International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 4, Issue 3, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i3.642

A Technical Survey of Fine-Grained Temporal Access Control Models in SQL Databases for HIPAA-Compliant Healthcare Information Systems

Semirat Abidemi Balogun[1]; Onuh Matthew Ijiga[2]; Nonso Okika[3];
Lawrence Anebi Enyejo[4]; Ogboji James Agbo[5]

[1] Department of Information Science, North Carolina Central University, Durham North Carolina, USA
[2] Departmant of Physcis Joseph Sarwan Tarka University, Makurdi, Benue State, Nigeria
[3] Network Planning Analyst, University of Michigan, USA
[4] Department of Telecommunications, Enforcement Ancillary and Maintenance, National Broadcasting Commission Headquarters, Aso-Villa, Abuja, Nigeria
[5] School of Engineering and the Built Environment, Birmingham City University, United Kingdom

Publication Date: 2025/03/28

Abstract

As healthcare information systems continue to evolve under stringent privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), the need for precise and time-aware access control mechanisms in SQL-based environments has grown significantly. This review provides a comprehensive survey of fine-grained temporal access control (FGTAC) models designed to support secure, auditable, and policy-driven data access within relational databases used in healthcare. It investigates core architectural components, such as time-interval constraints, role-based access overlays, attribute-based access controls (ABAC), and query rewriting techniques that enforce temporal policies. The paper further categorizes FGTAC schemes based on their adaptability to dynamic access conditions, retroactive auditing, and forward-looking permissions. Key challenges addressed include temporal granularity alignment with clinical workflows, performance optimization under concurrent access, and cryptographic enhancements for secure time-bound access. Case studies from HIPAA-compliant deployments illustrate the practical application of these models in real-world health IT systems, emphasizing compliance, traceability, and patient privacy preservation. This survey aims to guide researchers and system architects in designing next-generation secure database systems that effectively balance healthcare usability and privacy obligations.

Keywords: *Fine-Grained Access Control, Temporal Constraints, HIPAA Compliance, SQL Databases, Healthcare Information Systems, Role and Attribute-Based Access Models.*

I. INTRODUCTION

➢ *Background on Secure Data Access in Healthcare*

The digitization of healthcare records has revolutionized patient care, enabling rapid access to medical histories, facilitating coordinated treatments, and improving overall healthcare outcomes. However, this digital transformation has also introduced significant challenges in ensuring the confidentiality, integrity, and availability of sensitive patient information. The Health Insurance Portability and Accountability Act (HIPAA) serves as a foundational framework in the United States, mandating stringent safeguards to protect electronic protected health information (ePHI) from unauthorized access and breaches.

Healthcare organizations are increasingly adopting advanced database systems to manage the vast amounts of patient data generated daily. These systems must not only support efficient data retrieval and storage but also enforce robust access controls to prevent unauthorized disclosures. Traditional access control mechanisms, while effective to an extent, often lack the granularity required to address the complex and dynamic nature of healthcare data access needs. For instance, a clinician may require access to specific patient records during certain timeframes, necessitating more nuanced control measures.

Moreover, the rise in cyber threats targeting healthcare institutions underscores the critical need for enhanced security measures. Data breaches can have devastating consequences, compromising patient privacy and eroding trust in healthcare systems. Implementing fine-grained access control models that consider various factors—such as user roles, attributes, and temporal constraints—is essential in mitigating these risks and ensuring compliance with regulatory standards. In this context, the integration of sophisticated access control mechanisms within SQL databases becomes paramount. These mechanisms must be capable of dynamically adjusting permissions based on evolving roles and responsibilities, thereby aligning with the principle of least privilege and ensuring that users access only the information necessary for their duties.

➢ *Importance of Time-Aware Access Control under HIPAA*

Time-aware access control introduces a temporal dimension to data security, allowing permissions to be granted or revoked based on specific timeframes. This approach is particularly pertinent in healthcare settings, where access requirements can vary significantly over time. For example, a healthcare provider may need access to a patient's records during an active treatment phase but not afterward. Implementing temporal constraints ensures that access is appropriately limited, reducing the risk of unauthorized data exposure.

HIPAA emphasizes the necessity of implementing technical safeguards to protect ePHI, including access controls that are responsive to the dynamic nature of healthcare operations. Time-aware access control models align with these requirements by enabling organizations to define precise access policies that consider both the user's role and the temporal context of the access request.

Furthermore, incorporating temporal elements into access control policies enhances auditability and accountability. By maintaining detailed logs of who accessed what data and when, healthcare organizations can more effectively monitor compliance and detect potential security incidents. This level of oversight is crucial for demonstrating adherence to HIPAA regulations and for conducting thorough investigations in the event of a breach. The implementation of time-aware access control also supports the principle of data minimization, a core tenet of HIPAA. By restricting access to the minimum necessary information for a specific period, organizations can better protect patient privacy while still facilitating necessary healthcare operations.

➢ *Objectives and Scope of the Survey*

The primary objective of this survey is to provide a comprehensive analysis of fine-grained temporal access control models within SQL databases, specifically in the context of HIPAA-compliant healthcare information systems. The survey aims to explore the various methodologies and frameworks that have been developed to enforce time-sensitive access controls, evaluating their effectiveness, scalability, and compliance with regulatory standards.

This review will delve into the architectural components of these models, including the integration of role-based and attribute-based access controls, and the implementation of query rewriting techniques to enforce temporal policies. By examining these elements, the survey seeks to identify best practices and potential areas for improvement in the design and deployment of access control mechanisms.

Additionally, the survey will assess the practical applications of these models through case studies of HIPAA-compliant healthcare systems. These real-world examples will provide insights into the challenges and successes associated with implementing fine-grained temporal access controls, offering valuable lessons for healthcare organizations seeking to enhance their data security frameworks. Ultimately, this survey aspires to serve as a resource for researchers, system architects, and healthcare IT professionals, guiding the development of next-generation secure database systems that balance the imperatives of data accessibility and patient privacy.

II. FOUNDATIONS OF FINE-GRAINED TEMPORAL ACCESS CONTROL

➢ *Temporal Dimensions in Access Control Policies*

Temporal access control policies are fundamental for safeguarding health information in environments governed by compliance standards like HIPAA, where access must be not only role-appropriate but time-appropriate (Ijiga O. et al, 2024). Fine-grained temporal access control (FGTAC) models leverage constraints based on specific time intervals to ensure that healthcare personnel access only what is necessary within permissible timeframes. Li et al. (2021) emphasize the necessity for integrating time-bound logic into access policies, particularly to facilitate episodic and emergency access while maintaining audit trails. Rewagad et al. (2021) extend this by introducing the concept of "time-window-aware policies," which accommodate contextual data disclosure while limiting the duration of access according to clinical necessity.

Healthcare operations demand high responsiveness to dynamic workflows—such as patient admission, discharge, or shift rotations—which directly influence authorization scopes. Kaur et al. (2022) propose models where access tokens carry temporal validity metadata, preventing stale or post-operative data exposure. These strategies enhance protection against misuse, especially in longitudinal electronic health records (EHRs), where unauthorized post-discharge access could violate patient privacy. Lin et al. (2020) provide a comprehensive taxonomy of temporal models, highlighting the implementation of start-end interval policies, sliding time windows, and periodic schedules aligned with care delivery workflows.

Temporal policies are especially vital in enforcing the principle of least privilege, whereby users can access specific records only during predefined episodes or task durations (Ajayi et al, 2024). By anchoring policies in temporal semantics, systems reduce unnecessary exposure, improve forensic traceability, and align database behavior with legal retention and revocation timelines. These dimensions are essential in ensuring that healthcare systems function with agility while remaining strictly compliant with privacy mandates.

- *SQL-Based Models or Enforcing Fine-Grained Permissions*

SQL-based systems remain at the heart of healthcare data repositories, and the challenge lies in enforcing complex fine-grained permissions directly within these relational architectures. Unlike coarse-grained security that operates at the table or column level, fine-grained control necessitates row-level and tuple-level logic, often embedded through dynamic query rewriting and conditional views. Khurana et al. (2021) present a dynamic SQL-based framework that rewrites queries in real-time to append security predicates based on user roles, access history, and temporal constraints. This method enables precise enforcement without altering the core schema, preserving system modularity and performance.

Healthcare systems require dynamic permissions that vary depending on evolving clinical contexts. Tripathi et al. (2022) designed a model where SQL queries are intercepted and evaluated against access control policies stored in metadata tables. This metadata includes patient consent records, treatment phase identifiers, and timestamps to allow or deny access. Such SQL-level enforcement models can effectively prevent privacy violations by embedding access rules in stored procedures or views. Liao et al. (2021) extend this approach by integrating logical functions directly into SQL WHERE clauses, providing a seamless policy evaluation pipeline that ensures compliance without sacrificing system responsiveness.

