Attribute-Based Encryption with Secure Multi-Party Computation for Fine-Grained Access Control in Cloud-Based Healthcare Systems.

Asheshemi Nelson Oghenekevwe[1], Michael Adawaren[2]

[1]Department of Computer Science, Federal University of Petroleum Resources Efurun, Delta State-Nigeria.

[1]Department of Computer Science, Federal Polytechnic Orogun, Delta State.

[2]Department of Computer Science, Delta State University Abraka, Delta State-Nigeria

DOI: https://doi.org/10.51244/IJRSI.2025.1213CS0022

Received: 25 December 2025; Accepted: 31 December 2025; Published: 15 January 2026

ABSTRACT

Cloud-based healthcare systems have transformed the management and sharing of electronic health records (EHRs), telemedicine data, and collaborative medical research by offering scalability, cost efficiency, and real time accessibility. However, this transformation exposes patient data to risks such as breaches, insider threats, and unauthorized disclosures. Traditional access control mechanisms like Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Identity-Based Encryption (IBE) prove insufficient in dynamic, multi-stakeholder healthcare environments. This research proposes a hybrid framework integrating Attribute Based Encryption (ABE) for fine-grained, policy-driven confidentiality and Secure Multi-Party Computation (SMC) for privacy-preserving collaborative analytics. The framework ensures that sensitive health data remains protected while enabling secure computations across distributed institutions. ABE enforces patient- and context centric access policies, while SMC enables multi-institutional analytics without exposing raw records. The proposed system is evaluated through security analysis and performance benchmarks, highlighting trade-offs between encryption costs, ciphertext expansion, computation overheads, and communication latency. The results demonstrate that ABE + SMC integration can achieve confidentiality, collusion resistance, and regulatory compliance (HIPAA/GDPR), while supporting practical applications such as multi-hospital predictive analytics, genomics, and clinical trials. Despite challenges in key management, revocation, and computational scalability, this hybrid model represents a paradigm shift toward secure, collaborative, and patient-centric healthcare ecosystems.

Keywords: Attribute-Based Encryption; Secure Multi-Party Computation; Cloud Healthcare Security; Fine Grained Access Control; Privacy-Preserving Analytics; Electronic Health Records.

INTRODUCTION

Cloud computing has revolutionized modern healthcare by enabling efficient storage, retrieval, and sharing of Electronic Health Records (EHRs), telemedicine services, and remote diagnostic platforms. Healthcare organizations increasingly leverage cloud infrastructures to reduce costs, enhance scalability, and ensure seamless collaboration across institutions (Kaushik & Gandhi, 2022; Saini et al., 2021). The rapid adoption of cloud-based solutions allows physicians, hospitals, insurance providers, and researchers to access sensitive patient data in real-time, facilitating clinical decision-making, personalized treatment, and predictive analytics (Vaishali et al., 2021; Raman et al., 2024). Despite these benefits, cloud-based healthcare systems face significant challenges in data security and privacy, particularly when handling life-critical information such as laboratory results, diagnostic images, and genomic datasets (Samonte et al., 2024; Ganesan et al., 2024). One of the primary concerns in healthcare cloud systems is data breaches, which often result in unauthorized disclosure of patient records. Studies reveal that healthcare remains among the most targeted industries for cyberattacks, with breaches leading to identity theft, insurance fraud, and loss of patient trust (Thamrin & Xu, 2021; Edemacu et al., 2020). Insider threats are equally alarming, as employees with privileged access can deliberately or accidentally leak confidential data (Azbeg et al., 2023; Rani et al., 2022). Furthermore, the outsourcing of sensitive health data to third-party cloud providers amplifies risks of unauthorized access, surveillance, and data misuse (Deebak & Hwang, 2024; Mupila et al., 2025).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

Traditional access control mechanisms such as Role-Based Access Control (RBAC) and Identity-Based Encryption (IBE) are insufficient in addressing these threats. RBAC often fails in large-scale healthcare systems where roles are dynamic, while IBE suffers from rigid key management limitations (Choksy et al., 2023; Wang et al., 2021). These shortcomings necessitate fine-grained access control approaches that can enforce context specific policies, such as granting a cardiologist access to cardiac-related EHR entries but restricting access to psychiatric records. Attribute-Based Encryption (ABE) has emerged as a promising paradigm, allowing encryption policies to be tied directly to user attributes (He et al., 2023; Yang & Zhang, 2022). Unlike RBAC, ABE supports flexible, patient-centric access models where data owners define who can decrypt medical records based on attributes such as specialty, institution, or purpose of use (Sun et al., 2023). Cloud-based healthcare systems have become the backbone of modern medical data management, enabling flexible and efficient sharing of electronic health records, telemedicine services, and collaborative research. However, these systems face a critical challenge: ensuring secure, privacy-preserving, and fine-grained access to sensitive medical information across distributed stakeholders. Existing access control models such as RBAC and IBE are inadequate, as they lack adaptability to dynamic healthcare environments and are vulnerable to insider misuse, collusion, and unauthorized disclosures (Choksy et al., 2023; Edemacu et al., 2020). Attribute-Based Encryption (ABE) provides fine-grained control by embedding access policies into cryptographic keys or ciphertexts, but it struggles with scalability, efficient key revocation, and enabling secure computations on encrypted data (He et al., 2023; Das & Namasudra, 2022).

