Faculty of Natural and Applied Sciences Journal of Computing and Applications
Print ISSN: 3026-8133
www.fnasjournals.com
Volume 2; Issue 4; December 2025; Page No. 143-153.
DOI: https://doi.org/10.63561/jca.v2i4.1083

A Framework for Secure Management of Health Records in Grid Computing Environments

***[1]Omoniyi, A.O., [1]Oladimeji, B.J., [1]Bamikole, O. E., & [2]Olojido, J.B.**
[1]Faculty of Nursing, Rufus Giwa Polytecnic Owo,, Ondo State, Nigeria,
[2]Achievers University, Owo, Ondo State, Nigeria

***Corresponding author email**: omoniyiojo@gmail.com

Abstract

The integration of grid computing into healthcare has enabled the efficient storage, sharing, and processing of large-scale medical data across distributed environments. While this advancement enhances collaboration, research, and patient care, it also raises critical security and privacy challenges. This study addresses the protection of e-health records in a grid-enabled environment by developing a security framework that ensures confidentiality, integrity, and controlled access to sensitive patient information. The methodology adopted includes an overview of grid and health grid architecture, an analysis of existing grid security infrastructure, and the implementation of pseudonymization and encryption techniques to safeguard data. The proposed system introduces a layered security model incorporating authentication, authorization, accountability, and reversible pseudonymization to balance privacy preservation with accessibility for healthcare providers and researchers. Results demonstrate that the framework effectively minimizes unauthorized access risks, strengthens patient trust, and supports ethical and legal compliance in health data management. This work contributes to advancing secure e-health infrastructures and recommends the adoption of integrated cryptographic and pseudonymization techniques for scalable, reliable, and privacy-aware health grid systems.

Keywords: E-Health Records, Grid Computing, Security, Pseudonymization, Authentication

Introduction

The swift digital evolution of the healthcare sector has significantly reshaped how medical information is produced, managed, and exchanged. Today, Electronic Health Records (EHRs) serve as a fundamental component of contemporary healthcare infrastructures, offering immediate access to patient data while enhancing clinical decision-making processes. Furthermore, the expansion of telemedicine, the Internet of Medical Things (IoMT), and artificial intelligence-powered diagnostic systems has dramatically increased both the volume and sensitivity of medical data, resulting in a data landscape that is growing more rapidly than ever before. While these innovations improve efficiency and patient outcomes, they also expose healthcare systems to complex cybersecurity risks, data breaches, and privacy violations (Al-Janabi et al., 2023; WHO, 2024).

Distributed computing models such as grid and cloud environments are increasingly adopted to manage the large-scale storage, computation, and sharing of medical records across institutions. These infrastructures facilitate collaborative research, remote healthcare delivery, and multi-institutional data integration, particularly for computationally intensive tasks such as medical imaging, genomic analysis, and predictive modeling. However, the dynamic, multi-user, and cross-organizational nature of these environments introduces significant security, privacy, and trust challenges (Zhang et al., 2022) The protection of sensitive patient information against unauthorized access, insider threats, data breaches, and malicious cyberattacks has become a critical priority in modern healthcare environments. As digital systems continue to expand, ensuring robust security mechanisms is essential to maintain

Cite this article as:
Omoniyi, A.O., Oladimeji, B.J., Bamikole, O. E., & [2]Olojido, J.B. (2025). A framework for secure management of health records in grid computing environments**.** *FNAS Journal of Computing and Applications, 2*(4), 143-153. https://doi.org/10.63561/jca.v2i4.1083

patient confidentiality, preserve data integrity, and guarantee the availability of healthcare services. and advanced cyberattacks has therefore become a primary concern for both practitioners and researchers.

Globally, healthcare institutions have increasingly become primary targets for cybercriminals, largely because medical records possess exceptionally high monetary value on the black market—often surpassing that of financial data (IBM Security, 2023). Rising incidents of ransomware attacks, unauthorized data sharing, and breaches affecting cloud-based health platforms underscore the urgent need for comprehensive and multi-layered cybersecurity frameworks. In addition to technical vulnerabilities, ethical and legal responsibilities further heighten the importance of strong data protection. Regulatory requirements—such as the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States—demand strict adherence to privacy standards, making the protection of patient data essential for maintaining user trust and ensuring the integrity of modern e-health systems (Abouelmehdi et al., 2023).In this context, the integration of grid-enabled infrastructures with advanced security mechanisms such as authentication, authorization, encryption, and pseudonymization offers promising solutions. These mechanisms not only mitigate unauthorized access but also ensure accountability, non-repudiation, and privacy preservation. As healthcare increasingly shifts toward collaborative, data-driven ecosystems, securing EHRs within grid-enabled environments is no longer optional but a fundamental prerequisite for sustainable e-health innovation.

This study therefore investigates the security of electronic health records within a grid-enabled computing environment, critically evaluating the existing vulnerabilities, operational challenges, and emerging threats associated with distributed healthcare data systems. It further proposes strategic, evidence-based measures aimed at enhancing data protection, improving system resilience, and ensuring that sensitive patient information remains secure throughout its lifecycle. By addressing both technical and ethical dimensions, the research contributes to the development of resilient, patient-centered digital healthcare infrastructures.

Healthcare has become a primary target for cyberattacks (ransomware, data theft) because EHRs contain high-value, sensitive information; simultaneous growth in cloud, grid, IoMT and AI increases the attack surface and the need for privacy-preserving, distributed protection mechanisms. Recent systematic reviews emphasize that traditional perimeter defenses are insufficient and that privacy-enhancing architectures are required for collaborative healthcare platforms. (IBM Security, 2023; Abouelmehdi et al., 2023).

Pseudonymization remains a core, practical approach for sharing health data across sites (including grid-like federations) while enabling linkage for longitudinal studies. Recent work focuses on robust, standards-aware de-identification for modern data models such as FHIR, and scalable pseudonymization tools designed for multi-site deployments (trusted-third-party models, reversible pseudonyms with secure keying (The ORCHESTRA Consortium, 2024; Wani & Can, 2025).