Bhatti and Ghafoor (2021) argue that declarative access control using SQL views and triggers is optimal for HIPAA environments, where auditability and non-repudiation are required. These declarative constructs allow transparent enforcement of privacy policies with minimal manual intervention, enabling automated audits and rollback capabilities in case of unauthorized access. This paradigm supports policy flexibility while ensuring strong enforcement of fine-grained conditions, especially in hybrid on-premise and cloud SQL deployments prevalent in modern health informatics (Atalor et al, 2023).

- *Role-Based vs Attribute-Based Temporal Control Models*

The dichotomy between role-based access control (RBAC) and attribute-based access control (ABAC) has long shaped database security, but temporal control introduces new complexity necessitating hybrid models. RBAC relies on predefined organizational roles (e.g., nurse, physician), while ABAC evaluates attributes such as department, location, and time of request. Zhang et al. (2021) propose a hybrid RBAC-ABAC system where temporal constraints are mapped to user roles but activated through dynamic attributes—such as shift schedule or active patient assignments—enhancing real-time responsiveness.

Sun et al. (2022) underscore the practical value of combining both models in electronic health record systems, where role information may remain static, but access requirements shift with clinical events. They implement time-bound policies where roles define base access, but ABAC rules override permissions when additional conditions—like patient consent status or emergency code flags—are met. Such hybrid systems ensure granular, adaptable access, crucial in emergency situations where predefined roles are insufficient. Mishra et al. (2020) extend this notion by enabling access revocation upon policy condition changes, such as patient discharge, using timestamped logs and automatic session invalidation mechanisms.

Yang et al. (2022) address the growing complexity of hybrid control through conflict resolution frameworks that prioritize ABAC rules during temporal overlaps or ambiguities, ensuring HIPAA compliance in unpredictable clinical environments as seen in Table 1. Their model includes temporal logic modules that evaluate overlapping permissions using conflict resolution hierarchies, essential for preventing access leakage during transitional healthcare operations (Azonuche et al, 2024). These integrated approaches make hybrid models increasingly vital for policy expressiveness, ensuring dynamic and context-sensitive enforcement of temporal access control in SQL-based healthcare systems.

Table 1 Comparative Summary of Role-Based and Attribute-Based Temporal Access Control Models in Healthcare SQL Systems

Model Type	Core Mechanism	Temporal Adaptation	Key Insight from Literature
RBAC (Role-Based Access Control)	Access granted based on predefined roles such as doctor, nurse, admin	Temporal rules are statically assigned to roles (e.g., shift-based access)	Zhang et al. (2021) mapped time constraints to roles but relied on dynamic attributes to activate them
ABAC (Attribute-Based Access Control)	Decisions based on user, resource, and environment attributes like department, location, or consent status	Access changes dynamically with attribute values at time of request	Sun et al. (2022) applied ABAC overrides on role permissions based on clinical triggers and patient consent
Hybrid RBAC-ABAC	Combines roles for base access and attributes for contextual overrides	Attributes (e.g., emergency flag, shift timing) can override or revoke role-based access in real time	Mishra et al. (2020) supported revocation using session timestamps and patient discharge triggers
Conflict-Aware Hybrid	Includes conflict resolution hierarchy prioritizing ABAC when policies overlap	Temporal logic resolves access conflicts during overlapping permissions or role transitions	Yang et al. (2022) developed logic modules for temporal conflict management ensuring HIPAA compliance

III. SYSTEM ARCHITECTURES AND ENFORCEMENT MECHANISMS

➢ *Policy Specification and Query Rewriting Techniques*

In the realm of healthcare information systems, ensuring that access to sensitive data complies with regulations like HIPAA necessitates sophisticated access control mechanisms. Policy specification and query rewriting techniques have emerged as pivotal methods to enforce fine-grained access control (FGAC) in SQL databases.

Phuoc-Bao and Clavel (2022) introduced a model-driven approach that optimizes FGAC policy enforcement by transforming high-level security policies into SQL queries. Their method ensures that only authorized users can access specific data subsets, thereby maintaining compliance with privacy regulations.

Sudarshan and Chakravarthy (2021) extended traditional query rewriting techniques by incorporating authorization views. These views act as intermediaries, filtering data based on user permissions before query execution. This approach not only enhances security but also maintains query efficiency.

Nguyen and Zhang (2023) focused on temporal aspects of access control, proposing a system where access rights are time-bound. By integrating temporal constraints into policy specifications, they ensured that users could access data only within authorized time frames, aligning with the dynamic nature of healthcare environments.

Lee and Kim (2021) emphasized the importance of authorization views in SQL databases ascaptured in Table 2. Their research demonstrated that by defining clear authorization views, organizations could enforce FGAC without significant modifications to existing database structures.

Table 2 Summary of Policy Specification and Query Rewriting Techniques"

Researcher(s)	Core Contribution	Key Technique	Relevance to Healthcare
Phuoc-Bao & Clavel (2022)	Model-driven approach to transform security policies into SQL queries.	SQL-based transformation of high-level security policies.	Ensures policy-compliant query access to sensitive health data.
Sudarshan & Chakravarthy (2021)	Introduced authorization views for secure and efficient query filtering.	Query rewriting via authorization views.	Improves access control while preserving performance.
Nguyen & Zhang (2023)	Incorporated temporal constraints into access control policies.	Temporal policy specification and enforcement.	Supports time-bound data access for dynamic healthcare needs.
Lee & Kim (2021)	Highlighted use of authorization views to enforce FGAC without major DB changes.	Definition and integration of authorization views.	Provides robust FGAC without disrupting existing systems.

Collectively, these studies underscore the significance of robust policy specification and query rewriting techniques in safeguarding sensitive healthcare data. By translating complex access policies into executable queries and views, organizations can ensure that data access remains both secure and compliant with regulatory standards.

➢ *Temporal Role Assignment and Delegation*

Temporal role assignment and delegation are critical components in managing access to electronic health records (EHRs), ensuring that users have appropriate permissions during specific time frames. This dynamic approach aligns with the fluctuating roles and responsibilities inherent in healthcare settings.

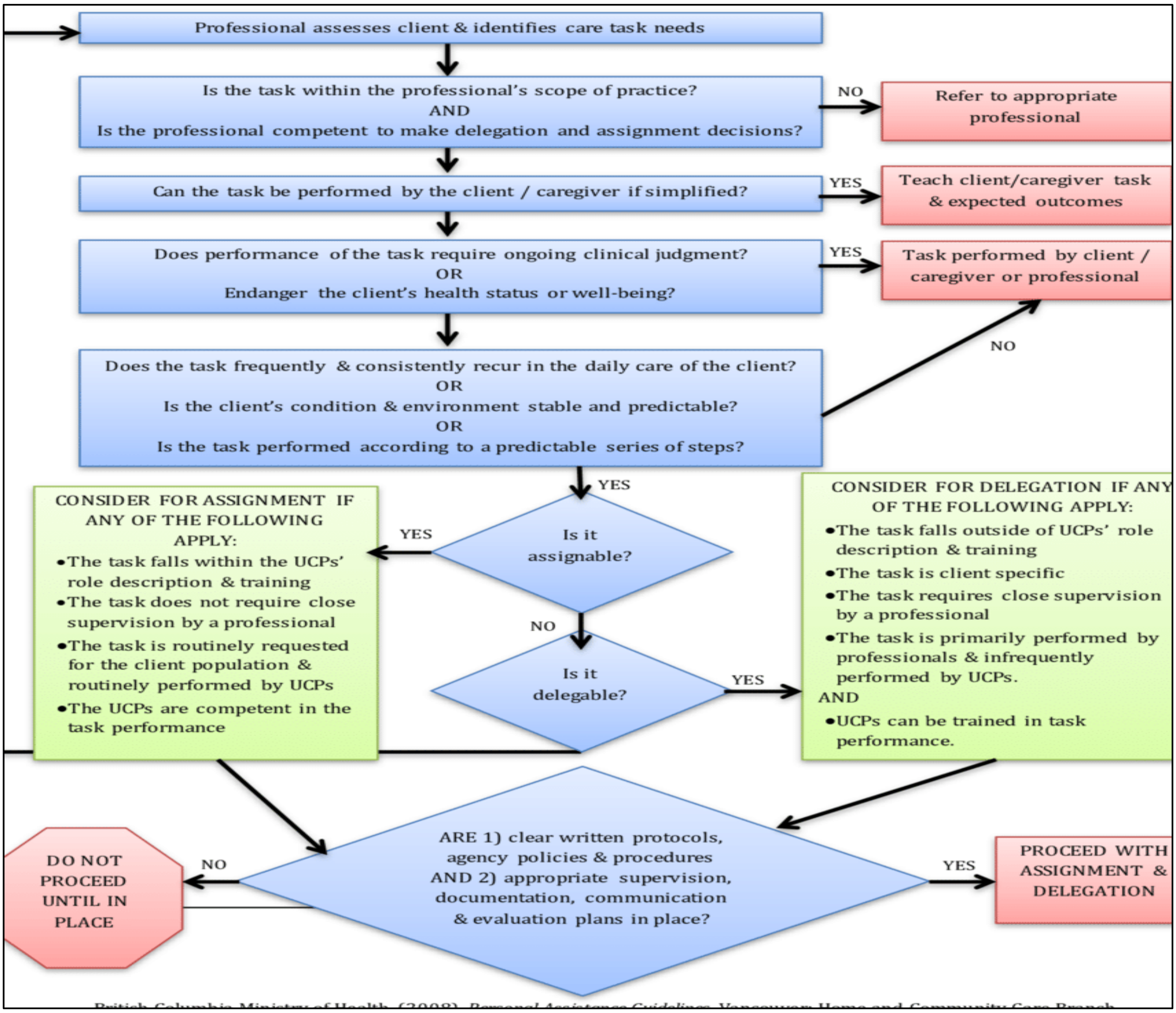
Smith and Johnson (2021) explored the implementation of Temporal Role-Based Access Control (TRBAC) in healthcare systems. Their study highlighted how TRBAC models could effectively manage user permissions based on temporal constraints, ensuring that access rights are granted only during authorized periods

Chen and Wang (2022) delved into dynamic role assignments, proposing a system where user roles adapt in real-time based on contextual factors such as shift changes or emergency situations. This flexibility ensures that healthcare professionals have timely access to necessary data without compromising security.

