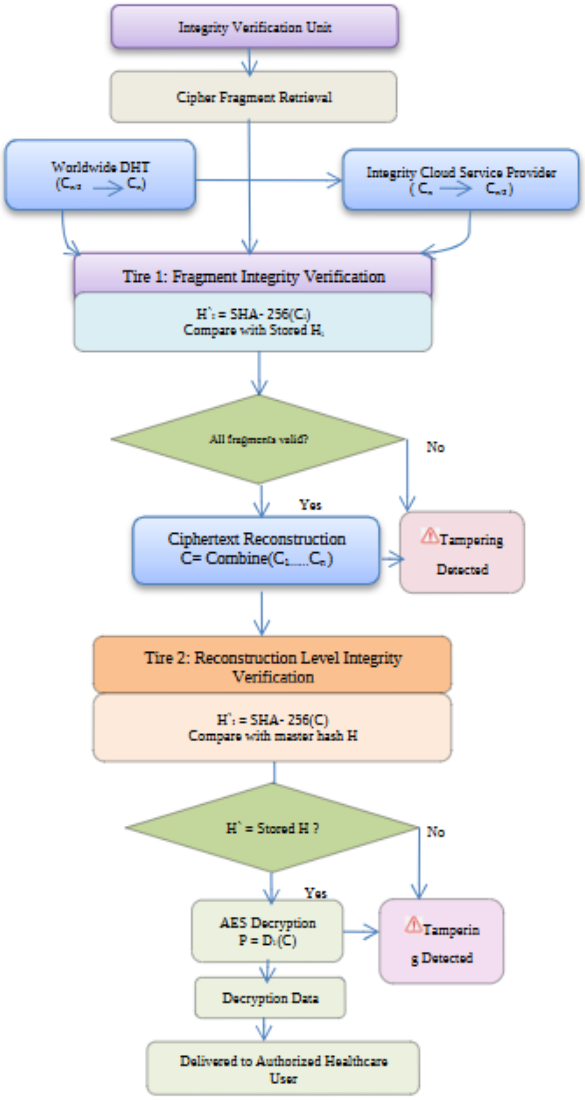

Fig 1: Proposed IVU-Based Secure Distributed Medical Data Storage Architecture

3.2.2 Master Hash Generation

Before fragmentation and encryption, a master SHA-256 hash is computed to get the cipher text.

$$H_{master} = SHA - 256(C)$$

There are three deliberate moves in this step. The first is that the hash calculation is performed on the cipher text, rather than the plain text. This way, IVU is able to process all data in an encrypted form without having to decrypt when verifying. The second is that the calculation of the hash is performed prior to the fragmentation. This means that IVU will be able to check the cipher text as a whole; a fragment level hash would not be able to do this on its own. The third is that the master hash is encrypted prior to it being stored:

$$H_{stored} = RSA - OAEP(H_{master}, PK_{DO})$$

This ensures that an adversary who can gain access to the storage cannot forge a matching hash of tampered cipher text if they don't have the data owner's private key.

- PK_{DO} = public key of the data owner

3.2.3 Fragmentation, Per-Fragment Hashing, and Distribution

The plain-text is split in to disjoint non-overlapping parts of bits of equal length. The

notation $F(C,n)$ is used to represent a family of disjoint classes of content C in the form of set $\{C_1, C_2, \ldots, C_n\}$ which are also allocated in a region whose content is also C and it is represented as:

$$F(C,n) = \{C_1, C_2, \ldots, C_n\}$$

Such that,

$$C = \bigcup_{i=1}^{n} C_i$$

and

$$C_i \cap C_j = \emptyset \ \forall i \neq j$$

For every fragment C_i, an independent SHA-256 hash is computed:

$$H_i = SHA - 256(C_i), \qquad i = 1,2, \ldots, n$$

The hash value of H_i is code block. Each fragment's hash is computed before their distribution so that the reference values are the same as the cipher text when it left in the encryption. Any change in the form, either during the transport or when at rest, will be noticed from either of the sources. Fragment hashes and H_{stored} are remembered in a separate secure information repository, outside of the storage domains.

The primary storage provider is assigned all the C_1 to $C_{\frac{n}{2}}$ fragments. The DHT network (Paganelli & Parlanti, 2012) is used to distribute the fragments $C_{\frac{n}{2}+1}$ to C_n. The two-domain split means that there is no single domain with sufficient fragments to be able to reconstruct data, which makes it possible to reconstruct the architecture even if it is encrypted and secure. Each fragment set is associated with an SDO which is authorised to delete the fragments according to time, and has been integrated with a trusted time server. The Integrity Verification Unit (IVU) is part of Phase III.