Secure storage and transfer are foundational for grid storage. Advances include: (a) using distributed key-share schemes (shamir-style secret sharing) to avoid single key servers; (b) stronger transport/message protection (TLS/WS-Security); and (c) homomorphic encryption to enable some computations over encrypted EHRs. Reviews show homomorphic encryption and scalable key-management are promising, but performance and complexity still limit wide production use A significant body of recent work explores blockchain for audit trails, consent management, and decentralized access control for EHRs. Systematic reviews (2021–2024) find that blockchain improves traceability and tamper evidence, but scalability, privacy (storing off-chain vs on-chain), and integration with legacy EHR systems are practical hurdles. Hybrid models (blockchain for metadata/consent; encrypted off-chain storage for records) are the most common design pattern. (Abouelmehdi et al., 2023; Teo et al., 2024).

Grid security infrastructures historically used X.509 PKI and GSI models for authentication/authorization. Contemporary research advances these earlier designs by integrating more sophisticated authorization models such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), which enable fine-grained, context-aware, and highly scalable mechanisms for regulating access to sensitive health information.strong multi-factor authentication, and fine-grained policy enforcement integrating patient consent. Recent studies emphasize the importance of strong auditing and non-repudiation mechanisms for accountability in multi-institutional grids. (Zhang et al., 2022; Ali et al., 2024).

GDPR, HIPAA and similar regulations make pseudonymization, data minimization, and consent management legal necessities. Recent legal/technical work clarifies that pseudonymization reduces regulatory risk but does not remove it unless data are truly anonymized; consequently, technical solutions must be coupled with governance (consent capture, data use agreements, and auditing). Papers on FL governance and data custodianship stress procedural controls and transparency for trust. (WHO, 2024; Abouelmehdi et al., 2023).

Notable recent contributions include: ORCHESTRA Pseudonymization Tool (2024) for rapid pseudonymisation deployment; FED-EHR (2025) and other privacy-by-design FL frameworks tailored for EHRs; and multiple blockchain-based prototypes evaluated in pilot studies and systematic reviews (2021–2024). These studies indicate feasibility but also point out performance, integration, and user-acceptance gaps. (The ORCHESTRA Consortium, 2024; Wani & Can, 2025; Abbas et al., 2024).

Methods and Materials

The study adopted a design science research methodology (DSRM) to develop and evaluate a security framework for e-health records in a grid-enabled environment. DSRM is suitable for information systems research where the goal is to design, build, and assess an artifact that addresses a practical problem. The methodology followed these iterative phases:

Problem identification and motivation

Recognizing that distributed grid environments in healthcare face critical challenges of data confidentiality, integrity, and access control.
Emphasis was placed on privacy preservation in multi-institutional data sharing.

Definition of objectives of the solution

The objective was to design a security model combining authentication, authorization, pseudonymization, encryption, and distributed key management to protect e-health records.

Design and development

Construction of an architectural model and algorithms for pseudonymization, encryption, and secure access control.
Use of layered security (Grid Security Infrastructure + pseudonymization + encryption + auditing).

Demonstration

The model was applied in a simulated grid-enabled health environment to show how medical records can be securely stored, transmitted, and accessed.

Evaluation

The framework was assessed using **security analysis (threat modeling, attack scenarios, compliance mapping)** and performance indicators such as confidentiality strength, computational overhead, and scalability.

Communication

Findings were documented for academic dissemination and practical use in healthcare IT governance.
design methods
Grid computing is centered on the secure, flexible, and coordinated sharing of large-scale computational and data resources across distributed systems. By enabling seamless collaboration among geographically dispersed nodes, grid infrastructures support innovative applications that depend on high-throughput processing to address highly complex computational challenges. Even when users are geographically separated, they can collaborate by accessing pooled resources within a shared Grid environment, organized into Virtual Organizations (VOs)**,** which form the backbone of Grid applications. By pooling computing power from various institutions worldwide, Grid computing enables dynamically formed collaborations, making it particularly useful for fields like medicine.

The **architecture of Grid computing** is layered:
The **network layer** (base) links all resources,

Cite this article as:
Omoniyi, A.O., Oladimeji, B.J., Bamikole, O. E., & [2]Olojido, J.B. (2025). A framework for secure management of health records in grid computing environments**.** *FNAS Journal of Computing and Applications, 2*(4), 143-153. https://doi.org/10.63561/jca.v2i4.1083

The **resource layer** consists of computers, storage, sensors, and other connected assets,
The **middleware layer** acts as the "intelligence" that integrates and manages these resources, and
The **application layer** (top) provides user-facing applications across fields like science, engineering, and finance, as well as service functions like usage monitoring, billing, and account management.

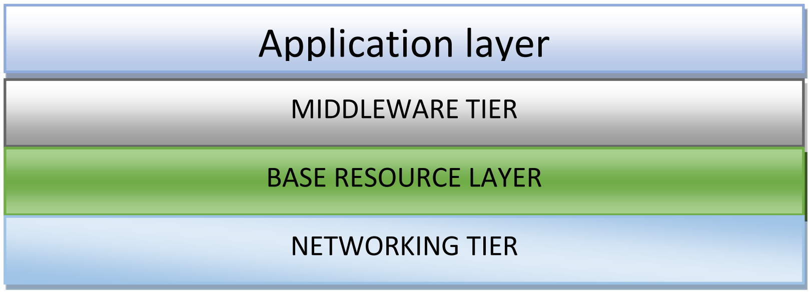

Fig 1. The Grid Layers

Healthcare providers today require more than just the ability to store and move large volumes of medical information. They also need systems that allow them to retrieve, modify, and intelligently merge diverse data sources to produce meaningful clinical insights. This need forms the basis of the HealthGrid concept. A HealthGrid is designed to address the distributed computing needs of hospitals and medical research by linking multiple healthcare organizations into a shared platform where clinically useful data can be kept and accessed by authorized participants. Within this framework, information of medical relevance can be made readily available to a wide range of users—doctors, support staff, healthcare centers, administrative bodies, research institutions, and even patients. For the system to operate effectively, it must uphold strict standards of data security, ethical responsibility, and regulatory compliance. It must also reinforce core healthcare obligations such as confidentiality and duty of care, while managing potential challenges related to information transparency and public access rights.