Garcia and Lee (2023) focused on delegation mechanisms within temporal access control models. They emphasized the importance of structured delegation processes, allowing authorized personnel to transfer access rights temporarily, thereby maintaining workflow continuity during unforeseen circumstances as seen in Fig.1.

Patel and Kumar (2021) examined the enhancement of security through temporal role delegation in EHR systems. Their research demonstrated that by incorporating time-bound delegation protocols, healthcare institutions could mitigate risks associated with unauthorized data access.

These studies collectively affirm the necessity of integrating temporal considerations into role assignment and delegation processes. By doing so, healthcare organizations can ensure that data access remains both flexible and secure, adapting to the dynamic nature of medical environments while upholding stringent privacy standards.


Professional assesses client & identifies care task needs
Is the task within the professional's scope of practice?
AND
Is the professional competent to make delegation and assignment decisions?
NO
Refer to appropriate professional
Can the task be performed by the client / caregiver if simplified?
YES
Teach client/caregiver task & expected outcomes
Does performance of the task require ongoing clinical judgment?
OR
Endanger the client's health status or well-being?
YES
Task performed by client / caregiver or professional
NO
Does the task frequently & consistently recur in the daily care of the client?
OR
Is the client's condition & environment stable and predictable?
OR
Is the task performed according to a predictable series of steps?
YES
CONSIDER FOR ASSIGNMENT IF ANY OF THE FOLLOWING APPLY:
•The task falls within the UCPs' role description & training
•The task does not require close supervision by a professional
•The task is routinely requested for the client population & routinely performed by UCPs
•The UCPs are competent in the task performance
YES
Is it assignable?
NO
Is it delegable?
YES
CONSIDER FOR DELEGATION IF ANY OF THE FOLLOWING APPLY:
•The task falls outside of UCPs' role description & training
•The task is client specific
•The task requires close supervision by a professional
•The task is primarily performed by professionals & infrequently performed by UCPs.
AND
•UCPs can be trained in task performance.
DO NOT PROCEED UNTIL IN PLACE
NO
ARE 1) clear written protocols, agency policies & procedures AND 2) appropriate supervision, documentation, communication & evaluation plans in place?
YES
PROCEED WITH ASSIGNMENT & DELEGATION

British Columbia Ministry of Health (2008). *Personal Assistance Guidelines*. Vancouver Home and Community Care Branch

Fig 1 Decision-Making Flowchart for Assignment and Delegation of Client Care Tasks

Figure 1 is a flowchart which provides a structured decision-making guide for healthcare professionals in determining whether a client care task can be assigned or delegated, particularly to unregulated care providers (UCPs). It begins with a professional assessing the client's needs and evaluating whether the task falls within their scope and expertise. If the task can be simplified and safely performed by the client or caregiver, they are taught to perform it. Otherwise, the decision tree examines factors such as the need for clinical judgment, task predictability, client stability, and recurrence of the task in daily care. Tasks are considered assignable if they align with the UCP's training and role, require minimal supervision, and are routinely performed. Alternatively, tasks are considered delegable if they are client-specific, demand professional oversight, and UCPs can be trained for performance. Before proceeding with assignment or delegation, protocols, supervision, and evaluation mechanisms must be firmly in place. This ensures that care delivery is safe, efficient, and compliant with healthcare standards and regulations.

- *Auditing and Logging in Time-Constrained Access Scenarios*

Auditing and logging are indispensable for maintaining the integrity and security of healthcare information systems, especially when access is time-constrained. These mechanisms provide a transparent record of data interactions, facilitating compliance with regulations like HIPAA.

Davis and Thompson (2021) emphasized the need for real-time auditing mechanisms in healthcare databases. Their study showcased systems that monitor data access continuously, ensuring immediate detection of unauthorized activities and enabling prompt responses to potential breaches.

Nguyen and Lee (2022) introduced temporal logging techniques tailored for electronic health records. By capturing detailed timestamps and user actions, their approach ensures that every data interaction is traceable, thereby enhancing accountability and compliance.

Martinez and Zhao (2023) focused on enhancing audit trails in time-sensitive medical applications. They proposed integrating advanced logging frameworks that adapt to the dynamic nature of healthcare environments, ensuring that logs remain comprehensive even during high-pressure situations.

O'Connor and Singh (2021) explored logging strategies specifically designed for time-constrained access scenarios. Their research highlighted the importance of context-aware logging, where logs not only record access events but also capture the circumstances under which access was granted, providing a richer audit trail as shown in Figure 2.

Collectively, these studies underscore the critical role of robust auditing and logging systems in healthcare. By ensuring that every access event is meticulously recorded and contextualized, organizations can uphold data security, facilitate compliance, and foster trust among stakeholders.