At the same time, Secure Multi-Party Computation (SMC) allows multiple healthcare providers or researchers to jointly compute functions over private datasets without revealing raw inputs, enabling privacy-preserving analytics (Egala et al., 2021; Shahzad et al., 2024). However, SMC alone incurs heavy computational and communication overheads, limiting its applicability in large-scale, real-time healthcare settings. The absence of a unified framework that combines ABE's policy-driven access control with SMC's collaborative computation hinders the realization of secure, efficient, and compliant cloud-based healthcare ecosystems. However, while ABE ensures fine-grained data confidentiality, it does not natively support collaborative computation on encrypted health data. This limitation is critical in scenarios such as multi-hospital epidemiological studies, remote patient monitoring, and AI-driven diagnostics, where multiple parties must perform computations without revealing raw patient information (Ovie & Akinloye, 2025; Gyawali & Karyakarte, 2023). Here, Secure Multi-Party Computation (SMC) plays a pivotal role. SMC enables multiple entities to jointly compute functions over private inputs without disclosing them to each other (Egala et al., 2021; Joy et al., 2025). In healthcare, SMC has been applied to privacy-preserving genome analysis, collaborative disease prediction, and secure clinical trial management (Shahzad et al., 2024; Dornala et al., 2023).

Integrating ABE with SMC offers a complementary solution: ABE enforces fine-grained access to encrypted health data, while SMC ensures that computations can be securely performed on this encrypted data without violating privacy (Samonte et al., 2024; Sruthi & Martha, 2025). Such a hybrid framework aligns with global regulatory requirements like HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation), which mandate strict safeguards for patient data confidentiality, accountability, and auditability (Sharma, 2024; Waghodekar, 2024). While cloud computing provides unparalleled opportunities for real-time healthcare collaboration, remote monitoring, and big data analytics, it simultaneously exposes healthcare systems to critical risks of privacy violation, insider misuse, and cross-institutional vulnerabilities. To address these challenges, the adoption of a hybrid security architecture based on Attribute-Based Encryption (ABE) and Secure Multi-Party Computation (SMC) is essential for ensuring robust fine-grained access control, secure collaborative computation, and compliance with global healthcare security standards (Madavarapu et al., 2023; Pandiaraj et al., 2023; Zarkesh et al., 2024).

Related Works

Access control for cloud-based healthcare: models, limits, and cryptographic turn

Cloud architectures have enabled electronic health records (EHRs), telemedicine, and remote diagnostics to scale across organizations, but the same elasticity and multi-tenancy complicate policy enforcement, insider risk mitigation, and cross-domain compliance. Classical authorization has historically centered on Role-Based Access Control (RBAC) privileges bundled as roles and assigned to users augmented in some settings by Attribute-Based Access Control (ABAC) policies over user, resource, and environmental attributes evaluated

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

by a policy decision point and by cryptographic distribution such as Identity-Based Encryption (IBE) public keys derived from identities such as email addresses. In healthcare, these models each encounter limitations: RBAC struggles with role explosion and emergency "break-glass" contexts; ABAC depends on always-online, trusted enforcement points and struggles once data leaves a perimeter; and IBE lacks native fine-grained, composable policy semantics and suffers from key escrow and revocation challenges. These shortcomings motivate a cryptographically enforced, data-centric approach, notably Attribute-Based Encryption (ABE), which binds access policies to ciphertexts or to decryption keys themselves, and can be combined with Secure Multi-Party Computation (SMC) to compute over private inputs without disclosure both particularly relevant to multiinstitution analytics and privacy-preserving clinical decision support (Kaushik & Gandhi, 2022; Samonte et al., 2024; Ganesan et al., 2024).

Traditional access control approaches can be grouped into Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Identity-Based Encryption (IBE). RBAC ties privileges to roles assigned to users, ABAC enforces policies based on attributes of users, resources, and contexts, while IBE derives public keys from user identities such as email addresses. However, in the healthcare context, each approach faces critical shortcomings.

i. RBAC suffers from role explosion in large federated care systems, where complex hierarchies of roles lead to administrative overhead and authorization errors (Choksy et al., 2023).

ii. ABAC, although flexible and context-aware, relies on server-side enforcement. Once data leaves the trusted perimeter of the provider (e.g., uploaded to cloud storage or shared with researchers), ABAC fails to prevent offline misuse or unauthorized replication (Thamrin & Xu, 2021).

iii. IBE, while simplifying key management, lacks the fine-grained, composable policies needed in clinical workflows and suffers from key escrow and revocation complexity, making it ill-suited for dynamic healthcare environments (Shahzad et al., 2024).