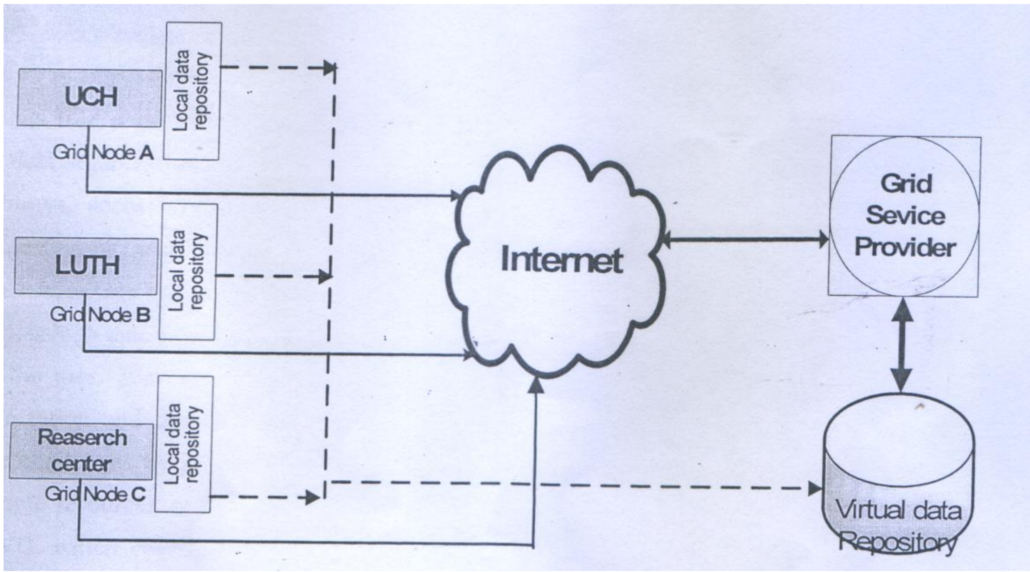

Fig 2: A typical Health Grid Scenario security control for unauthorized users.

Enabling secured data exchange between healthcare providers distributed across networks is one of the major concerns of medical applications. The Grid addresses security issues by providing a common infrastructure for secure access and communication between grid-connected sites. This infrastructure includes authentication and authorization mechanisms, amongst other things, supporting security across orsanizational boundaries.

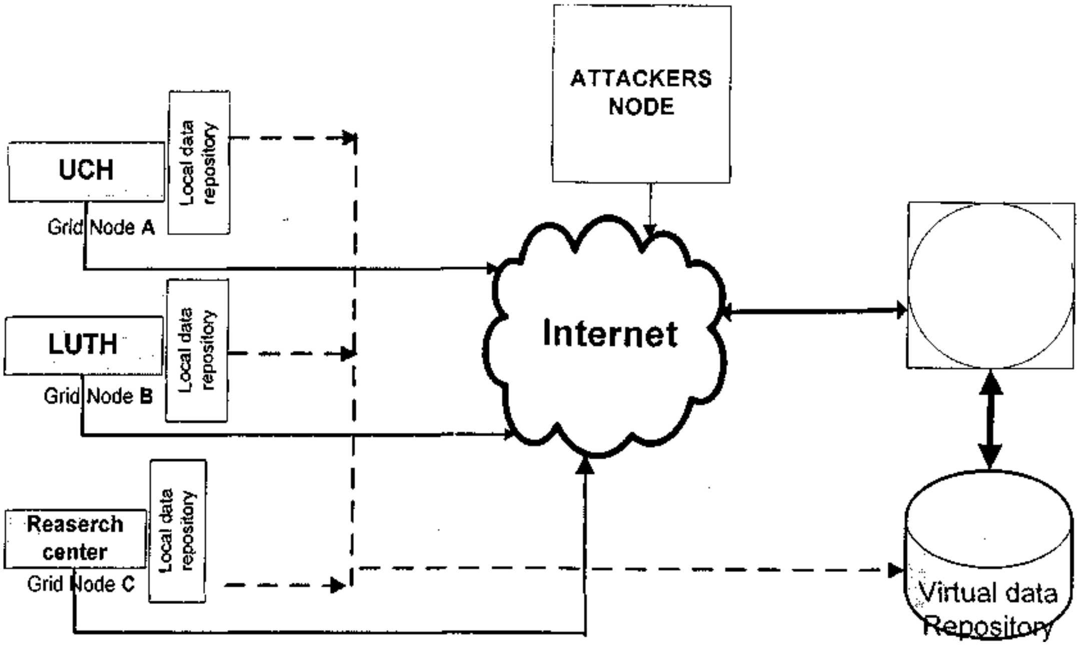

Fig 3: A typical HealthGrid Scenario with Attackers Node

From the above figure, an external node is an attacker's node that serves as threat to medical record. This attacker node can be variety of personality and organization which serve as a threat for medical record or the entire healthgrid system. Security threats to medical record sharing systems can arise from a variety of sources. These include individuals seeking personal information about public figures or private citizens, such as journalists or reporters. Internal threats may come from system administrators or other personnel within the organization who access records for non-health-related purposes, often motivated by the potential monetary value of such data. External cybercriminals who gain unauthorized access to a general practitioner’s database may exploit this information to commit more severe crimes. Additionally, personnel at the data-hosting site who are not held to strict legal accountability may attempt to access identifiable patient records. Other potential threats include the disclosure of health information for law enforcement or national security purposes, as well as requests from insurance companies for clients’ medical data. Some of these security challenges can be mitigated through the Grid Security Infrastructure (GSI), a component of the Globus Toolkit. GSI provides essential security services that underpin all Grid-based applications, ensuring secure authentication, authorization, and controlled access across distributed healthcare environments.