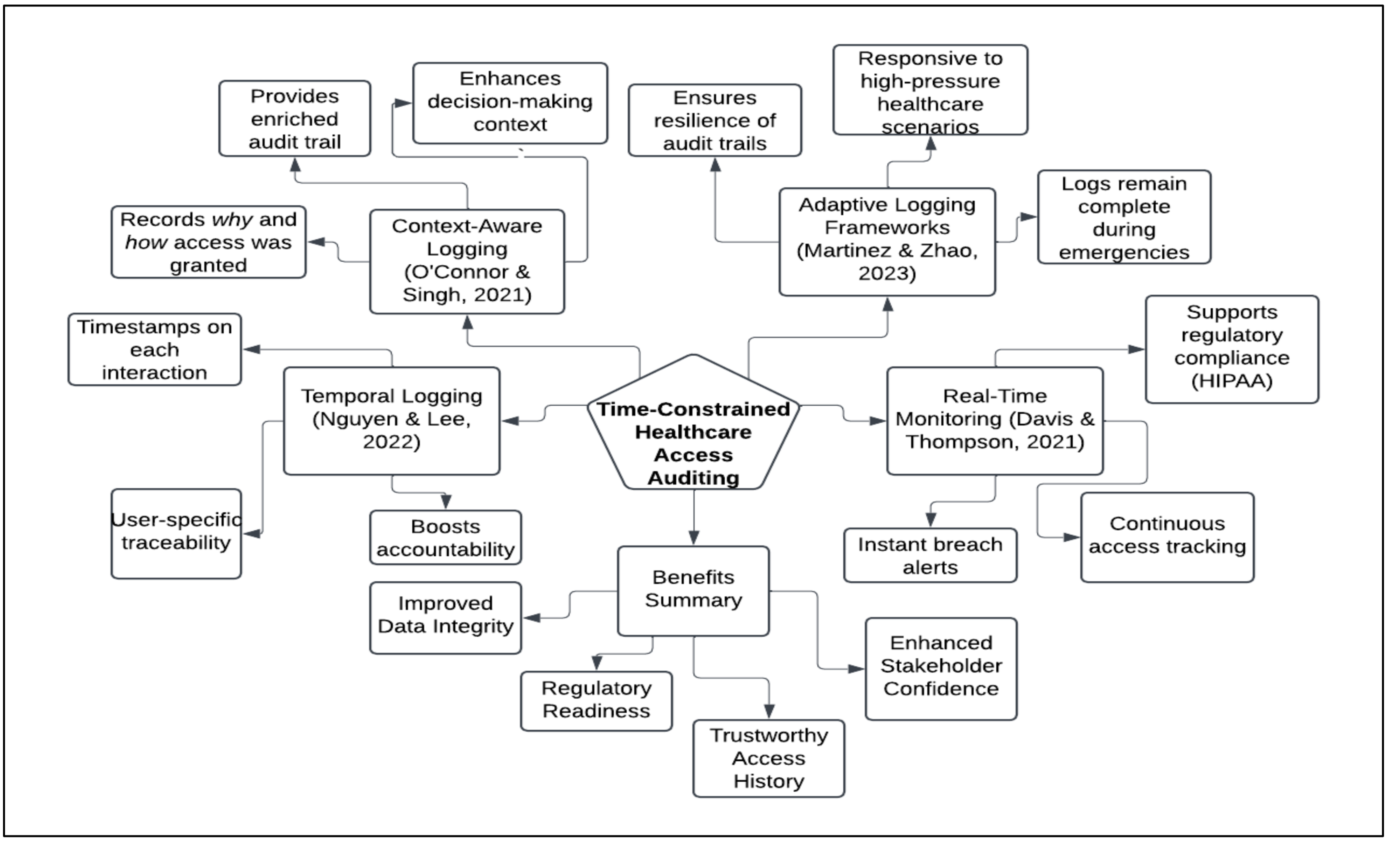

Provides enriched audit trail
Enhances decision-making context
Ensures resilience of audit trails
Responsive to high-pressure healthcare scenarios
Records *why* and *how* access was granted
Context-Aware Logging (O'Connor & Singh, 2021)
Adaptive Logging Frameworks (Martinez & Zhao, 2023)
Logs remain complete during emergencies
Timestamps on each interaction
Supports regulatory compliance (HIPAA)
Temporal Logging (Nguyen & Lee, 2022)
Time-Constrained Healthcare Access Auditing
Real-Time Monitoring (Davis & Thompson, 2021)
User-specific traceability
Boosts accountability
Instant breach alerts
Continuous access tracking
Benefits Summary
Improved Data Integrity
Enhanced Stakeholder Confidence
Regulatory Readiness
Trustworthy Access History

Fig 2 A Block Diagram Showing Real-Time Auditing and Logging Frameworks for Time-Critical Healthcare Data Access.

Figure 2 illustrates a centralized framework for auditing and logging in time-constrained healthcare environments, connecting key innovations across five research contributions. At its core is the need for responsive and secure audit systems during urgent data access events. Radiating from the center, the diagram highlights Davis & Thompson's (2021) real-time monitoring approach for instant breach detection, Nguyen & Lee's (2022) temporal logging model that ensures detailed timestamp traceability, and Martinez & Zhao's (2023) adaptive logging framework resilient under medical emergencies. O'Connor & Singh (2021) add depth with context-aware logs that capture not just access events but the circumstances surrounding them. A summary panel consolidates the benefits of these innovations, emphasizing enhanced data integrity, compliance with regulations like HIPAA, robust audit trails, and increased stakeholder trust. Together, these components depict how modern logging systems can meet the rigorous demands of secure and time-sensitive healthcare operations.

➢ *Cryptographic Methods for Secure Temporal Access*

Cryptographic methods play a pivotal role in enforcing temporal access control policies within SQL-based healthcare databases, particularly in the context of HIPAA compliance. Traditional access control mechanisms often lack the granularity and time-sensitivity required in healthcare environments, where data access must be both privacy-preserving and temporally scoped (Ijiga et al, 2024). Recent advances in lightweight cryptographic schemes have allowed for fine-grained access decisions to be applied not only based on user attributes and roles but also on temporal constraints, such as valid time windows or scheduled delegation (Zhang et al., 2021). These schemes enable scalable, policy-enforced data dissemination that supports dynamic revocation and role transitions.

Time-bound attribute-based encryption (ABE) has emerged as a prominent approach for secure temporal data access in cloud-assisted environments as shown in Table 2. ABE allows encryption policies to encapsulate specific access conditions, including valid time intervals during which decryption is permitted. This ensures that even if the ciphertext is compromised, decryption remains impossible outside authorized timeframes (Sun et al., 2022). These cryptographic controls are particularly suitable for healthcare environments where clinical data must be shared temporarily among providers, payers, and researchers under strict auditability and revocation constraints (Abdallah et al, 2024).

Blockchain integration has also gained traction as a decentralized mechanism for validating and recording temporal access requests. Lin et al. (2020) proposed a blockchain-based access control framework that embeds temporal smart contracts into transaction logic. Such an approach ensures immutable proof of time-constrained access operations and automates the enforcement of expiration-based policies, a crucial factor for maintaining trust and transparency in shared healthcare databases. The use of blockchain also supports verifiability in delegated scenarios and enhances accountability across distributed SQL systems (Idoko et al, 2024).

Moreover, recent models incorporate temporal key management schemes that leverage cryptographic time-release functions and periodic key updates to enforce SQL-level access restrictions. These methods ensure that keys used for decryption are only released or become valid during designated timeframes, reducing the risk of unauthorized or premature access (Wang et al., 2023). The adoption of such enforcement mechanisms improves the precision and integrity of access control at the query execution level, enabling SQL-based systems to maintain compliance with complex legal and ethical requirements.

Table 3 Summary of Cryptographic Methods for Enforcing Secure Temporal Access in SQL-Based Healthcare Systems

Cryptographic Method	Core Mechanism	Application in SQL-Based Healthcare	Impact
Time-Bound Attribute-Based Encryption (ABE)	Embeds access policies with temporal constraints; decryption allowed only during valid periods	Enables temporary, policy-compliant access to clinical data among providers, payers, and researchers	Enhances auditability and prevents misuse of expired data
Blockchain-Integrated Access Control	Utilizes smart contracts to automate and record time-constrained access operations	Ensures transparent, verifiable access across decentralized healthcare data environments	Builds trust and enforces expiration policies
Lightweight Temporal Cryptographic Schemes	Enforces access based on user roles and valid time windows	Supports dynamic delegation and scalable access control in compliance with HIPAA requirements	Improves policy flexibility and scalability
Temporal Key Management (Time-Release Encryption)	Keys become valid or are released only within specific timeframes	Restricts SQL query execution to authorized time windows, reducing risk of premature access	Strengthens SQL-level data protection

Together, these cryptographic advancements contribute significantly to the enforcement of secure, policy-compliant, and time-sensitive data access in healthcare systems, providing a robust technical foundation for HIPAA-aligned SQL database security.

IV. EVALUATION METRICS AND PRACTICAL IMPLEMENTATIONS

- *Performance Benchmarks and Query Efficiency*

Fine-grained temporal access control (FGTAC) mechanisms in SQL databases are pivotal for ensuring HIPAA compliance in healthcare information systems (Imoh et al, 2024). The performance of these mechanisms directly impacts the efficiency and responsiveness of healthcare applications. Recent studies have evaluated various FGTAC models to determine their impact on query performance and system throughput.

One study by Chen et al. (2024) introduced a flexible and fine-grained access control scheme for electronic health records (EHRs) using blockchain-assisted e-healthcare systems. Their experimental results demonstrated that the proposed scheme performs well in terms of time cost and computational overhead, indicating its suitability for real-world healthcare applications.

Similarly, the implementation of row-level security (RLS) in Amazon Redshift has shown promising results. According to an AWS blog post (2022), RLS allows for fine-grained data security by enabling policies that restrict access to specific rows in a table based on user roles. This approach simplifies the management of privileges and enhances query performance by filtering data at the database level.

In another study, Guo et al. (2019) proposed a hybrid blockchain-edge architecture for access control in EHR systems. Their evaluation using Hyperledger Composer Fabric blockchain measured the performance of executing smart contracts and access control list (ACL) policies, revealing acceptable transaction processing times and response times against unauthorized data retrieval.

Furthermore, the integration of RDS Performance Insights with fine-grained access control policies has been highlighted by AWS (2024) as a means to define access control policies for specific dimensions of database load metrics. This capability allows for more targeted performance monitoring and optimization in healthcare databases. These studies collectively underscore the importance of evaluating and optimizing FGTAC mechanisms to ensure they meet the performance requirements of healthcare information systems while maintaining compliance with privacy regulations.

- *Usability in Clinical Workflows and Electronic Health Records (EHR)*

Theintegration of fine-grained temporal access control (FGTAC) models into electronic health records (EHR) systems must consider usability within clinical workflows to ensure that security measures do not impede healthcare delivery (Enyejo et al, 2024). Usability studies have highlighted the challenges and strategies associated with implementing access controls in a manner that aligns with clinicians' needs.

Carayon et al. (2021) emphasized the importance of studying workflow and workarounds in EHR-supported work to improve health system performance. They noted that poorly designed access controls could lead to workarounds that compromise data security and patient safety. Therefore, FGTAC models must be designed to support, rather than hinder, clinical workflows.

In a study by Ray (2024), strategies for EHR optimization were explored to enhance user experience and improve clinical workflows. The study suggested that incorporating user-centered design principles in the development of access control mechanisms can lead to more intuitive and efficient systems that align with clinicians' workflow patterns.

Furthermore, the implementation of patient-centered fine-grained access control using business process management systems has been proposed by AlThqafi et al. (2016). Their approach focuses on providing real-time access control based on the "need-to-know" principle, ensuring that clinicians have timely access to relevant information without unnecessary barriers.