Role-Based Access Control (RBAC) in healthcare clouds

RBAC has been widely implemented in hospital information systems due to its simplicity and structured authorization model. In single-domain environments, mapping permissions to roles such as "doctor," "nurse," or "billing clerk" is efficient (Reddy Vanga, 2025). However, federated healthcare ecosystems introduce complexity. When multiple hospitals, specialties, and clinical contexts are considered, the role-explosion problem arises, producing an unmanageable number of roles. Additionally, RBAC is coarse-grained, granting access to all data associated with a role even when clinical necessity is narrower (Kaushik & Gandhi, 2022). For example, a cardiologist may require access only to cardiovascular test results, not psychiatric evaluations.

RBAC also struggles with break-glass scenarios, where emergency overrides are needed. Attempts to model emergency access with RBAC often result in either over-authorization (introducing privacy risks) or under authorization (hindering urgent care) (Saini et al., 2021). These shortcomings underscore the need for cryptographic models such as ABE, where access can be bound to attributes like specialty, institution, and treatment purpose (Samonte et al., 2024).

Attribute-Based Access Control (ABAC): power and pitfalls

ABAC allows context-sensitive, fine-grained access decisions based on attributes of users, data, and environment. This model supports delegation, making it suitable for Internet of Medical Things (IoMT) settings where devices generate sensitive patient telemetry. For instance, an attending physician may temporarily delegate limited access rights to a resident physician (Choksy et al., 2023).

Despite its flexibility, ABAC has significant pitfalls. Server-side enforcement assumes a trusted environment, which is not realistic in cloud or cross-institutional sharing scenarios (Thamrin & Xu, 2021). Once data is exported to research environments or external providers, ABAC cannot prevent offline decryption or unauthorized replication. Recent studies have therefore proposed ABAC–cryptographic hybrids, where ABAC is combined with cryptographic primitives such as ABE, ensuring access policies persist with the data itself (Ganesan et al., 2024; Azbeg et al., 2023).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

Identity-Based Encryption (IBE) for e-health: why it falls short

IBE allows public keys to be derived from user identities, simplifying key distribution. This has seen adoption in secure email and messaging within healthcare organizations. However, in cloud-based healthcare, IBE falls short due to its lack of expressive policy support. Encryptors must either enumerate specific recipients or assign broad group identities, which does not align with the need for multi-attribute, fine-grained access policies in clinical environments (Prasanna, 2025).

Furthermore, IBE suffers from key escrow, since private keys are generated by a trusted authority that could decrypt any message. Key revocation is also cumbersome, often requiring either time-bound identities or mass key updates (Shahzad et al., 2024). These limitations make IBE unsuitable for dynamic, multi-stakeholder healthcare systems, where flexible policies and efficient revocation are essential.

Why cryptographic, data-centric control is needed

The limitations of RBAC, ABAC, and IBE highlight the need for data-centric security. Healthcare systems increasingly rely on cross-organization data sharing for epidemiology, pharmaco-surveillance, and real-world evidence generation (Madavarapu et al., 2023). Remote diagnostics and tele-ICU systems similarly require secure analytics across institutional boundaries.

Data-centric cryptography such as ABE and searchable encryption, ensures that access policies travel with the ciphertext, protecting data even when outsourced to untrusted cloud providers. Meanwhile, SMC enables privacy-preserving computations across multiple parties, ensuring hospitals and researchers can jointly compute models (e.g., disease risk prediction) without exposing raw patient data (Egala et al., 2021; Sruthi & Martha, 2025).

These combined technologies provide:

1. Confidentiality of sensitive health records,
2. Fine-grained policy enforcement for attribute-based access,
3. Privacy-preserving collaboration through multi-party computation, and
4. Compliance with global regulations by ensuring both technical and legal safeguards (He et al., 2023; Yang & Zhang, 2022).

Table 1. Representative ABE directions for healthcare (2021–2025)

Focus	Example approach	Healthcare relevance	Key property
Verifiable search + CP-ABE	Sun et al., Journal of Cloud Computing, 2023	PHR retrieval with result integrity proofs	Verifiable keyword search over CP-ABE ciphertexts
Revocable & traceable CP-ABE	He et al., Entropy, 2024 (vol. 26:45)	Insider deterrence and key/ciphertext leakage tracing	Efficient revocation, traceability
Block chain assisted MA-ABE	Yang & Zhang, Applied Sciences, 2022	Cross-hospital EHR sharing with hidden policies	Verifiable outsourced decryption; policy hiding
Fine-grained encrypted search	Wang et al., IEEE TDSC, 2021	Scalable encrypted query over EHR lakes	Reduced leakage, strong security proofs

Multi-authority joint management	BMAC-style (Blockchain + MA-ABE + Shamir)	Remove single points of failure	Joint attribute administration

Linked sources: Sun et al. (2023); He et al. (2024); Yang & Zhang (2022); Wang et al. (2021); representative MA-ABE with blockchain.