Authentication

Authentication ensures that a user or resource is who they claim to be. The simplest form is username/password, while stronger methods use X.509 digital certificates, which bind identity to a public key and are validated by trusted third parties.

Authorization

Authorization restricts access to only approved users. It can be based on individual identities, group memberships, or roles. Once authenticated, the system decides what resources the user may access, usually under the control of the resource owner.

Shortcomings of GSI

Although GSI offers basic protection, it is limited for biomedical use. Security must be guaranteed at three levels:

Cite this article as:
Omoniyi, A.O., Oladimeji, B.J., Bamikole, O. E., & [2]Olojido, J.B. (2025). A framework for secure management of health records in grid computing environments**.** *FNAS Journal of Computing and Applications, 2*(4), 143-153. https://doi.org/10.63561/jca.v2i4.1083

Data storage (at healthcare centers).
Data transfer (movement across domains).
Data access (retrieval by authorized users).
Current grid middleware lacks strong privacy measures such as automatic pseudonymisation and improved integrity checks.
Encryption and passwords limit access but cannot stop misuse by trusted insiders. **Pseudonymisation** addresses this gap by replacing sensitive identifiers (e.g., name, SSN, address) with pseudonyms, thereby protecting patient privacy while still allowing useful analysis of the data.

Pseudonymisation
Pseudonymisation (or de-identification) separates personal identifiers from medical records.
Protected Health Information (PHI): identifiable and must be safeguarded.
De-identified data: less restricted, as it cannot directly reveal identity**..**

Pseudonymisation of Medical Records
In practice, patient-identifiable data is separated from clinical data and replaced with pseudonyms before leaving the local database. This way, researchers or external users can only access pseudonymised medical data, while only authorized healthcare providers can re-link records to real patients when necessary. The scenario in fig. 3a below shows the flow of data from a clinical database and the process of identifying the patient identifiable data and splitting them to different table in order to de-identify the record.

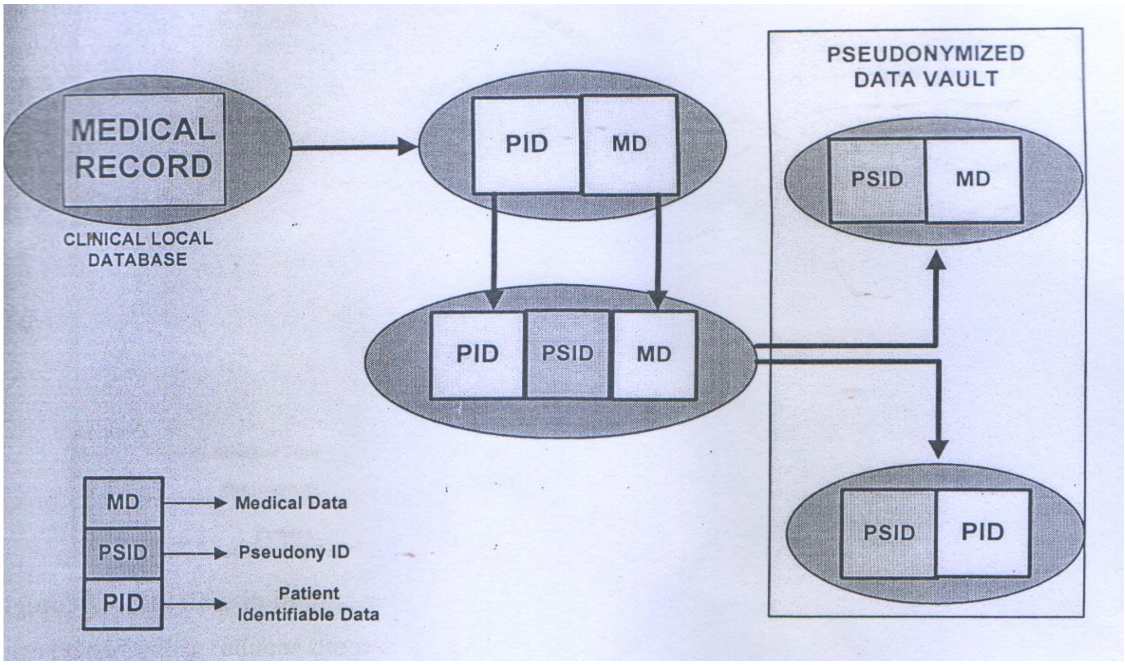

FIGURE 4: Data flow in pseudonymisation Process

PID- stands for patient identifiable data (This data include Social security Number SSN,
NHSno e.t.c which varies from one locality to another, Name),
MD- stands for medical data which are necessary for treatment or research purposes and
PSID- stands for Pseudonym ID which is later used to refer to a record.
Each patient is uniquely identified using their social security number, which is protected through **pseudonymisation**. This process occurs at points B and C (as illustrated in Figure 3b) before the information is stored in the pseudonymised data vault. To ensure complete privacy of medical records, additional security measures are necessary. These measures

Cite this article as:
Omoniyi, A.O., Oladimeji, B.J., Bamikole, O. E., & [2]Olojido, J.B. (2025). A framework for secure management of health records in grid computing environments**.** *FNAS Journal of Computing and Applications*, *2*(4), 143-153. https://doi.org/10.63561/jca.v2i4.1083

aim to prevent unauthorized users from accessing or misusing the data, even in the event that the pseudonymised vault is compromised. One effective approach is to store the data in **encrypted form**, adding an extra layer of protection against potential breaches.