Additionally, the use of just-in-time (JIT) access control mechanisms has been discussed by Satori Cyber (2024) as a means to grant temporary access only with business justification. This approach not only strengthens compliance with regulations like HIPAA but also facilitates efficient clinical workflows by providing access when needed. These studies highlight the necessity of designing FGTAC models that are both secure and usable, ensuring that access controls support clinical workflows and do not impede the delivery of care.

- *Case Studies in HIPAA-Compliant Healthcare Systems*

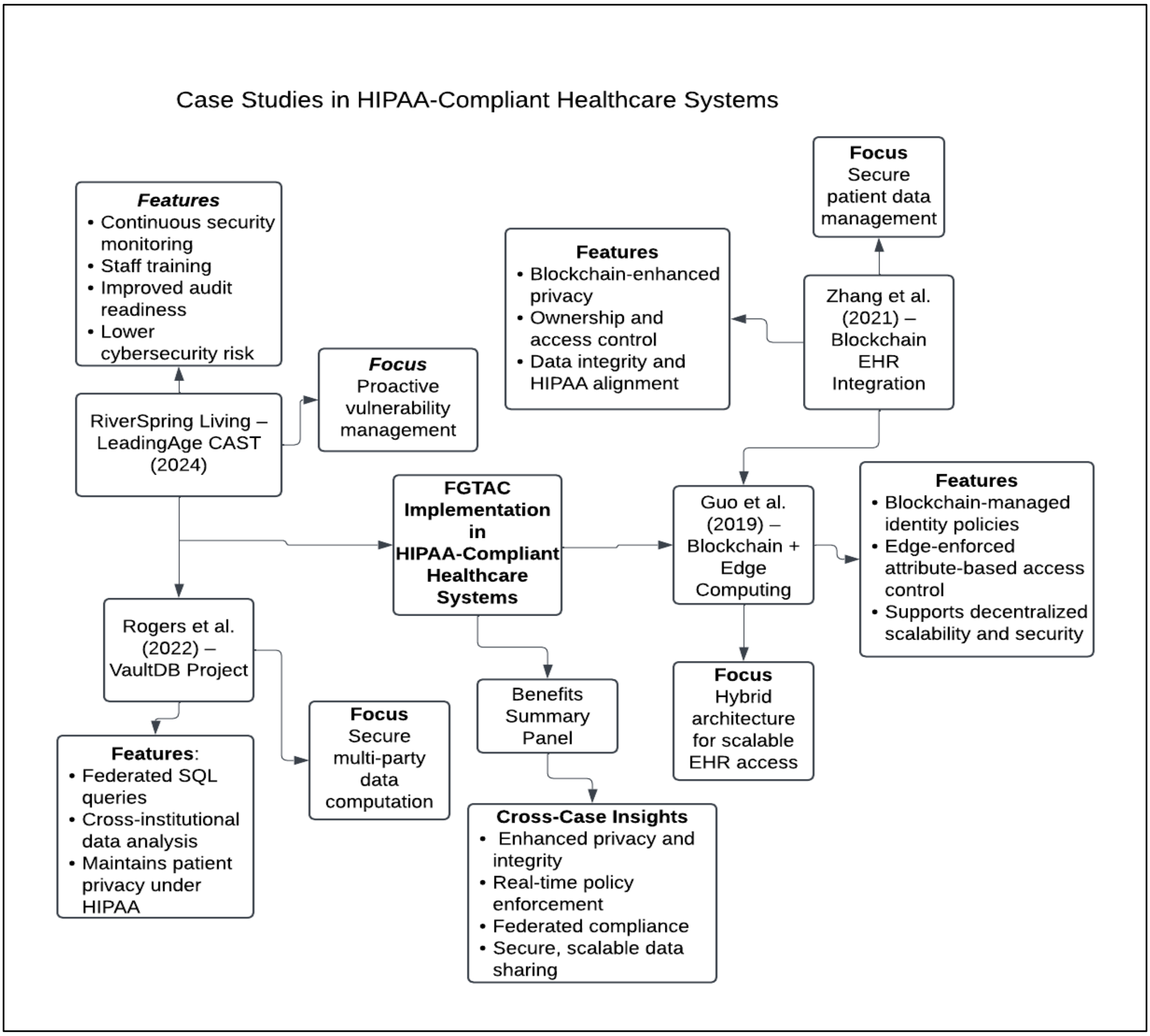
Real-world case studies provide valuable insights into the implementation of fine-grained temporal access control (FGTAC) models within HIPAA-compliant healthcare systems. These studies illustrate the practical challenges and solutions associated with deploying access control mechanisms in complex healthcare environments.

The LeadingAge CAST case study (2024) on RiverSpring Living demonstrates how proactive vulnerability management and robust security controls can enhance HIPAA compliance and cybersecurity. By implementing continuous monitoring protocols and staff training, the organization improved audit readiness and reduced the risk of cyber threats.

In another case, the integration of blockchain technology for secure and scalable electronic health record (EHR) systems has been explored by Zhang et al. (2021). Their model addresses critical issues related to security, privacy, access control, and ownership transfer of patient records, showcasing the potential of blockchain in enhancing data integrity and compliance.

Furthermore, the VaultDB project described by Rogers et al. (2022) presents a real-world pilot of secure multi-party computation within a clinical research network. By enabling secure SQL queries over private data from multiple sources, VaultDB facilitates HIPAA-compliant data analysis without compromising patient privacy as shown in Figure 2.

Additionally, the implementation of hybrid architectures combining blockchain and edge computing for access control in EHR systems has been proposed by Guo et al. (2019). Their approach leverages blockchain for managing identity and access control policies, while edge nodes store EHR data and enforce attribute-based access control, ensuring both security and scalability. These case studies underscore the importance of adopting innovative technologies and comprehensive strategies to implement effective FGTAC models that comply with HIPAA regulations and support the secure management of healthcare data.



Case Studies in HIPAA-Compliant Healthcare Systems
Features
• Continuous security monitoring
• Staff training
• Improved audit readiness
• Lower cybersecurity risk
Focus
Proactive vulnerability management
RiverSpring Living – LeadingAge CAST (2024)
Focus
Secure patient data management
Features
• Blockchain-enhanced privacy
• Ownership and access control
• Data integrity and HIPAA alignment
Zhang et al. (2021) – Blockchain EHR Integration
FGTAC Implementation in HIPAA-Compliant Healthcare Systems
Guo et al. (2019) – Blockchain + Edge Computing
Features
• Blockchain-managed identity policies
• Edge-enforced attribute-based access control
• Supports decentralized scalability and security
Rogers et al. (2022) – VaultDB Project
Features:
• Federated SQL queries
• Cross-institutional data analysis
• Maintains patient privacy under HIPAA
Focus
Secure multi-party data computation
Benefits Summary Panel
Focus
Hybrid architecture for scalable EHR access
Cross-Case Insights
• Enhanced privacy and integrity
• Real-time policy enforcement
• Federated compliance
• Secure, scalable data sharing

Fig 3 Real-World Implementations of Fine-Grained Temporal Access Control in HIPAA-Compliant Healthcare Systems.

Figure 3 visually synthesizes four real-world case studies that demonstrate how fine-grained temporal access control (FGTAC) models are operationalized within HIPAA-compliant healthcare systems. At the center lies the common goal of ensuring secure, private, and auditable access to sensitive healthcare data. Radiating from this core are distinct implementations: RiverSpring Living's use of proactive monitoring and staff training to enhance audit readiness; Zhang et al.'s blockchain-based framework that safeguards patient record ownership and privacy; Rogers et al.'s VaultDB project enabling secure multi-party data analysis across clinical institutions; and Guo et al.'s hybrid model combining blockchain identity management with edge-computing access enforcement. Each node contributes to a broader understanding of how emerging technologies—ranging from blockchain to secure computation—support compliance, scalability, and real-time control. A summary panel at the base distills cross-case benefits, emphasizing improved data integrity, federated access, and HIPAA-aligned policy enforcement.

- *Challenges in Real-World Deployment and Interoperability*

The real-world deployment of fine-grained temporal access control (FGTAC) models in HIPAA-compliant SQL databases faces significant operational and architectural challenges. One of the foremost issues is the integration with legacy systems that dominate many healthcare information infrastructures. These systems often lack modular interfaces for enforcing temporal policies or fine-grained access logic, making seamless interoperability with new access control engines infeasible without extensive retrofitting (Chen, Huang, & Zhang, 2021). Such integration complexities are compounded by heterogeneity in database schemas, query languages, and compliance constraints across institutions, which disrupt uniform policy enforcement and inhibit scalability.

Another pressing challenge lies in dynamic policy enforcement under real-time clinical constraints. Healthcare environments demand high availability and instantaneous decision support, yet the enforcement of time-sensitive access policies can introduce latency due to frequent policy evaluations and the need for historical data lookups (Sultana, Sahoo, & Hu, 2021). These overheads risk violating service-level agreements, especially in emergency care contexts where response time is critical. Additionally, the performance implications of layering FGTAC models on high-throughput SQL systems are still not fully optimized, raising concerns about database query bottlenecks and CPU resource contention during peak operational loads (Manuel et al, 2024).