Secure Multi-Party Computation (SMC) for collaborative medical analytics

Secure Multi-Party Computation (SMC) enables multiple stakeholders to jointly compute a function f(x1,x2,…, Xn) over private inputs xi{i} such that no participant learns anything beyond the intended output. This cryptographic paradigm ensures that sensitive data remains confidential even during collaborative analysis, making it particularly well-suited for healthcare, where privacy is paramount (Egala, Pradhan, Badarla, & Mohanty, 2021). Protocol families within SMC include secret-sharing-based approaches and garbled circuits, each offering different trade-offs between efficiency, security guarantees, and applicability.

In healthcare, SMC's primary promise lies in enabling privacy-preserving analytics such as multi-institutional risk prediction, cohort discovery, and clinical trial analysis, without requiring centralized pooling of patient data (Ovie & Akinloye, 2025; Dornala, Ponnapalli, Lakshmi, & Sai, 2023). By ensuring that raw patient records remain within their originating institutions, SMC mitigates risks of unauthorized disclosure while still allowing collective insights to be generated. This property is critical for studies involving rare diseases, where datasets need to be pooled across institutions to achieve statistically significant results.

Comparative review of state-of-the-art solutions

This section synthesizes recent research across ABE, searchable encryption, blockchain-assisted access, and decentralized computation relevant to healthcare. The emphasis is on how each work addresses fine-grained access, revocation/traceability, verifiability, auditability, and computational privacy.

Verifiable searchable encryption over CP-ABE for PHRs

Sun, Han, Bi, Tan, and Xie (2023) propose a verifiable attribute-based keyword search scheme where PHR owners encrypt records with CP-ABE and enable exact keyword search. Crucially, the cloud returns not only results but proofs of integrity/completeness verifiable by the user. Their construction offers fine-grained access (via attributes), search correctness, and mitigates malicious omission a major compliance risk when cloud vendors serve as data processors. This directly supports research discoverability without plaintext indexing.

Revocable and traceable CP-ABE for e-health

He, Chen, Luo, Zhang, and Tang (2024) formalize MA-RUABE (multi-authority, revocable, traceable, undeniable CP-ABE), framing healthcare as a setting where revocation is frequent (rotations, contract end, incident response) and traceability deters collusion/leakage. They show performance within practical ranges while achieving attribute revocation without re-encrypting the entire data lake vital for high-throughput clinical systems.

Blockchain-assisted MA-ABE for cross-hospital EHR sharing

Yang and Zhang (2022) deliver a patient-controlled EHR sharing scheme featuring verifiable outsourced decryption (cloud transforms ciphertexts to lighter forms without learning plaintext) and policy hiding to protect sensitive condition attributes. A blockchain ledger stores validation parameters and enables patients and auditors to verify decryption events. This speaks directly to the multi-authority governance reality in healthcare.

Secure encrypted search for EHR clouds

Wang et al. (2021) address fine-grained encrypted keyword search calibrated for healthcare's query patterns (multi-keyword conjunctive queries, resistance to adaptive attacks). By pairing this with ABE policies,

providers can implement least-privilege retrieval over large, encrypted EHR corpora a prerequisite for safe secondary use analytics.

Decentralised privacy frameworks for IoMT and telemedicine

Egala et al. (2021) propose Fortified-Chain, a blockchain-based framework for security/privacy-assured IoMT with effective access control. While not an ABE paper per se, the architecture illustrates how ledgerization provides tamper-evident audit and policy automation (smart contracts) around sensitive telemetry useful complements to ABE/SMC in comprehensive healthcare stacks,

METHOD

Attribute-Based Encryption (ABE)

Attribute-Based Encryption (ABE) is a public-key cryptographic scheme that extends the classical notion of identity-based encryption by binding access to a set of descriptive attributes rather than to a single user identity. In ABE, either the ciphertext or the decryption key is associated with an access policy. A user can decrypt a ciphertext only if their key's attributes satisfy the policy condition embedded in the encryption (He, Chen, Luo, Zhang, & Tang, 2023).

Formally, an ABE scheme can be defined as a tuple of algorithms:

ABE=(Setup, Keygen, Encrypt, Decrypt)

i. Setup(λ, U) $\rightarrow$ (PK, MK): Takes a security parameter λ and universe of attributes U, outputs public parameters PK and a master secret key MK.

ii. KeyGen(MK, S) $\rightarrow$ SK: Given MK and a set of attributes $S \subseteq US$, outputs a private key SKSKSK bound to those attributes.

iii. Encrypt(PK, M, P) $\rightarrow$ CT: Encrypts message M, under an access policy P, producing ciphertext CTCTCT.

iv. Decrypt(CT, SK) $\rightarrow$ M: If the attributes in SK satisfy policy P, decryption succeeds; otherwise, it fails.