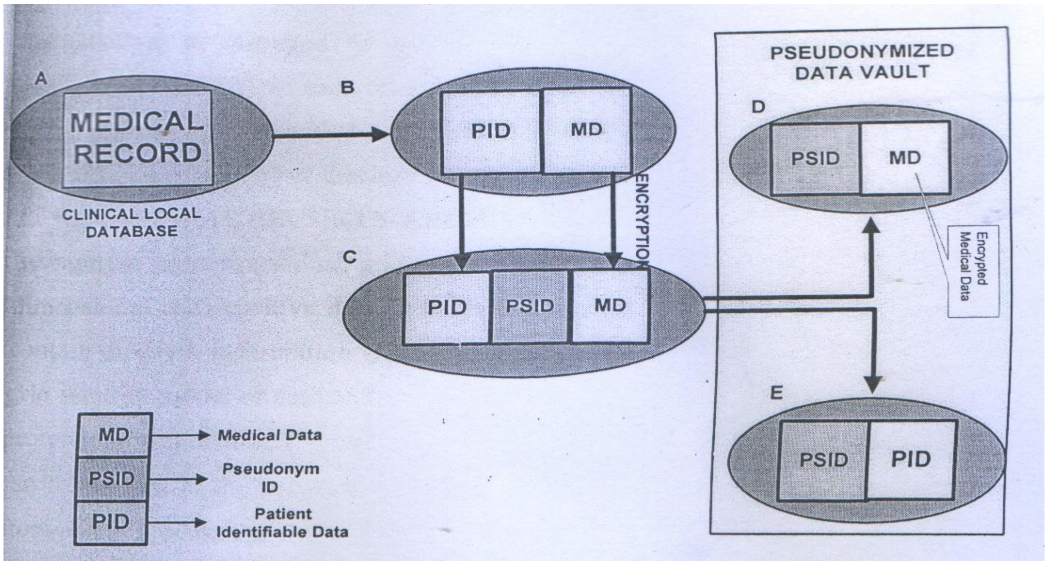

Figure4: Data flow in pseudonymisation Process.

Storing data in encrypted form significantly reduces the risk of unauthorized disclosure. However, authorized personnel must still be able to access the information when necessary, which requires secure mechanisms for granting access to decryption keys.

Encryption

Is the process of transforming information into a coded format that can only be interpreted by individuals who possess the appropriate decryption method. It is widely applied to electronic data, whether stored locally on a computer or transmitted over unsecured networks, such as the Internet. Encryption works by converting the original plaintext message into ciphertext using a specific encryption algorithm and a corresponding encryption key. Both pseudonymisation and encryption are typically performed by a legally recognized, trusted third party (TTP). In the case of reversible pseudonyms, re-identification relies on a secret key, and the pseudonymisation process is implemented as a TTP service. To ensure authorized access, decryption keys are securely stored on key servers managed by the grid service provider, while unique pseudonyms are assigned to each record by the TTP. A pseudonym serves to represent an individual or group of individuals without revealing their true identities, thus preserving privacy while allowing authorized personnel to access and use the data in a controlled and secure manner.

General Security Architecture

Medical applications differ from conventional grid applications because they involve high-dimensional, heterogeneous, and highly sensitive dat**a** with varying privacy requirements. A grid security model must therefore guarantee reliable data protection, prevent unauthorized access, and establish trust between patients and healthcare providers—trust that encourages patient consent for data storage and research use while safeguarding patient rights.

To achieve this, the Grid Security Infrastructure (GSI) combines core mechanisms—authentication, authorization, and accounting—with additional measures such as pseudonymisation and encryption. Pseudonymisation can be performed either at the medical source (e.g., hospital administrator) or through a trusted third party (TTP) before data is stored on the grid.

To improve both security and system reliability, a distributed key management approach is recommended, rather than depending on a single key server, which may introduce bottlenecks and become a potential point of vulnerability.

Cite this article as:
Omoniyi, A.O., Oladimeji, B.J., Bamikole, O. E., & ^{2}Olojido, J.B. (2025). A framework for secure management of health records in grid computing environments**.** *FNAS Journal of Computing and Applications*, *2*(4), 143-153. https://doi.org/10.63561/jca.v2i4.1083

(e.g., denial-of-service or targeted attacks). In this approach, decryption and re-identification keys are divided into **shares** and stored across multiple independent key servers. Access to a record requires a minimum number (*m*) of shares, ensuring that even if some servers fail or are compromised, security and availability are maintained.