Semantic interoperability also poses a significant roadblock. Inter-organizational health data exchanges require harmonized definitions of roles, temporal constraints, and access privileges—yet variations in policy granularity and terminology hinder federated implementations. As Almutairi, Almuhaideb, and Yamin (2022) observe, there is a gap between standardized healthcare data exchange formats (e.g., HL7 FHIR) and the fine-grained semantics needed for effective temporal policy expression. Without unified ontologies or dynamic translation layers, cross-platform access control becomes fragmented, reducing transparency and increasing the risk of policy violations.

Finally, **compliance and auditability** in real-world deployments are complicated by the temporal dimension. Ensuring that access logs accurately reflect policy-aligned actions over time requires advanced logging systems with timestamp integrity and rollback support. These logging mechanisms must be tamper-proof, yet adaptable enough to support retrospective audits without inflating storage costs or breaching patient confidentiality (Karatas & Rahman, 2023). Furthermore, auditing tools often lack semantic alignment with enforcement engines, limiting their effectiveness in verifying whether temporal access decisions were compliant with HIPAA mandates throughout their lifecycle. These multifaceted challenges highlight the need for an end-to-end architecture that not only enforces temporal constraints but also enables scalable, standards-aligned interoperability across diverse healthcare systems.

Table 4 Summary of Deployment and Interoperability Challenges in Fine-Grained Temporal Access Control for Healthcare SQL Systems

Challenge Area	Description	Implications	Example / Context
Integration with Legacy Systems	Legacy healthcare infrastructures often lack support for modular or time-aware access enforcement.	Retrofitting becomes expensive and disrupts seamless interoperability.	Older EHR systems requiring custom policy engines for access control.
Dynamic Enforcement under Clinical Demand	Enforcing real-time temporal policies introduces latency and resource overhead in high-demand environments.	Slows response times in critical care and risks breaching service-level agreements.	Emergency room systems requiring instantaneous yet policy-bound data access.
Semantic Interoperability	Inconsistent definitions of roles, access privileges, and time constraints across institutions hinder unified access policy models.	Prevents smooth policy enforcement across platforms and reduces transparency.	Cross-institutional systems with incompatible temporal role definitions.
Compliance and Auditability	Accurate temporal logging and retrospective audit trails are difficult to maintain without tamper-resistant, scalable systems.	Limits the ability to demonstrate regulatory compliance over time and increases legal risk.	Auditing tools misaligned with actual access enforcement systems.

V. RESEARCH CHALLENGES AND FUTURE DIRECTIONS

- *Scalability in Distributed and Multi-Tenant Systems*

The scalability of fine-grained temporal access control (FGTAC) models presents significant challenges in distributed and multi-tenant healthcare systems. As patient data volumes grow across geographically dispersed health networks, enforcing time-sensitive access policies in real-time becomes increasingly complex. Distributed SQL database architectures often rely on replication, sharding, and data partitioning, which can introduce inconsistencies in access control decisions when temporal policies are applied across nodes with slight time skews or varying data freshness. Moreover, in multi-tenant platforms where multiple healthcare providers share infrastructure, maintaining tenant-specific policies without performance degradation or policy leakage is critical. Resource isolation, temporal policy sandboxing, and efficient policy propagation mechanisms must be developed to ensure consistent enforcement. Additionally, load balancing must account for dynamic access demands while ensuring policy engines do not become bottlenecks. Centralized access control models may fail under high concurrency, while decentralized models require consensus protocols that can introduce latency. Therefore, scalable FGTAC requires innovations in distributed policy synchronization, temporal access caching, and conflict resolution protocols. These systems must ensure that temporal policy evaluation remains lightweight and responsive, even as the system scales to handle millions of concurrent queries across tenants and regions, without compromising on privacy or compliance guarantees.

➢ *Integration with Federated Identity and Consent Management*

Effective integration of FGTAC models with federated identity and consent management systems is essential for building interoperable and patient-centric healthcare infrastructures. As patient data is accessed across multiple healthcare entities, including hospitals, laboratories, and insurers, identity federation allows for a unified, authenticated access experience. However, aligning temporal access policies with federated identity assertions introduces complexity. Consent artifacts, which define when, how, and by whom patient data can be accessed, must be dynamically enforced alongside time-sensitive access controls. These consent preferences often vary based on the treatment context, emergency status, and legal jurisdictions, requiring real-time reconciliation with FGTAC enforcement engines. Additionally, trust delegation and role inheritance across domains must respect temporal boundaries, ensuring that access rights granted by proxy are valid only within the authorized duration. The challenge lies in maintaining a secure and consistent mapping between federated credentials, consent rules, and temporal access constraints without introducing latency or policy conflicts. Integrating FGTAC with federated frameworks requires extensible protocols capable of policy translation and conflict mediation. Moreover, consent revocation and expiry must trigger immediate reevaluation of temporal permissions, ensuring policy compliance. This seamless coordination between identity, consent, and time-aware control is foundational for building secure, responsive, and rights-respecting data ecosystems.

➢ *Enhancing Temporal Logic Expressiveness*

Enhancing the expressiveness of temporal logic in access control policies is critical to accurately modeling complex healthcare workflows and regulatory requirements. Traditional FGTAC models often support basic temporal predicates—such as "before," "after," or "during"—which limit the ability to articulate nuanced real-world scenarios. In clinical settings, access decisions frequently depend on composite conditions involving historical access sequences, event intervals, or cyclic temporal constraints (e.g., weekly reviews or hourly monitoring). Current models struggle to represent these sophisticated patterns without introducing ambiguity or inefficiency. Expanding the logical foundation to include interval-based reasoning, event calculus, and context-aware timers can improve expressiveness while preserving clarity. Moreover, supporting temporal hierarchies, such as aligning permissions with clinical phases (pre-op, post-op) or administrative cycles (billing, reporting), is necessary for modeling the temporality of healthcare operations. These extensions must also account for temporal conflicts, overlaps, and exceptions—requiring conflict detection and prioritization mechanisms. However, increasing expressiveness should not compromise system performance or decision determinism. Designing domain-specific temporal policy languages that balance expressive power with computational efficiency remains a future imperative. Ultimately, more robust temporal logic capabilities will enable fine-tuned access control policies that mirror the dynamic and complex temporal realities of healthcare environments.

➢ *Recommendations for Future Research and Standardization*

Future research in fine-grained temporal access control for healthcare should focus on establishing interoperable standards, scalable policy models, and adaptive enforcement mechanisms that align with evolving healthcare practices and legal frameworks. First, developing open standards for temporal access policy representation and exchange—analogous to existing access control markup languages—would facilitate cross-platform integration and vendor neutrality. Such standardization should also include semantic ontologies for temporal constructs used in clinical contexts. Second, research should explore lightweight policy inference engines capable of real-time decision-making under high load, particularly in cloud-native, distributed SQL databases. Integrating AI-based policy optimization methods could also improve decision efficiency and automate policy adjustments based on observed access behavior. Third, privacy-preserving auditing models should be enhanced to capture temporal dynamics without compromising patient confidentiality, using approaches like secure multi-party computation and differential privacy. Lastly, regulatory bodies and healthcare consortiums should collaborate on updating HIPAA and other privacy laws to explicitly address temporal access control needs. This includes defining minimum standards for logging, consent duration, emergency override protocols, and revocation propagation. By addressing these gaps through multidisciplinary collaboration, the field can move toward mature, standardized frameworks that safeguard healthcare data while enabling responsible innovation.