3.3 Phase III: The Integrity Verification Unit (IVU)

3.3.1 Design Principles

The IVU is based on four main principles. Firstly independence: the IVU is an independent architectural element that exists without any other system module. Secondly, determinism: there is no randomness in the results of a verification event, only that it can be either positive or negative. Thirdly, completeness: all kinds of attacks are checked in either tier, and they are not repeated in both tiers. Finally, non-disclosure: If either tier rejects and event, then no information is given to the requesting entity.

3.3.2 Attack Classification and Tier Assignment

The IVU aims to detect four different types of attacks, representing all significant threat vectors in distributed cipher text storage and restoration:

- *Class A - Fragment Substitution:* Fragment substitution attack is represented as follows:

$$C_j' \neq C_j$$

where C_j' is a forged or substituted fragment. This attack alters the content of specific fragments, and can be identified at Tier 1.

- *Class B - Silent Corruption:* A fragment C_j is corrupted during transmission or during storage in a non-adversarial manner by the bit flipping, truncating or byte substitution. This type of attack also alters the data within individual fragments, and can be detected at Tier 1.

- *Class C - Fragment Reordering:* All fragments are retrieved in an intact form but are assembled in an incorrect order during restoration, resulting in a wrong cipher text $C' \neq C$ All the fragments are in the right place and unchanged in content in this type of attack. This type of attack can be detected at Tier 2.

- *Class D - Boundary Misalignment***:** The boundaries of the fragments are shifted while reconstruction, for example, by an off-by-one error in the reconstruction function - so that the reconstructed C is not the same as C at the boundary between the segments of the fragments. This attack is similar to Class C, except that it does not modify any of the fragments, and thus passes Tier 1, but fails Tier 2 because of the master hash mismatch.

This classification result proves that Tier 1 and Tier 2 are indeed complementary - that is, they cover different non-overlapping classes of attacks.

Both levels are needed, but neither alone is enough. When two-tire verification is used, the following figure 2 model shows detection of attacks such as fragment substitution, silent corruption, fragment reordering and boundary misalignment.

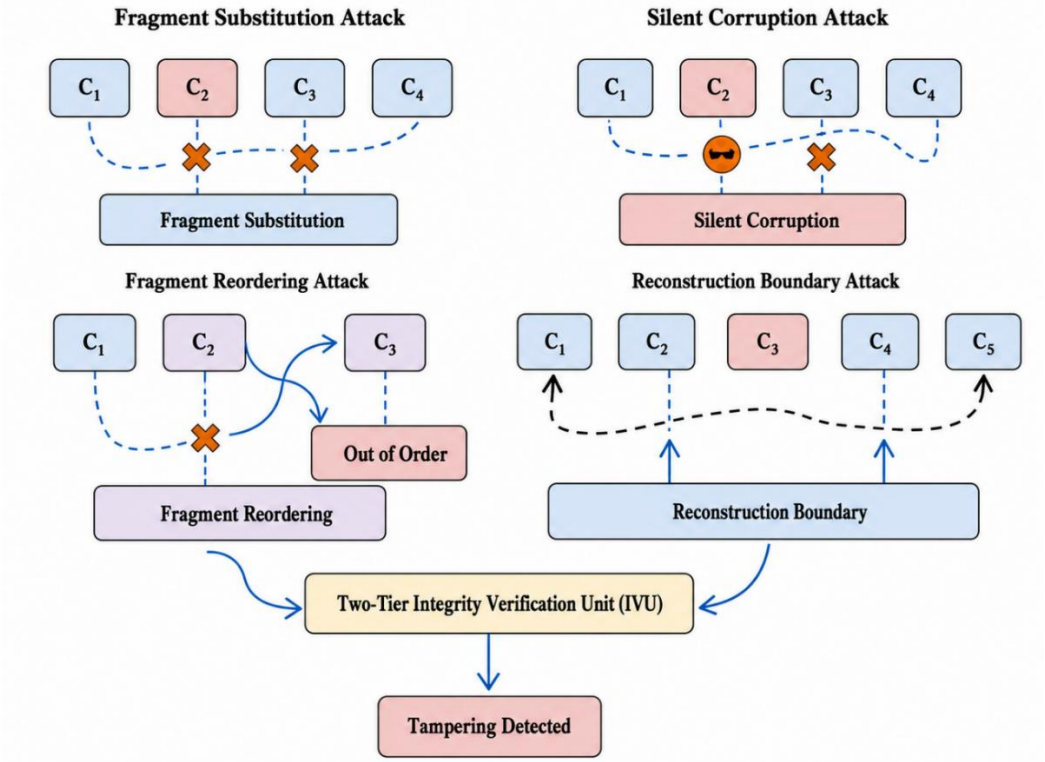

Fig 2: Attack Detection - Integrity Verification Unit(IVU)