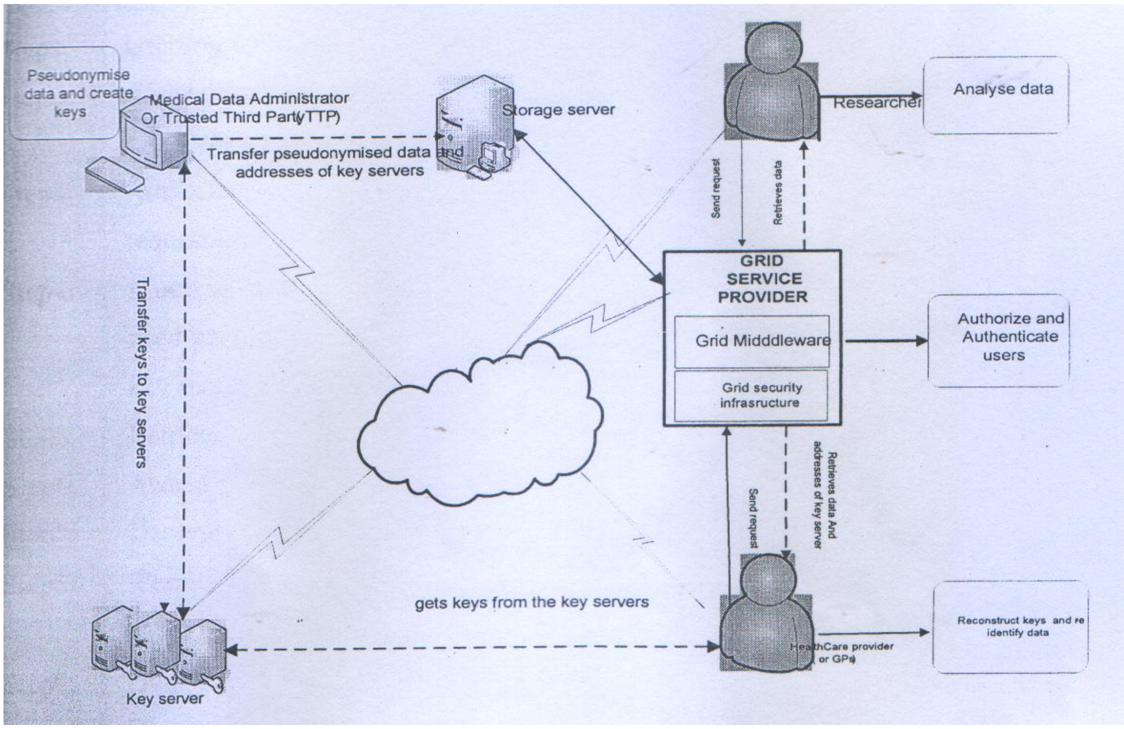
Pseudonymise data and create keys
Medical Data Administrator Or Trusted Third Party(TTP)
Storage server
Transfer pseudonymised data and addresses of key servers
Researcher
Analyse data
Send request
Retrieves data
GRID SERVICE PROVIDER
Grid Midddleware
Grid security infrasructure
Authorize and Authenticate users
Transfer keys to key servers
Send request
Retrieves data And addresses of key server
gets keys from the key servers
Reconstruct keys and re identify data
HealthCare provider or GPs
Key server

Figure 5: Security Architecture.

Before any service is performed in grid, a user has to be authenticated by the grid security infrastructure by the use of X.509 certificate or simple username/password mechanism. It is not enough to be authenticated; the access to any data in the grid has to be by permission or right to access. The process by which the authority or right over a particular data is determined is known as authorization as discussed in section 3.4. Access to data is given based on the level of authority. For example in the architecture above, if a medical practitioner or care provider request for a patient record, because he is likely to need the medical history of that patient before any treatment commenced, he is given the permission to retrieve the pseudonymised record and the addresses of the key servers, he gets the keys from the servers, reconstruct and re-identify the record. In the case of a researcher, he is only given access to psuedonymised data because he is not likely to need the full information about the patient for any research work. The algorithm below shows a step by step procedures involved in any grid activity.

Algorithm: Secure Access to Medical Records in a Grid Environment

Step 1: User logs on to the grid.
Step 2: Authenticate the user (via username/password or X.509 digital certificate).
Step 3: Authorize the user (access rights determined by the user's role).
Step 4: If the user is a *care provider* (requires patient record for treatment), then:
Step 5: The system provides the location of the decryption key on the key server.
Step 6: The user retrieves the decryption key from the key server to access the encrypted data.
Step 7: Access is granted to the storage server.
Step 8: Decrypt the retrieved data.
Step 9: Permission is granted to re-identify pseudonymised data (by mapping identifiers to pseudonyms).
Step 10: Proceed to Step 14.
Step 11: If the user is a *researcher* (requires data for research purposes), then:
Step 12: The system supplies the location of the decryption key stored on the key server.

Step 13: The user accesses the key server to obtain the decryption key.
Step 14: The user retrieves the encrypted medical data from the storage server.
Step 15: Permission to re-identify data is denied.
Step 16: Log all activities performed by every user (accountability).
Step 17: Exit the application.

Algorithm:
Secure Access to Medical Records in a Grid Environment
Step 1: The user initiates a login session on the grid platform.
Step 2: The system performs authentication using credentials such as a username/password pair or an X.509 digital certificate.
Step 3: Authorization is applied, where access rights are determined according to the user's assigned role.
Step 4: If the authenticated user is a healthcare provider requiring patient records for clinical care:
Step 5: The system provides the location or reference to the decryption key, which is securely stored on the key server.
Step 6: The user accesses the key server to obtain the decryption key required to decode the data. **Step 7:** Access is granted to the storage server containing the patient records.
Step 8: The encrypted data is decrypted for use.
Step 9: Re-identification of pseudonymised data is permitted by linking the pseudonymised fields with the original identifiers.
Step 10: Proceed to logging and exit.
Step 11: If the authenticated user is a **researcher** requiring data for research purposes:
Step 12: The system provides the user with the location of the decryption key stored on the key server. Step 13**:** The user retrieves the decryption key.
Step 14: The encrypted data is retrieved from the storage server.
Step 15: Re-identification of patient data is strictly denied.
Step 16: All user activities are logged to ensure accountability and auditing.
Step 17: The session ends, and the application is closed.