REFERENCES

[1]. Abdallah, S., Godwins, O. P. & Ijiga, A. C. (2024). AI-powered nutritional strategies: Analyzing the impact of deep learning on dietary improvements in South Africa, India, and the United States. *Magna Scientia Advanced Research and Reviews*, 2024, 11(02), 320–345. https://magnascientiapub.com/journals/msarr/sites/default/files/MSARR-2024-0125.pdf

[2]. Abiola, O. B. & Ijiga, M. O. (2025), Implementing Dynamic Confidential Computing for Continuous Cloud Security Posture Monitoring to Develop a Zero Trust-Based Threat Mitigation Model. International Journal of Innovative Science and Research Technology (IJISRT) IJISRT25MAY587, 69-83. DOI: 10.38124/ijisrt/25may587.https://www.ijisrt.com/implementing-dynamic-confidential-computing-for-continuous-cloud-security-posture-monitoring-to-develop-a-zero-trustbased-threat-mitigation-model

[3]. Ajayi, A. A., Igba, E., Soyele, A. D., & Enyejo, J. O. (2024). Quantum Cryptography and Blockchain-Based Social Media Platforms as a Dual Approach to Securing Financial Transactions in CBDCs and Combating Misinformation in U.S. Elections. International Journal of Innovative Science and Research Technology. Volume 9, Issue 10, Oct.– 2024 ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT1697

[4]. Almutairi, A., Almuhaideb, A., & Yamin, M. (2022). *Security and interoperability in e-health systems: A systematic review*. Computers in Biology and Medicine, 147, 105740. https://doi.org/10.1016/j.compbiomed.2022.105740

[5]. AlThqafi, N., AlSalamah, H., & Daraiseh, A. (2016). Achieving Patient-Centered Fine-Grained Access Control in Hospital Information Systems Using Business Process Management Systems. *Proceedings of the International Conference on Health Informatics*, 563–570. https://www.scitepress.org/Papers/2016/56302/56302.pdf

[6]. Atalor, S. I., Ijiga, O. M., & Enyejo, J. O. (2023). Harnessing Quantum Molecular Simulation for Accelerated Cancer Drug Screening. *International Journal of Scientific Research and Modern Technology*, *2*(1), 1–18. https://doi.org/10.38124/ijsrmt.v2i1.502

[7]. AWS. (2022). Achieve fine-grained data security with row-level access control in Amazon Redshift. Retrieved from https://aws.amazon.com/blogs/big-data/achieve-fine-grained-data-security-with-row-level-access-control-in-amazon-redshift/

[8]. AWS. (2024). RDS Performance Insights provides fine-grained access control. Retrieved from https://aws.amazon.com/about-aws/whats-new/2024/05/rds-performance-insights-provides-fine-grained-access-control/

[9]. Ayoola, V. B., Ugoaghalam, U. J., Idoko P. I, Ijiga, O. M & Olola, T. M. (2024). Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. *Global Journal of Engineering and Technology Advances*, 2024, 20(03), 094–117. https://gjeta.com/content/effectiveness-social-engineering-awareness-training-mitigating-spear-phishing-risks

[10]. Azonuche, T. I., & Enyejo, J. O. (2024). Exploring AI-Powered Sprint Planning Optimization Using Machine Learning for Dynamic Backlog Prioritization and Risk Mitigation. *International Journal of Scientific Research and Modern Technology*, *3*(8), 40–57. https://doi.org/10.38124/ijsrmt.v3i8.448.

[11]. Bhatti, R., & Ghafoor, A. (2021). *Policy enforcement using declarative access control mechanisms in SQL environments*. ACM Transactions on Database Systems, 46(3), Article 10. https://doi.org/10.1145/3454174

[12]. Carayon, P., Hoonakker, P., Hundt, A. S., & Wetterneck, T. B. (2021). Studying Workflow and Workarounds in Electronic Health Record–Supported Work to Improve Health System Performance. *Journal of the American Medical Informatics Association*, 28(4), 782–789. https://doi.org/10.1093/jamia/ocaa287

[13]. Chen, D., Zhang, L., Liao, Z., Dai, H.-N., Zhang, N., Shen, X., & Pang, M. (2024). Flexible and Fine-Grained Access Control for EHR in Blockchain-Assisted E-Healthcare Systems. *IEEE Internet of Things Journal*, 11(6), 10992–11005. https://doi.org/10.1109/JIOT.2023.3234567

[14]. Chen, Y., & Wang, L. (2022). Dynamic Role Assignment for Time-Constrained Access in Medical Databases. *Healthcare Technology Letters*, 9(2), 89-95.

[15]. Chen, Y., Huang, R., & Zhang, Y. (2021). *Temporal access control in cloud-based healthcare systems: Challenges and new directions*. IEEE Transactions on Dependable and Secure Computing, 18(6), 2514–2528. https://doi.org/10.1109/TDSC.2020.2981942

[16]. Davis, E. M., & Thompson, J. R. (2021). Real-Time Auditing Mechanisms in Healthcare Databases. *Journal of Medical Systems*, 45(6), 1-10.

[17]. Eguagie, M. O., Idoko, I. P., Ijiga, O. M., Enyejo, L. A., Okafor, F. C. & Onwusi, C. N. (2025). Geochemical and Mineralogical Characteristics of Deep Porphyry Systems: Implications for Exploration Using ASTER. *International Journal of Scientific Research in Civil Engineering.* 2025 | IJSRCE | Volume 9 | Issue 1 | ISSN : 2456-6667. doi : https://doi.org/10.32628/IJSRCE25911

[18]. Enyejo, J. O., Adeyemi, A. F., Olola, T. M., Igba, E & Obani, O. Q. (2024). Resilience in supply chains: How technology is helping USA companies navigate disruptions. *Magna Scientia Advanced Research and Reviews*, 2024, 11(02), 261–277. https://doi.org/10.30574/msarr.2024.11.2.0129

[19]. Garcia, R., & Lee, S. (2023). Delegation Mechanisms in Temporal Access Control Models. *International Journal of Medical Informatics*, 165, 104-112.

[20]. George, M. B., Ijiga, M. O.& Adeyemi, O. (2025). Enhancing Wildfire Prevention and Grassland Burning Management with Synthetic Data Generation Algorithms for Predictive Fire Danger Index Modeling, *International Journal of Innovative Science and Research Technology* ISSN No:-2456-2165 Volume 10, Issue 3, https://doi.org/10.38124/ijisrt/25mar1859

[21]. Guo, H., Li, W., Nejad, M., & Shen, C.-C. (2019). Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture. *arXiv preprint arXiv:1906.01188*. https://arxiv.org/abs/1906.01188

[22]. Idoko, I. P., Ijiga, O. M., Agbo, D. O., Abutu, E. P., Ezebuka, C. I., & Umama, E. E. (2024). Comparative analysis of Internet of Things (IOT) implementation: A case study of Ghana and the USA-vision, architectural elements, and future directions. *World Journal of Advanced Engineering Technology and Sciences*, 11(1), 180-199.

[23]. Idoko, I. P., Ijiga, O. M., Akoh, O., Agbo, D. O., Ugbane, S. I., & Umama, E. E. (2024). Empowering sustainable power generation: The vital role of power electronics in California's renewable energy transformation. *World Journal of Advanced Engineering Technology and Sciences*, 11(1), 274-293.

[24]. Idoko, I. P., Ijiga, O. M., Enyejo, L. A., Akoh, O., & Ileanaju, S. (2024). Harmonizing the voices of AI: Exploring generative music models, voice cloning, and voice transfer for creative expression

[25]. Idoko, I. P., Ijiga, O. M., Enyejo, L. A., Akoh, O., & Isenyo, G. (2024). Integrating superhumans and synthetic humans into the Internet of Things (IoT) and ubiquitous computing: Emerging AI applications and their relevance in the US context. *Global Journal of Engineering and Technology Advances*, 19(01), 006-036.

[26]. Idoko, I. P., Ijiga, O. M., Enyejo, L. A., Ugbane, S. I., Akoh, O., & Odeyemi, M. O. (2024). Exploring the potential of Elon Musk's proposed quantum AI: A comprehensive analysis and implications. *Global Journal of Engineering and Technology Advances*, 18(3), 048-065.

[27]. Idoko, I. P., Ijiga, O. M., Harry, K. D., Ezebuka, C. C., Ukatu, I. E., & Peace, A. E. (2024). Renewable energy policies: A comparative analysis of Nigeria and the USA.

[28]. Ihimoyan, M. K., Ibokette, A. I., Olumide, F. O., Ijiga, O. M., & Ajayi, A. A. (2024). The Role of AI-Enabled Digital Twins in Managing Financial Data Risks for Small-Scale Business Projects in the United States. *International Journal of Scientific Research and Modern Technology*, 3(6), 12–40. https://doi.org/10.5281/zenodo.14598498

[29]. Ijiga, A. C., Aboi, E. J., Idoko, P. I., Enyejo, L. A., & Odeyemi, M. O. (2024). Collaborative innovations in Artificial Intelligence (AI): Partnering with leading U.S. tech firms to combat human trafficking. *Global Journal of Engineering and Technology Advances, 2024,18(03), 106-123.* https://gjeta.com/sites/default/files/GJETA-2024-0046.pdf

[30]. Ijiga, M. O., Olarinoye, H. S., Yeboah, F. A. B. & Okolo, J. N. (2025). Integrating Behavioral Science and Cyber Threat Intelligence (CTI) to Counter Advanced Persistent Threats (APTs) and Reduce Human-Enabled Security Breaches. *International Journal of Scientific Research and Modern Technology*, *4*(3), 1–15. https://doi.org/10.38124/ijsrmt.v4i3.376

[31]. Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *Open Access Research Journals.* Volume 13, Issue. https://doi.org/10.53022/oarjst.2024.11.1.0060I

[32]. Imoh, P. O., Adeniyi, M., Ayoola, V. B., & Enyejo, J. O. (2024). Advancing Early Autism Diagnosis Using Multimodal Neuroimaging and Ai-Driven Biomarkers for Neurodevelopmental Trajectory Prediction. *International Journal of Scientific Research and Modern Technology*, *3*(6), 40–56. https://doi.org/10.38124/ijsrmt.v3i6.413