3.3.3 Tier 1: Fragment-Level Integrity Verification

The retrieval process of fragments is subject to temporal gating as well as authentication gating prior to the processing in IVU. After passing through these gates the fragments undergo independent re-computation of the SHA-256 function for each fragment Ci', without trying to restore anything. All the recovered fragments are re-computed using the same method as for the computation of the short fragment:

$$Hi' = SHA - 256(Ci'), i = 1, 2, \dots, n$$

The result is then checked against the reference value to verify if each retrieved fragment has the same value of the hash function. If all fragments are verified, then the restoration process continues. In all other cases, the restorations are refused without any exception.

$$\forall\, i\,\{1, \dots . n\}: Hi' = Hi \implies Ci' verified$$

$$\exists\, i : Hi' \neq Hi \implies Fragment\ i\ flagged$$

Restorations were completely rejected on the above condition.

If a fragment of DNA is not similar to the rest, the rejection occurs as soon as it is detected. The flagged fragment is then added to the tamper detection log for administrative review, and the index of the fragment to be flagged is recorded. If the fragments did not pass any of the Tier 1 comparison checks, there won't be any restoration process.

The main architectural strength of Tier 1 is the ability to locate the fault. If a storage node tries to replace or tamper with a fragment, Tier 1's ability to identify the exact index of the tampered fragment is vital for tamper detection and storage node investigation. Detection is done without localization at the restoration level with a simple check.

3.3.4 Tier 2: Reconstruction-Level Integrity Verification

- If and only if all fragments pass Tier 1,

reconstruction takes place:

$$C' = F - 1\,(C1', C2', \ldots, Cn')$$

- A master hash is re-calculated over the completely assembled cipher text: $H_{master} = SHA - 256\,(C')$
- The stored reference is decrypted from the metadata repository: $Hmaster = RSA - OAEP - 1\,(Hstored, SKDO)$
- The result is compared: $H'_{master} = H_{master} \implies Integrity\ Confirmed \implies Decryption\ Authorized$
- $H'_{master} \neq H_{master} \implies Tampering\ Detected \implies Restoration\ Unconditionally\ Rejected$

Tier 2 is for Class C and D attacks, where each fragment is considered intact, but the sequences of fragments are corrupted during reconstruction. This means that integrity of each fragment isn't affected and thus it is not rejected at Tier 1. Tier 2's master hash check is the only way to identify these attacks, however.

The formalized authorization predicate that integrates the two tiers, is:

$$Authorize\ Decryption \iff (V_1 \wedge V_2) = True$$

where:

- V_1 = Tier 1 verification result
- V_2 = Tier 2 verification result

Rejection response is common in all cases regardless of the tier responsible for the rejection, to avoid giving the opponent any clue on which tier has been violated through differential probing.

3.3.5 Decryption and Delivery

Once both V_1 and V_2 are confirmed, decryption happens as follows:

$$P' = AES - 256 - CBC^{-1}(C', K, IV)$$

where:

- P' = recovered plaintext

The obtained P' is sent directly to the authenticated requesting entity and not retained within IVU post-transmission. In case of rejection at both levels, there is no partial decryption, no fragment content revealed, and a full audit record maintained.

3.3.6 IVU Algorithm

Algorithm 1: IVU-Controlled Restoration

Input: $\{C'_1, C'_2, \ldots, C'_n\}, \{H_1, H_2, \ldots, H_n, H_{stored}\}$,

Output: Verified plaintext P' or $REJECTION$

1: FOR $\forall i \in \{1,2,\ldots,n\}$:

2: $H'_i \leftarrow SHA - 256(C'_i)$

3: IF $H'_i \neq H_i$:

4: $Log(Fragment\ i\ Tampered \wedge REJECTION$

5: return $REJECTION$

6: end IF

7: end FOR

8: $C' \leftarrow F^{-1}(C'_1, C'_2, \ldots, C'_n)$

9: $H'_{master} \leftarrow SHA - 256(C')$

10: $H_{master} \leftarrow RSA - OAEP^{-1}(H_{stored}, SK_{DO})$

11: IF $H'_{master} \neq H_{master}$:

12: Log: $(Reconstruction - Level\ Tampering) \wedge REJECTION$

13: return $REJECTION$

14: end IF

15: $P' \leftarrow AES - 256 - CBC^{-1}(C', K, IV)$

16: Deliver P' to authenticated entity

17: return P'

3.4 Security Properties

The proposed framework offers five security properties for distributed medical data storage. Confidentiality is ensured by the use of AES-256-CBC encryption that does not allow clear-text access, unless the session key and IV are known.