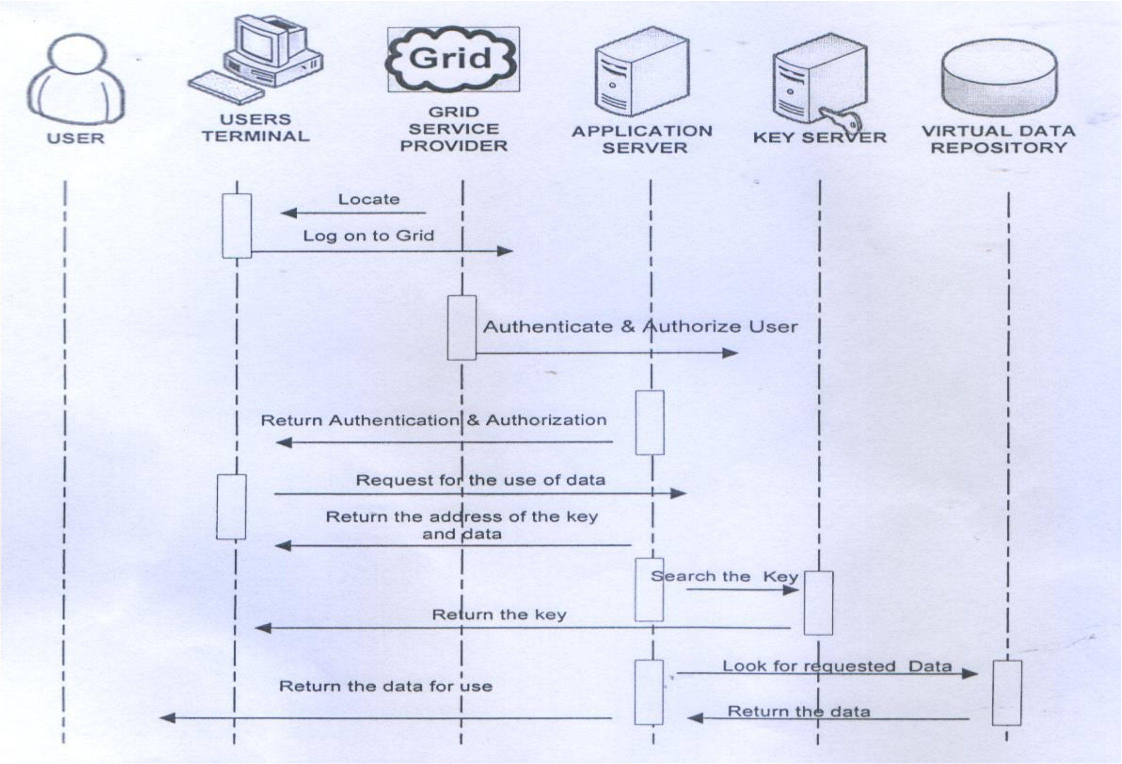

Figure 6: Information Request Message Flow

Cite this article as:
Omoniyi, A.O., Oladimeji, B.J., Bamikole, O. E., & ^{2}Olojido, J.B. (2025). A framework for secure management of health records in grid computing environments**.** *FNAS Journal of Computing and Applications*, *2*(4), 143-153. https://doi.org/10.63561/jca.v2i4.1083

The information request message flow represents system behavior as a sequence of steps carried out over time. It illustrates how workflows, message exchanges, and system components interact to achieve a desired outcome. When a user logs into the healthgrid service, their credentials are transmitted over the network to the application and service layer, where the Grid Security Infrastructure (GSI) is hosted through the Grid Service Provider. This layer handles both authentication and authorization. Once the user is successfully authenticated, they can submit a request for access to data and its corresponding decryption key. The system provides the address of the relevant key stored on the key server, which the user retrieves to decrypt the requested data. Simultaneously, the system grants controlled access to the data repository, enabling the user to obtain the authorized medical records.

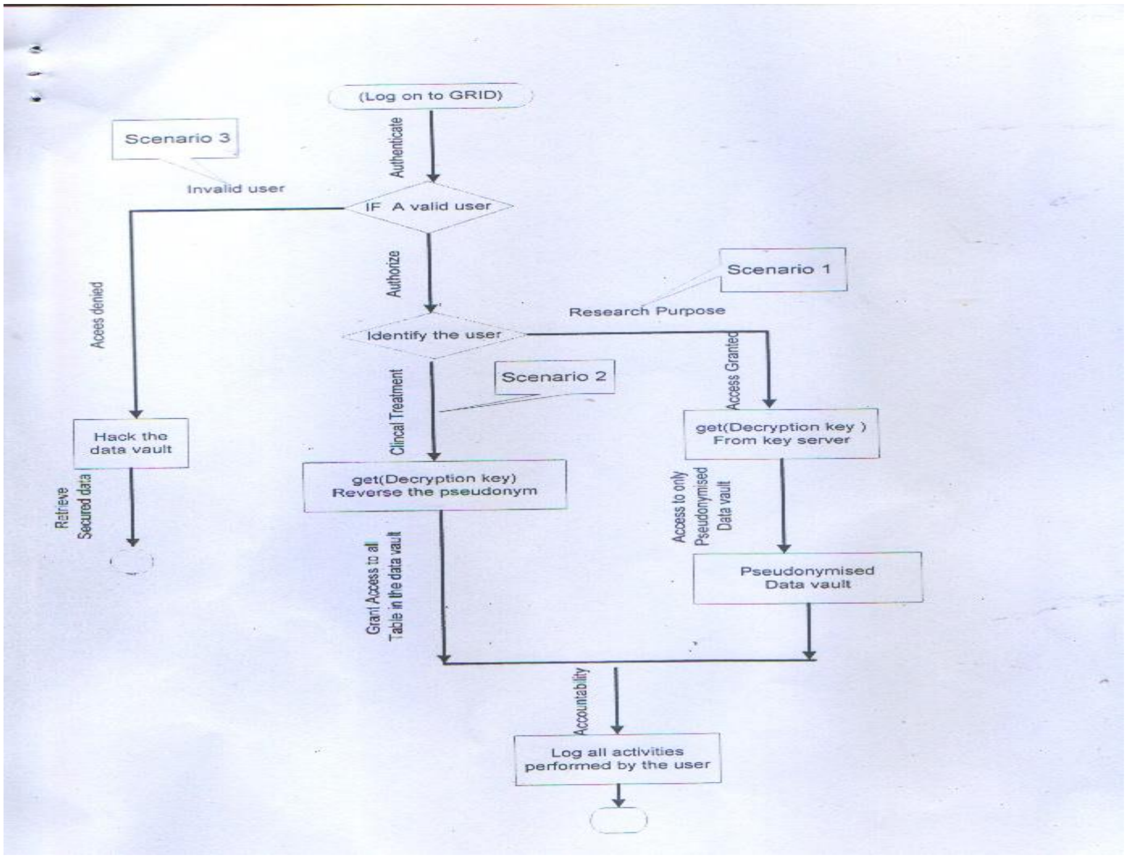

Fig 7: Process Flowchart.