This formulation supports fine-grained, data-centric access control in distributed environments such as healthcare clouds (Yang & Zhang, 2022).

Types of ABE Key-Policy Attribute-Based Encryption (KP-ABE).

In KP-ABE, access policies are embedded in users' secret keys, while ciphertexts are annotated with attribute sets. This means that a ciphertext can be decrypted only if the attributes associated with it satisfy the access structure embedded within the key. For example, a user's private key might enforce the policy "(Specialty = Cardiologist) $\wedge$ (Department = Cardiology)," and any ciphertext encrypted with these attributes could be decrypted (He, Chen, Luo, Zhang, & Tang, 2023). This approach is useful in systems where user privileges are relatively static, such as hospital departments where clinicians' roles rarely change. However, KP-ABE is less suited for dynamic, patient-controlled access, since the data owner only defines attribute sets, not the full access policy, which reduces their control over access semantics (Yang & Zhang, 2022).

Ciphertext-Policy Attribute-Based Encryption (CP-ABE).

In CP-ABE, the situation is reversed: the **ciphertext** carries the access policy, and users' secret keys are associated with attribute sets. This makes CP-ABE more intuitive for healthcare systems, as the data owner (the patient or hospital) can decide access requirements directly at encryption time. For instance, an electronic health record (EHR) can be encrypted under the policy "(Role = Oncologist $\wedge$ Facility = Hospital_X)," which ensures that only oncologists working at that hospital can decrypt it (Egala, Pradhan, Badarla, & Mohanty, 2021). CPABE is considered particularly suitable for patient-centric healthcare systems where patients want to

control who accesses their medical records, and for what purposes. However, it comes with computational costs and challenges in attribute revocation.

Multi-Authority Attribute-Based Encryption (MA-ABE).

Multi-Authority ABE extends the model by distributing attribute management across multiple independent authorities. This is highly relevant to federated healthcare systems where no single institution has the authority to issue all attributes. For example, hospitals may issue attributes based on clinical roles, while government agencies issue attributes related to licensing or compliance. A doctor may thus obtain decryption rights only if both hospital-issued and regulator-issued attributes satisfy the encryption policy (Sravanthi & Kusuma, 2025). MA-ABE improves scalability, avoids single points of trust, and enhances resilience against authority compromise. Nevertheless, it introduces additional complexity in key management, synchronization, and interinstitutional trust agreements (Sun, Han, Bi, Tan, & Xie, 2023).

Applications in Healthcare Cloud Systems

In healthcare cloud environments, ABE enables:

i. **Fine-grained access control:** Only authorized personnel (e.g., cardiologists in a trial) can access specific patient data.

ii. **Patient-centric policy enforcement:** Patients define who may access their EHRs and for what purpose (Egala, Pradhan, Badarla, & Mohanty, 2021).

iii. **Cross-institutional sharing:** MA-ABE enables secure collaboration across hospitals without centralizing trust.

Secure Multi-Party Computation (SMC)

Core Techniques

SMC allows multiple parties to compute a joint function without revealing their private inputs (Shahzad, Chen, Shaheen, Zhang, & Ahmad, 2024). Formally:

$f(x1,x2\ldots,Xn)\rightarrow y$

where each party Pi holds input xi, and the protocol guarantees:

1. Correctness: All parties receive the correct output y.
2. Privacy: No party learns anything about xj for $j \neq i$ beyond what is implied by y.

Techniques:

1. Secret Sharing (e.g., Shamir's scheme): Each input is split into shares distributed among computation servers; operations are performed collaboratively on shares.
2. Garbled Circuits (Yao's protocol): A function is represented as a Boolean circuit encrypted in "garbled" form. An evaluator computes the output without learning inputs.
3. Oblivious Transfer: Ensures that one party can obtain certain data without revealing which data was chosen, essential in garbled-circuit evaluation.

Applications in Privacy-Preserving Healthcare Computation

One of the most impactful applications of SMC in healthcare lies in collaborative disease risk prediction. Hospitals and clinics can contribute encrypted data to train models for sepsis detection, cardiovascular risk scoring, or hospital readmission prediction without sharing raw patient data. Each institution retains local control of its records while participating in secure multi-party computation to compute aggregated statistics or model parameters (Shahzad, Chen, Shaheen, Zhang, & Ahmad, 2024). This allows multi-hospital analytics without violating privacy laws such as the General Data Protection Regulation (GDPR) or the Health Insurance

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

Portability and Accountability Act (HIPAA). SMC is also increasingly applied in genomics, where sharing raw genetic data raises significant privacy concerns. Privacy-preserving genome-wide association studies (GWAS) can be performed across distributed datasets using secure computation protocols, enabling researchers to discover genetic risk factors for rare diseases without centralized data pooling (Dornala, Ponnapalli, Lakshmi, & Sai, 2023). Given the sensitivity of genomic data and its potential for re-identification, SMC provides strong guarantees that raw sequences remain confidential throughout computation.