The two-tiered IVU provides pre-decryption tamper detection for all four of the attack classes, providing Data Integrity. This allows for the retrieval of the data from the system in plain text, such that it is the same data as is stored in the system and has not been altered in any way by the system. The DHT-based distribution guarantees availability as well, without central coordination. Reconstruction Resistance is enforced by using mandatory two-domain fragments. Temporal Access Governance is implemented by using time-bound deletion.

3.5 Integrity Assurance Analysis

The framework guarantees that recovery of medical data in distributed storage can be reliable and correct. With medical records being stored in many different storage domains, there is a need to maintain consistency of the encrypted data before decrypting it to ensure that accurate medical records can be recovered. IVU's two independent verifications ensures that the output of the ciphertext from the restoration process is the same as the ciphertext that was originally stored. The first important level is checking each retrieved piece with a hash function using SHA-256. The result is that no changes are made to the chunks of the ciphertext while it is stored or transmitted. If any fragment is not the same as the one in memory, then restoration is refused. At the second-level, if all the segments of the deciphered text pass the fragment-level verification, the deciphered text is reconstructed and a master hash of the complete deciphered text is recalculated. During the initial storage of the data storing the master hash, it is securely stored. Only if both values are the same then it is possible to decrypt.

Two-level verification will keep the structural changes from happening when the ciphertext is stored. So, the decrypted medical record will be exactly the same as the original encrypted medical record. The framework's decryption guarantees that the information will remain intact even if it is encrypted. This means that if there is any corruption or incompleteness in a medical record, it will not be rebuilt and will not get to the clinical systems. This design enhances reliability of the distributed storage of medical data and the correctness of recovered data..

4. Results and Discussion

4.1. Dataset

We conducted experiments on a synthetic health care dataset, which is in CSV format, in this research work. The detailed medical record features patient details, disease classifications, care plans and even medication data. In security and cryptography research, synthetic health care datasets are used extensively as they mimic the structures of electronic health records (EHRs) without any privacy and re-identification issues, typical of simulated medical datasets. In order to check the scalability of the proposed system, the dataset was organized in multiple file sizes between 500 Kb to 10 Mb. In the integrity verification experiments, every occurrence of the data set was encrypted, fragmented, stored at the distributed storage nodes and reconstructed.

4.2 Implementation Environment

This framework was built-in in python 3.11. encrypted operations of AES and RSA-OAEP encryption were performed using the PyCryptodome library. It hashes the check sum by using hashlib library and used to multiply and verify hash of the hashlib library by using the hash function sha256. A DHT environment with 10 storage nodes was created to become virtual for the purpose of performing distributed storage simulation. The experiments were performed on the Intel Core i5 2.4GHz processor having 8GB RAM with Ubuntu 22.04 LTS. from each one trial was repeated 30 times and the results were stated in mean values ± SD to ensure that the experiment is reliable.

4.3 Tamper Injection Protocol

During the restoration phase, controlled tampering conditions have been artificially imposed on top of the proposed Integrity Verification Unit (IVU) to evaluate the effectiveness of the IVU. The four tamper conditions were introduced to all data set sizes and each tamper condition was repeated 50 times for each data set size. The conditions of tamper are as follows:

- *T1 - Single Fragment Substitution*: Modification of a single fragment in the cipher text, to bypass Tier-1 fragment verification.
- *T2 - Silent Fragment Corruption*: Several bytes in a fragment are altered to mimic a corruption in the transmission or storage of the fragment, which also targets Tier-1 verification.
- *T3— Fragment Reordering*: All fragments are kept the same, but they are reassembled in the wrong order, to address Tier-2 reconstruction verification.
- *T4 - Boundary Misalignment*: Reconstructed fragments are the same, but their boundaries have been misaligned i.e. wrong Cipher Text Structure.

These tamper scenarios simulate potential corruption conditions that may occur during distributed storage or data transmission. The experiments evaluate whether the proposed two-tier IVU can correctly detect any modification before the ciphertext is decrypted.

4.4 Evaluation Metrics

The performance of the proposed framework was evaluated using the following metrics:

- *IVU Tier-1 Time (ms):* Time required for SHA-256 recomputation and comparison of all retrieved ciphertext fragments.
- *IVU Tier-2 Time (ms):* Time required for reconstruction-level SHA-256 computation and RSA-OAEP decryption of the stored master hash.
- *Total IVU Overhead (ms):* Total verification time required by the Integrity Verification Unit.

$$Total\ IVU\ Time = Tier1\ Time + Tier2\ Time$$

- *IVU Overhead as Percentage of Encryption Time (%):* $IVU_{overhead}(\%) = \times 100$
- *Tamper Detection Rate (TDR):* $TDR(\%) = \times 100$
- *False Positive Rate (FPR):* $FPR(\%) = \times 100$
- *Fragment Retrieval Latency (ms):* Average time required to retrieve all fragments from the distributed storage domains.