Discussion

The proposed model demonstrates how medical information can be safeguarded by restricting unauthorized access and separating patient identifiers from clinical data. This separation minimizes the risk of linking a patient's identity to their health records in the event of data leakage or a system breach. The security architecture presented in the preceding chapter outlines multiple strategies for protecting medical records within a grid environment. These strategies build on the core features of grid security infrastructure—such as authentication, authorization, and accountability**—**while integrating pseudonymisation at the point of data storage, typically within healthcare centers or clinical databases. Within this framework, when a healthcare provider or medical practitioner requests a patient's record for treatment, the system grants access to the pseudonymised record along with references to the key servers. Using the decryption keys, the provider can reconstruct and re-identify the patient's full record as needed for clinical care. Conversely, researchers are limited to pseudonymised data only, since full patient identifiers are not required for research purposes. The accompanying figure illustrates the information flow of this security architecture under three

Cite this article as:
Omoniyi, A.O., Oladimeji, B.J., Bamikole, O. E., & ^{2}Olojido, J.B. (2025). A framework for secure management of health records in grid computing environments**.** *FNAS Journal of Computing and Applications, 2*(4), 143-153. https://doi.org/10.63561/jca.v2i4.1083

different scenarios, highlighting how the model enforces **role-**based access, privacy protection, and controlled re-identification**.**

Scenario 1: shows the information process of the request made by researcher. After authenticated and authorized and authorized by service provider and the identity is known as a valid user and researcher. A limited access is given to the pseudonymized data vault at point D (as shown in figure 4b) with encryption key to decrypt the medical data

Scenario 2: in this case request is made by healthcare provider for clinical treatment. It is easy to access a local database and get patient medical records provided that the patient requested for care in a health care centre where he/she has registered for a treatment. In the case of requesting for medical treatment in another health care centre within the collaboratory grid, then there is need for re-identification to have full access to patient record. This is done by giving access to table at point D and E from 4b above and reverses the pseudonym. All these are achieved through the application layer of the grid after proper authentication and authorization.

Scenario 3: Provided that the hacker maneuvers its way to the data vault due to unsecured network connection, then information retrieved will be of no use due to lack of decryption key and re-identification keys.

to gain wider adoption, these security concerns must be thoroughly addressed.

Conclusion

The system enhances patient privacy and plays a crucial role in reinforcing trust in e-health services. However, factors such as the system's complexity, the large user base, and the substantial volume of clinical data significantly increase the potential security risks.. By incorporating privacy-preserving measures, particularly **pseudonymisation**, the solution helps reduce unauthorized access and ensures that only healthcare providers can link sensitive data back to individual patients.

Recommendation

In order to achieve to secure medical record within a grid environment, it is recommended that medical data should be encrypted and also only pseudonymized data should be transferred to the data repository to restrict the>access of some user to particular information.

References

Abbas, S. R., Abbas, Z., Zahir, A., & Lee, S. W. (2024). Federated learning in smart healthcare: A comprehensive review on privacy, security, and predictive analytics with IoT integration. Healthcare, 12(24), 2587. https://doi.org/10.3390/healthcare12242587

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2023). Big data security and privacy in healthcare: A review. Journal of Medical Systems, 47(2), 1–15. https://doi.org/10.1007/s10916-023-1763-5

Ali, M. S., Ahsan, M. M., Tasnim, L., Afrin, S., Biswas, K., Hossain, M. M., & Islam, M. K. (2024). Federated learning in healthcare: Model misconducts, security, challenges, applications, and future research directions—A systematic review. arXiv. https://arxiv.org/abs/2405.13832

IBM Security. (2023). Cost of a data breach report 2023. IBM. https://www.ibm.com/reports/data-breach

Prayitno, F., Shyu, C.-R., Trinanda Putra, K., Chen, H.-C., Tsai, Y.-Y., Tozammel Hossain, K. S. M., & Shae, Z.-Y. (2023). A systematic review of federated learning in the healthcare area: From the perspective of data properties and applications. Applied Sciences, 11(23), Article 11191. https://doi.org/10.3390/app112311191

Teo, Z. L., Jin, L., Li, S., Miao, D., Zhang, X., Ng, W. Y., Tan, T. F., Lee, D. M., Chua, K. J., Heng, J., Liu, Y., Goh, R. S. M., & Ting, D. S. W. (2024). Federated machine learning in healthcare: A systematic review on clinical applications and technical architecture. Cell Reports Medicine, 5(2), 101419. https://doi.org/10.1016/j.xcrm.2024.101419

The ORCHESTRA Consortium. (2024). A scalable pseudonymization tool for rapid deployment in large biomedical research networks: Development and evaluation study. JMIR Medical Informatics, 12, e49646. https://doi.org/10.2196/49646

Upreti, S., et al. (2024). A comprehensive survey on federated learning in the healthcare area: Concept and applications. CMES - Computer Modeling in Engineering & Sciences, 140(3), 2239–2274. https://doi.org/10.32604/cmes.2024.048932

Wani, R. U. Z., & Can, O. (2025). FED-EHR: A privacy-preserving federated learning framework for decentralized healthcare analytics. Electronics, 14(16), 3261. https://doi.org/10.3390/electronics14163261

World Health Organization. (2024). Global digital health security framework. https://www.who.int/publications

Cite this article as:
Omoniyi, A.O., Oladimeji, B.J., Bamikole, O. E., & [2]Olojido, J.B. (2025). A framework for secure management of health records in grid computing environments**.** *FNAS Journal of Computing and Applications, 2*(4), 143-153. https://doi.org/10.63561/jca.v2i4.1083