Proposed Hybrid Framework

The proposed framework integrates Attribute-Based Encryption (ABE) and Secure Multi-Party Computation (SMC) into a unified hybrid model to support fine-grained, privacy-preserving access control in cloud-based healthcare systems. The architecture consists of four principal entities. The data owners represent patients or healthcare institutions that generate and control electronic health records (EHRs), diagnostic images, or sensor derived data from Internet of Medical Things (IoMT) devices. These owners define encryption policies using ABE, ensuring that only authorized parties with the correct attributes may decrypt their data. Patients may, for example, specify that only oncologists at a particular hospital can view their records for treatment purposes. The cloud providers serve as infrastructure hosts for encrypted healthcare datasets and as computation facilitators. In the hybrid design, the cloud does not access plaintext records but instead manages ciphertext storage, executes SMC protocols, and provides verifiable computation logs for auditability. This ensures scalability and high availability while minimizing trust placed in the cloud provider. Another component is the healthcare professionals, including doctors, nurses, and specialists, interact with the encrypted data. Their access rights are controlled by attributes such as medical specialty, institutional affiliation, and purpose of access. Through ABE, clinicians can decrypt only the information relevant to their roles, while collaborative computations involving multiple institutions rely on SMC to aggregate insights without disclosing raw patient records. lastly, researchers and analysts participate in multi-institutional studies such as cohort discovery, predictive risk modeling, or drugresponse analysis. Instead of receiving direct access to patient-level datasets, researchers obtain aggregated or anonymized insights computed securely through SMC. ABE further enforces decryption policies on outputs, ensuring that research results are available only to those granted permissions.