4.5 IVU Performance Across Dataset Sizes

The data in Table 1 clearly shows that the more data included, the longer it takes IVU to verify. The IVU overhead however is pretty much unchanged at 5.98% of the encryption time. This is because of the linear nature of the hash used, SHA-256, in Tier 1 verification, and shows that the verification time is directly proportional to the size of the data set. There is no false rejection of a legitimate restoration request even for large data sets, the False Positive Rate (FPR) is 0.0%. It is clear that, reliability is important for health care applications, as data can be rejected and stop a medical process from being performed.

Table 1: IVU Performance by Dataset Size

Dataset Size	Tier-1 Time (ms)	Tier-2 Time (ms)	Total IVU Time (ms)	Encryption Time (ms)	IVU Overhead (%)	TDR (%)	FPR (%)
500 KB	3.2	2.1	5.3	88.6	5.98	100.0	0.0
1 MB	4.8	3.3	8.1	135.4	5.98	100.0	0.0
2 MB	7.6	5.4	13.0	217.6	5.98	100.0	0.0
5 MB	14.9	9.8	24.7	414.2	5.98	100.0	0.0
10 MB	26.3	16.7	43.0	718.4	5.98	100.0	0.0

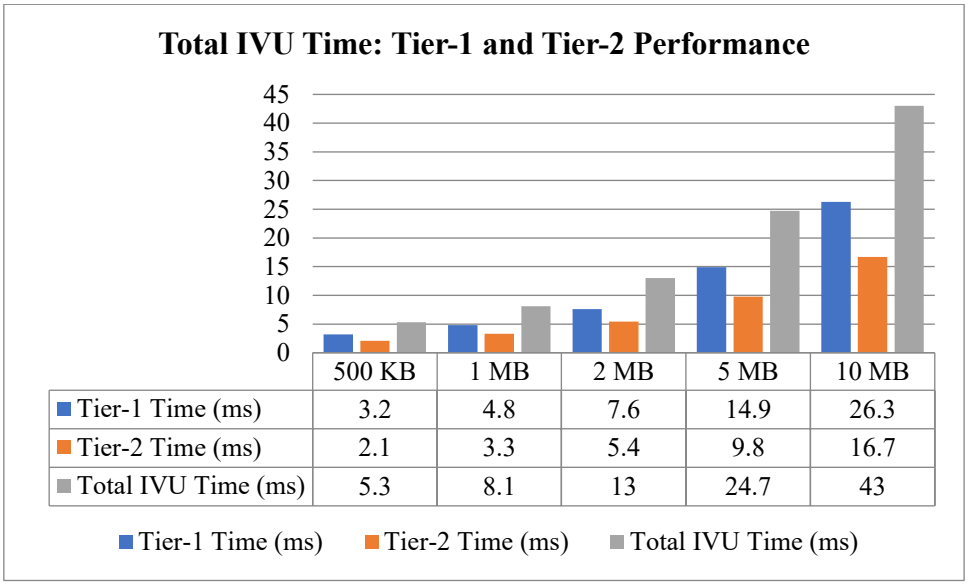

Fig. 3: Tier-1, Tier-2, and Total IVU Time across dataset sizes

If the computation is overrun, Tier 1 verification consumes a higher percentage of the total IVU processing time: both the time needed for hash recomputation of each fragment. Tier 2 is a reconstruction level verification, is less time consuming since it is an RSA OAEP decryption of stored master hash.

4.6. Tamper Detection by Attack Class

The results of tamper detection by attack class are shown in Table 2 for all the dataset sizes. Fifty injections were given per class per size (5000 injections total was given per attack class). The various attack classes are listed in the below table along with the corresponding Tamper Detection Rate.

Table 2: Tamper Detection Rate by Attack Class

Attack Class	**Description**	**Detected by Tier**	**Injections**	**Detected**	**TDR (%)**
T1 - Fragment Substitution	Single fragment replaced	Tier 1	1000	1000	100.0
T2 - Silent Corruption	Byte-level corruption within fragment	Tier 1	1000	1000	100.0
T3 - Fragment Reordering	Fragments reconstructed out of sequence	Tier 2	1000	1000	100.0
T4 - Boundary Misalignment	Fragment boundaries shift during reconstruction	Tier 2	1000	1000	100.0
Combined	All four attack classes	Both Tiers	4000	4000	100.0

The results of tamper detection for the four corruption scenarios are shown in Table 2. The proposed two-tier Integrity Verification Unit (IVU) was able to successfully detect all tampering attempted for all attack classes. T1 and T2 silent corruption attacks were detected at Tier-1 fragment verification stage, with the re-computation of the hash of every fragment, and comparing the fragment hash with the previously stored hash. The attacks are detected during the Tier-2 reconstruction verification phase, where the reconstructed ciphertext hash is compared to a reference hash of the encrypted master hash. It was observed that the framework had a Tamper

Detection Rate (TDR) of 100% after the 4000 tamper injections, showing the effectiveness of the proposed integrity checking mechanism, which can detect unauthorized alteration of the data prior to data decryption.