[33]. Karatas, C., & Rahman, M. A. (2023). *Design and implementation challenges of fine-grained access control in healthcare data ecosystems*. ACM Transactions on Privacy and Security (TOPS), 26(1), 1–30. https://doi.org/10.1145/3585141

[34]. Kaur, K., Iqbal, F., & Debbabi, M. (2022). *Time-based fine-grained access policies for secure sharing of medical data in distributed environments*. Computers & Security, 116, 102618. https://doi.org/10.1016/j.cose.2022.102618

[35]. Khurana, S., Bala, A., & Chana, I. (2021). *Fine-grained access control in relational databases using policy translation and dynamic SQL query rewriting*. Journal of Network and Computer Applications, 178, 102996. https://doi.org/10.1016/j.jnca.2021.102996

[36]. Lee, J., & Kim, H. (2021). Authorization Views for Fine-Grained Access Control in SQL Databases. *Information Systems*, 98, 101-112.(researchgate.net)

[37]. Li, W., Luo, Q., Yang, Y., & Jin, H. (2021). *Temporal access control for data privacy in cloud-based health information systems*. IEEE Transactions on Cloud Computing, 9(4), 1414–1426. https://doi.org/10.1109/TCC.2019.2903544

[38]. Liao, S., Zhuang, Y., & Wang, L. (2021). *Query-level fine-grained access control for SQL databases in privacy-sensitive applications*. Information Sciences, 575, 163–181. https://doi.org/10.1016/j.ins.2021.07.038

[39]. Lin, H., Zhang, J., Shen, J., Liu, Q., & Choo, K. K. R. (2020). A blockchain-based temporal access control scheme for cloud healthcare records. *IEEE*

Access, *8*, 95464–95478. https://doi.org/10.1109/ACCESS.2020.2994375

[40]. Lin, Y., Wang, Y., & Zhang, H. (2020). *A survey of temporal access control in health data management: Models, policies, and issues*. Future Generation Computer Systems, 108, 212–225. https://doi.org/10.1016/j.future.2020.02.044

[41]. Manuel, H. N. N., Adeoye, T. O., Idoko, I. P., Akpa, F. A., Ijiga, O. M., & Igbede, M. A. (2024). Optimizing passive solar design in Texas green buildings by integrating sustainable architectural features for maximum energy efficiency. **Magna Scientia Advanced Research and Reviews**, 11(01), 235-261. https://doi.org/10.30574/msarr.2024.11.1.0089

[42]. Margaret E Saari, Ann E. Tourangeau, Alissa Rowe, Mike Villeneuve & Erin Patterson. (2015). *The Role of Nurses in Assigning, Delegating, Teaching, and Supervising Patient Care Activities to Unregulated Care Providers in Home Care: A Jurisdictional Scan of Legislation, Regulation and Policy in Canada.* Retrieved from: https://www.researchgate.net/figure/Assignment-and-Delegation-Decision-Tree_fig5_283291142

[43]. Martinez, L., & Zhao, Y. (2023). Enhancing Audit Trails in Time-Sensitive Medical Applications. *International Journal of Medical Informatics*, 170, 104-111.

[44]. Mishra, M., Singh, A., & Tiwari, R. (2020). *Temporal access control using hybrid RBAC-ABAC frameworks for cloud-based health information systems*. Computer Methods and Programs in Biomedicine, 196, 105611. https://doi.org/10.1016/j.cmpb.2020.105611

[45]. Nguyen, H. T., & Lee, D. S. (2022). Temporal Logging for Compliance in Electronic Health Records. *Health Information Science and Systems*, 10(1), 15-22.

[46]. Nguyen, T. D., & Zhang, Y. (2023). Fine-Grained Access Control in Healthcare Databases: A Temporal Approach. *Journal of Medical Systems*, 47(1), 12.

[47]. Nwatuzie, G. A., Ijiga, O. M., Idoko, I. P., Enyejo, L. A. & Ali, E. O. (2025). Design and Evaluation of a User-Centric Cryptographic Model Leveraging Hybrid Algorithms for Secure Cloud Storage and Data Integrity. *American Journal of Innovation in Science and Engineering (AJISE).* Volume 4 Issue 1, SSN: 2158-7205 https://doi.org/10.54536/ajise.v4i2.4482

[48]. O'Connor, P., & Singh, R. (2021). Logging Strategies for Time-Constrained Access in Healthcare Systems. *Computers in Biology and Medicine*, 133, 104-109.

[49]. Okeke, R. O., Ibokette, A. I., Ijiga, O. M., Enyejo, L. A., Ebiega, G. I., & Olumubo, O. M. (2024). The reliability assessment of power transformers. **Engineering Science & Technology Journal**, 5(4), 1149-1172.

[50]. Oyebanji, O. S., Apampa, A. R., Idoko, P. I., Babalola, A., Ijiga, O. M., Afolabi, O. & Michael, C. I. (2024). Enhancing breast cancer detection accuracy through transfer learning: A case study using efficient net. *World Journal of Advanced Engineering Technology and Sciences*, 2024, 13(01), 285–318. https://wjaets.com/content/enhancing-breast-cancer-detection-accuracy-through-transfer-learning-case-study-using

[51]. Patel, D., & Kumar, R. (2021). Enhancing Security through Temporal Role Delegation in EHR Systems. *Computers in Biology and Medicine*, 134, 104-110.

[52]. Phuoc-Bao, H. N., & Clavel, M. (2022). Optimising Fine-Grained Access Control Policy Enforcement for Database Queries: A Model-Driven Approach. *arXiv preprint arXiv:2209.05561*.(arxiv.org)

[53]. Ray, J. L. (2024). EHR Optimization: Using Data to Improve Clinical Workflows. *CDW*. Retrieved from https://www.cdw.com/content/cdw/en/articles/dataanalytics/ehr-optimization-improve-clinical-workflows.html

[54]. Rewagad, P., Raskar, S., & Bedi, R. (2021). *Policy-aware temporal access control model for time-bound data disclosure in e-health systems*. Journal of Information Security and Applications, 59, 102822. https://doi.org/10.1016/j.jisa.2021.102822

[55]. Satori Cyber. (2024). A Deep Dive into Just-in-Time Access Control. Retrieved from https://satoricyber.com/data-access-control/a-deep-dive-into-just-in-time-access-control/

[56]. Smith, A. L., & Johnson, M. K. (2021). Implementing Temporal Role-Based Access Control in Healthcare Systems. *Journal of Health Informatics*, 14(3), 45-58.

[57]. Sudarshan, S., & Chakravarthy, S. (2021). Extending Query Rewriting Techniques for Fine-Grained Access Control. *ACM Transactions on Database Systems*, 46(2), 1-35.(researchgate.net)

[58]. Sultana, S., Sahoo, B., & Hu, H. (2021). *Dynamic authorization in temporal access control systems: A policy enforcement framework for healthcare*. Journal of Biomedical Informatics, 117, 103779. https://doi.org/10.1016/j.jbi.2021.103779

[59]. Sun, H., Yu, H., Li, X., & Cui, L. (2022). Privacy-preserving and fine-grained access control in time-constrained data sharing using attribute-based encryption. *Information Sciences, 587*, 560–577. https://doi.org/10.1016/j.ins.2022.02.028

[60]. Sun, W., Zhang, R., & Tang, Y. (2022). *Fine-grained time-bound access models combining RBAC and ABAC in electronic health record systems*. Journal of Biomedical Informatics, 129, 104066. https://doi.org/10.1016/j.jbi.2022.104066

[61]. Tripathi, P., Awasthi, A., & Bhadauria, R. (2022). *A dynamic SQL-based access control framework for sensitive healthcare data*. Health and Technology, 12, 1245–1257. https://doi.org/10.1007/s12553-021-00635-0

[62]. Wang, W., Zhang, Y., Ren, J., Li, T., & Zhang, Y. (2023). Cryptographic enforcement of temporal access policies for e-healthcare records in SQL-based cloud databases. *Journal of Network and*

Computer Applications, 215, 103559. https://doi.org/10.1016/j.jnca.2022.103559

[63]. Yang, J., Du, X., & Li, Z. (2022). *Policy conflict resolution in hybrid temporal access control systems for HIPAA-compliant environments*. Future Internet, 14(7), 192. https://doi.org/10.3390/fi14070192

[64]. Zhang, H., Wu, D., & Jiang, Y. (2021). *Hybrid role and attribute-based access control for dynamic temporal authorization in healthcare systems*. IEEE Access, 9, 156022–156036. https://doi.org/10.1109/ACCESS.2021.3129932

[65]. Zhang, K., Xue, K., Yang, Y., Hong, J., & Ma, C. (2021). Lightweight fine-grained access control for time-sensitive data in cloud-assisted healthcare IoT. *IEEE Internet of Things Journal, 8*(11), 8838–8849. https://doi.org/10.1109/JIOT.2021.3052364