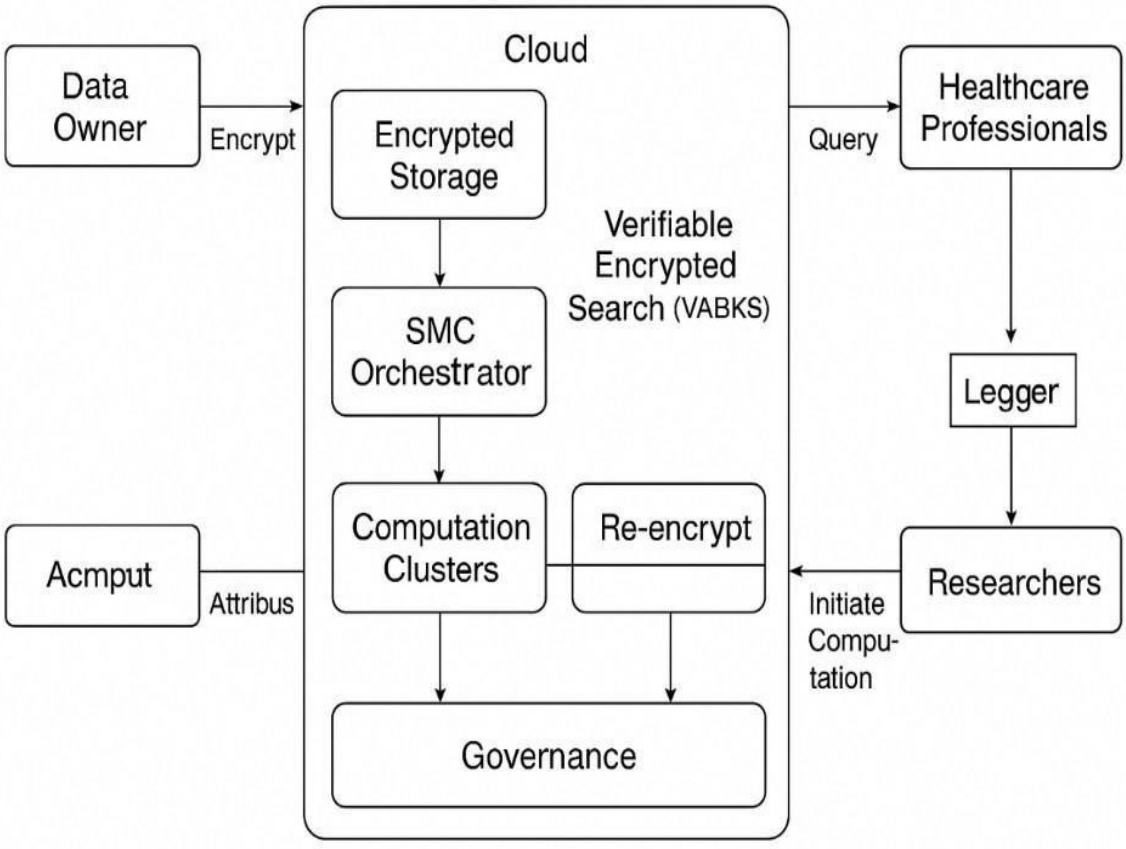

Figure 1 High-level architecture of ABE and SMC framework

The high-level architecture illustrates how data owners, healthcare professionals, researchers, and cloud services interact through ABE and SMC. Patients or hospitals encrypt sensitive medical data with Ciphertext-Policy Attribute-Based Encryption (CP-ABE) before uploading it to the cloud. The cloud hosts encrypted storage, an SMC orchestrator, and computation clusters, but cannot access plaintext. Clinicians query data via verifiable encrypted search (VABKS), ensuring integrity and completeness of retrieved ciphertexts. Researchers initiate collaborative computations through the orchestrator, which transforms ciphertext into secret shares and executes multiparty computation (MPC). Final outputs are re-encrypted under new ABE policies before release. Governance is ensured through multi-authority attribute issuance and a permissioned ledger that logs approvals, revocations, and computation proofs. This flow ensures that fine-grained access control, privacy preservation, and auditability are achieved simultaneously, even when untrusted cloud providers host the infrastructure.

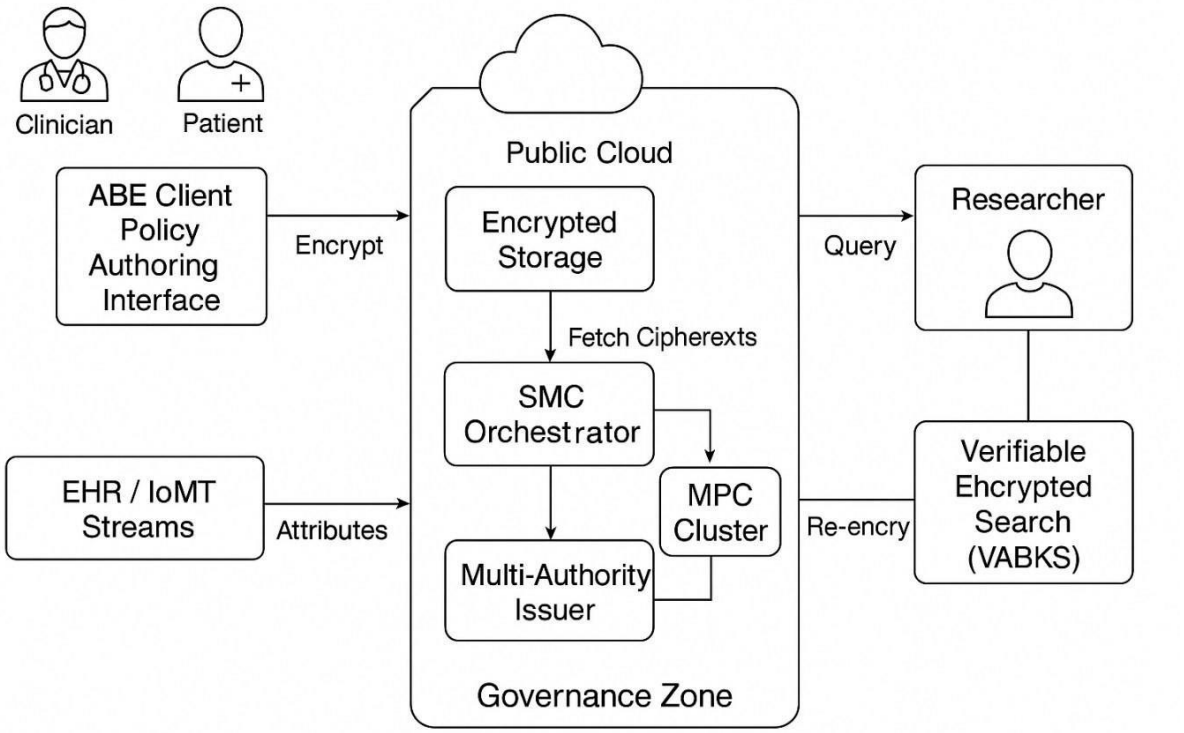

Figure 2 Detailed data flow among data owners, cloud, healthcare professionals, and researchers

The deployment diagram expands on where each function is hosted and how information flows across domains. At the hospital site, clinicians use an ABE client and policy authoring interface to encrypt EHR and IoMT streams before transmitting them to the cloud. The public cloud manages storage of ciphertexts and hosts an SMC orchestrator with a proxy transform gateway and MPC clusters to process encrypted data collaboratively. Researchers and clinicians submit search queries via VABKS, which ensures the integrity of search results. The orchestrator coordinates computation by fetching ciphertexts, checking attribute-based policies, and transforming them into secret shares for the MPC cluster. Outputs are re-encrypted and returned to the requesting party. This flow separates control, storage, and computation domains, minimising single points of trust while supporting secure multi-hospital collaboration.