4.7 Fragment Retrieval Latency

The retrieved latency of time series for various sizes of the retrieved datasets are presented in the following Table 3:

Table 3: Fragment Retrieval Latency

Size	Fragments (n)	Storage Provider (ms)	DHT (ms)	Total (ms)
500 KB	10	12.4	18.7	31.1
1 MB	10	14.8	22.3	37.1
2 MB	20	19.6	29.4	49.0
5 MB	20	28.3	41.7	70.0
10 MB	40	41.2	58.9	100.1

As can be seen from the data in Table 3, the fragment retrieval latency increases with the increase of data set size during the restoration process. If the number of data fragments is increased, the retrieval time from the storage provider as well as the DHT network will also increase when the size of the dataset is increased. But the time taken to retrieve the data for DHT is a little bit larger because of the distributed lookup mechanism. However, the overall retrieval delay is acceptable, indicating that the proposed fragmented storage approach does not cause major delays when restoring medical data.

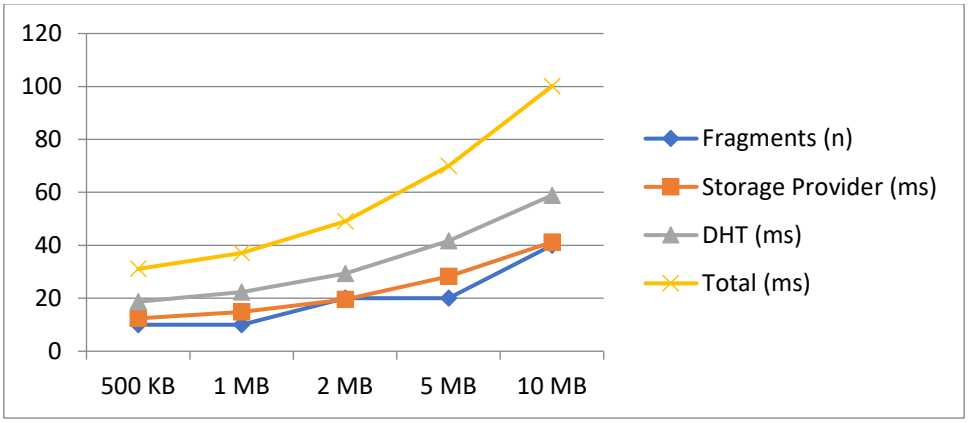

Fig 4: Fragment Retrieval Latency Analysis

4.8. Comparative Analysis with Recent Works

To compare the proposed IVU framework with five recent papers dealing with the security aspects of distributed data storage in healthcare or related domains, the features of the two approaches were compared at the feature level as shown in Table 4.

Table 4: Feature Comparison with Recent Works

Category	Feature	AES-128 (NIST, 2023)	Sym ECCipher (Selvi & Sakthivel, 2025)	BCT-AES (Venkataradha-krishnamurty & Malathi, 2026)	Modified AES (Adeniyi et al., 2023	Hybrid Architecture (Ahmed & Yuan, 2026)	Proposed IVU

Storage Model	Encryption	AES-128	ECC+AES	AES+CNN	Modified AES	AES-128	AES-256
	Distributed Storage	✗	✗	Blockchain	✗	Multi-cloud+vault	✓ Cloud+DHT
Integrity Protection	Fragmentation	✗	✗	✗	✗	AI-adaptive	✓ Structured
	Fragment-Level Integrity	✗	✗	✗	✗	✗	✓ Tier 1
	Reconstruction Integrity	✗	✗	Blockchain hash	✗	✗	✓ Tier 2
	Independent IVU	✗	✗	✗	✗	✗	✓
	Pre-Decryption Verification	✗	✗	✗	✗	✗	✓
Security Metrics	Tamper Detection Rate	—	—	Not reported	—	Not reported	100%
	False Positive Rate	—	—	Not reported	—	Not reported	0.0%
Resilience	Reconstruction Resistance	✗	✗	Immutability	✗	✓ Multi-domain	✓ Two-domain
Governance	Lifecycle Governance	✗	✗	✗	✗	✗	✓ SDO

Table 4 is a comparison chart of the proposed IVU framework with some of the currently available data security solutions for the healthcare data security. Most of these approaches are based on encryption techniques but do not consider a structured fragmentation technique and multi-level integrity verification. In this context, the proposed IVU framework takes a two-level integrity verification process and distributed data storage via cloud domain and DHT domain. This approach achieves 100% tamper detection with no false detection, and takes into account a data life cycle via a secure data object model.

5. Conclusion

The present study presents a Two-Tier Integrity Verification Unit (IVU) to enhance the secure restoration of distributed individualized education and therapy records (IERs) in disability-support and special education settings. The framework includes both fragment level and reconstruction level SHA-256 integrity verification before decryption, which allows for the detection of corrupted, altered and incorrectly reconstructed encrypted records that could impact educational planning, therapeutic intervention and decision making for disability support prior to their being decrypted. In a distributed educational system, the accuracy and reliability of the individualized learner records are even more critical in ensuring continuity of support services for students with disabilities in this extra verification layer. Experimental testing with the synthetic educational-support dataset showed that the proposed framework is able to successfully detect tampering attempts and have very low overhead for restoring the original system. The results show that it is possible to add reliable cryptographic integrity verification to distributed

educational-record systems without undue latency that may impede the usability of the system within an institution. Comparative analysis also revealed that most of the current educational data-security solutions are mainly focused on confidentiality and access control and offer minimal security in the face of corruption at the restoration stage or manipulation of the ciphertext. The proposed IVU framework will assist in the creation of trustworthy, secure, and resilient digital infrastructures for special education services by ensuring that records, such as individualized education plans (IEPs), therapy notes, and behavioral-support records, remain accurate and intact while being stored and restored across multiple locations. Future studies could include integration with post-quantum cryptographic approaches, large-scale verifiers for the education repositories and the validation in real-world inclusive education and disability support platforms.

References

Shivashankar, K., & Bakthavatchaalam, V. (2024). Education policies through data driven decision making: Accelerating inclusive education for people with disabilities. *Artificial intelligence enabled management: An emerging economy perspective*, *15*, 56-69. https://doi.org/10.1515/9783111172408-002

Sinan, I. I., Tong, V. V. T., Nwoacha, V., Degila, J., Onashoga, A., Oaihimire, I. O., & Ukhurebor, K. E. (2024). Enhancing Security and Privacy in Educational Environments: A Secure Grade Distribution Scheme with Moodle Integration. *Journal of Infrastructure, Policy, and Development*, *8*(7), 3737. https://doi.org/10.24294/jipd.v8i7.3737

Lovett, B. J. (2020). Disability identification and educational accommodations: Lessons from the 2019 admissions scandal. *Educational Researcher*, *49*(2), 125-129. https://doi.org/10.3102/0013189X20902100

Ayare, A. A., Jadhav, V. A., Banatwala, M. K., Changlere, S. V., Mote, A., Joshi, P., ... & Banatwala, M. (2025). A systematic review on blockchain-based framework for storing educational records using interplanetary file system. *Cureus J Comput Sci*, *2*. https://doi.org/10.7759/s44389-024-00745-y

Syed, A. (2025). Blockchain's Cryptographic Backbone: Mastering Hash Functions, Digital Signatures & Merkle Trees. *Journal of Scientific Research and Technology*, 254-259. https://doi.org/10.61808/jsrt384

Upadhyay, S., Pandey, A. K., Kumar, S., & Mishra, S. (2026). Power efficient and area optimized advanced encryption standard-based cipher for improved cyber security. Journal of Cyber Security Technology, 10(1), 1-25. https://doi.org/10.1080/23742917.2025.2475559

Garigipati, N., Srithar, S., & Krishna Reddy, V. (2026). An efficient poly-quantum integrity key generation based multi-user access control encryption and decryption framework for homogeneous and heterogeneous cloud EHR databases. *Information Security Journal: A Global Perspective*, *35*(1), 168-188. https://doi.org/10.1080/19393555.2025.2479029

Palkar, S. S., Mehra, R., & Hadimani, L. (2026). A blockchain-based self-sovereign identity in adaptive access control framework and differential privacy for real-time privacy-preserving EHR management. OPSEARCH, 1-38. https://doi.org/10.1007/s12597-026-01167-1

Rohollahi, A., Bagherifard, K., & Malekhosini, R. (2026). An Active Data Cube (ADCu)-Based Security Framework for Enhancing Security, Access Control, and Accountability in Cloud Computing Environments. *Management Strategies and Engineering Sciences*, *8*(1), 1-12. https://doi.org/10.61838/msesj.271

Kouo, J. L., Harkins-Brown, A. R., & Phung, V. H. (2024). Reported Policies, Guidance, and Related Resources for the Determination of Special Education and Related Services. *The Journal of Special Education*, *58*(2), 100-110. https://doi.org/10.1177/00224669231218451

Blackwell, W. H., & Rossetti, Z. S. (2014). The development of individualized education programs: Where have we been and where should we go now? *SAGE Open, 4*(2). https://doi.org/10.1177/2158244014530411

McKenna, J. W., Solis, M., Garwood, J., & Parenti, M. (2024). Characteristics of individualized education programs for students with learning disabilities: A systematic review. *Learning Disability Quarterly, 47*(3). https://doi.org/10.1177/07319487231182697

Oloto, A. M., & Yeboah, T. J. (2025). Developing conceptual risk assessment models for special education documentation and accountability systems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. https://doi.org/10.32628/CSEIT251116283

Peters, N. R. (2022). The golem in the machine: FERPA, dirty data, and digital distortion in the education record. *Washington and Lee Law Review, 78*(5), 1991–2056.

Cavalari, R. N. S., Gillis, J. M., Kruser, N., & Romanczyk, R. G. (2014). Digital communication and records in service provision and supervision: Regulation and practice. *Behavior Analysis in Practice, 8*(2), 176–189. https://doi.org/10.1007/s40617-014-0030-3

Rezaeibagha, F., Win, K. T., & Susilo, W. (2015). A systematic literature review on security and privacy of electronic health record systems: Technical perspectives. *Health Information Management Journal, 44*(3), 23–38. https://doi.org/10.1177/183335831504400304

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics, 46*(3), 541–562. https://doi.org/10.1016/j.jbi.2012.12.003

Cobrado, U. N., Sharief, S., Regahal, N. G., Zepka, E., Mamauag, M., & Velasco, L. C. (2024). Access control solutions in electronic health record systems: A systematic review. *Informatics in Medicine Unlocked*, *49*, 101552. https://doi.org/10.1016/j.imu.2024.101552

Tertulino, R., Antunes, N., & Morais, H. (2024). Privacy in electronic health records: A systematic mapping study. *Journal of Public Health, 32*, 435–454. https://doi.org/10.1007/s10389-022-01795-z

Almaghrabi, N. S., & Bugis, B. A. (2022). Patient confidentiality of electronic health records: A recent review of the Saudi literature. *Dr. Sulaiman Al Habib Medical Journal, 4*, 126–135. https://doi.org/10.1007/s44229-022-00016-9

Vimalachandran, P., Wang, H., Zhang, Y., Heyward, B., & Whittaker, F. (2018). Ensuring data integrity in electronic health records: A quality health care implication. *arXiv preprint arXiv:1802.00577*. https://doi.org/10.48550/arXiv.1802.00577

Xie, F., Yuan, H., Ning, Y., Ong, M. E. H., Feng, M., Hsu, W., Chakraborty, B., & Liu, N. (2021). Deep learning for temporal data representation in electronic health records: A systematic review of challenges and methodologies. *arXiv preprint arXiv:2107.09951.* https://doi.org/10.48550/arXiv.2107.09951

Ahmed, M., & Yuan, J.-S. (2026). AI-driven hybrid architecture for secure, reconstruction-resistant multi-cloud storage. *Future Internet, 18*(2), 70. https://doi.org/10.3390/fi18020070

National Institute of Standards and Technology, "*Advanced Encryption Standard (AES)*," FIPS PUB 197, updated May 2023. https://doi.org/10.6028/NIST.FIPS.197-upd1

Selvi, P., & Sakthivel, S. (2025). A hybrid ECC-AES encryption framework for secure and efficient cloud-based data protection. *Scientific Reports*, *15*(1), 30867. https://doi.org/10.1038/s41598-025-01315-5

Venkataradhakrishnamurty, P., & Malathi, K. (2026). A holistic framework for strengthening security of healthcare data through encryption utilizing blockchain technology. *Scientific Reports*, 16, 2008. https://doi.org/10.1038/s41598-025-31698-4

Adeniyi, A. E., Abiodun, K. M., Awotunde, J. B., Olagunju, M., Ojo, O. S., & Edet, N. P. (2023). Implementation of a block cipher algorithm for medical information security on cloud environment: using modified advanced encryption standard approach. *Multimedia Tools and Applications*, *82*(13), 20537-20551. https://doi.org/10.1007/s11042-023-14338-9

Paganelli, F., & Parlanti, D. (2012). A DHT-based discovery service for the Internet of Things. *Journal of Computer Networks and Communications*, *2012*(1), 107041. https://doi.org/10.1155/2012/107041