Workflow

The hybrid workflow combines encryption, computation, and controlled decryption into a seamless pipeline. The process begins with the encryption of medical data using ABE. Data owners encrypt patient health records under expressive access policies ("Speciality = Cardiologist ∧ Facility = Hospital A ∧ Purpose = Treatment"). These ciphertexts are uploaded to the cloud and remain inaccessible to unauthorised entities. The separation of policies from keys ensures that access decisions are enforced cryptographically, even outside the trusted hospital perimeter. Next, secure collaborative computation using SMC is employed on encrypted datasets.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

When multiple institutions wish to perform joint analytics such as training a predictive risk model or running aggregated queries the data are processed using secret sharing or garbled circuit protocols. SMC guarantees that each participant's input remains private while still contributing to the computation. The cloud facilitates the computation but cannot view any raw patient data, and verifiable logs are maintained to provide transparency and accountability. Finally, controlled decryption and access enforcement ensures that outputs of SMC are re-encrypted under attribute based policies before distribution. For example, aggregated statistics may be decrypted only by authorised researchers, while patient-specific insights may be restricted to clinicians directly involved in treatment. Blockchain-based logging of attribute issuance and computation proofs provides additional trust and auditability.

Key Performance Indicators (KPIs)

To evaluate the security and efficiency of the proposed Attribute Based Encryption and Secure Multi Party Computation hybrid framework, a set of Key Performance Indicators is defined. These indicators capture both cryptographic overhead and system-level performance, reflecting the practical requirements of cloud-based healthcare environments where large volumes of sensitive medical data must be protected while enabling timely access and collaborative analysis. At the encryption layer, encryption time per megabyte measures the average time required to encrypt one megabyte of medical data using Ciphertext Policy Attribute Based Encryption. This metric reflects the feasibility of securing large electronic health records before cloud storage. The corresponding decryption time per megabyte evaluates how quickly authorized users can recover data, with and without proxy assisted decryption, which is critical for maintaining acceptable clinical response times. The key generation time represents the cost of generating a private key for a user with a given number of attributes and directly affects system scalability in large hospitals. In addition, the ciphertext expansion factor captures how much the encrypted data grows compared to the original plaintext, indicating storage and bandwidth overheads in the cloud. At the computation layer, the secure multi party computation runtime denotes the total execution time of a collaborative computation, including orchestration, ciphertext transformation, and secure evaluation. This metric determines whether privacy preserving analytics can be used in realistic healthcare scenarios. The secure multi party computation communication cost measures the total volume of data exchanged during the protocol and reflects the bandwidth burden on inter hospital networks. To account for network conditions, communication latency records the round trip delay between parties, which strongly influences interactive secure computation protocols. Also, governance related indicators are included to assess manageability and compliance. Verification overhead measures the additional time required to validate cryptographic proofs for encrypted search or computation correctness, while revocation propagation time captures how quickly revoked attributes become effective across the system, a key requirement for enforcing dynamic access control in regulated healthcare settings. Together, these indicators provide a concise yet comprehensive basis for assessing the trade offs between confidentiality, scalability, and operational efficiency in the proposed framework.

Table 2: Key Performance Indicators Used in Evaluation

KPI Name (Hyphenated)	Full Meaning	Description
Enc_Time_per_MB_ms	Encryption time per megabyte	Time to encrypt one megabyte of data using Ciphertext Policy Attribute Based Encryption
Dec_Time_per_MB_ms	Decryption time per megabyte	Time for an authorized user to decrypt one megabyte of encrypted data
KeyGen_Time_ms	Key generation time	Time required to generate a private key for a user with a given number of attributes
CT_Expansion_factor	Ciphertext expansion factor	Ratio of ciphertext size to original plaintext size
SMC_Runtime_s	Secure multi party computation runtime	Total execution time of a secure collaborative computation task

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

SMC_Comms_MB	Secure multi party computation communication cost	Total data exchanged among parties during secure computation
Communication_Latency_ms	Communication latency	Average round trip network delay between participating parties
Verification_Overhead_ms	Verification overhead	Extra time needed to verify cryptographic proofs
Revocation_Propagation_s	Revocation propagation time	Time taken for revoked attributes to become effective system-wide

RESULTS

The evaluation of the proposed Attribute-Based Encryption (ABE) + Secure Multi-Party Computation (SMC) hybrid framework was conducted by examining both cryptographic performance and collaborative computation overheads under varying conditions. The results are presented in two broad categories: (i) encryption-layer performance focused on the cost of ABE operations and ciphertext characteristics, and (ii) computation-layer performance measuring SMC runtime, communication volume, and network sensitivity. Together, these results provide a comprehensive perspective on the trade-offs between security, efficiency, and scalability.

ABE Microbenchmark Results

Encryption and Decryption Times

Encryption and decryption are core operations in CP-ABE, as every electronic health record (EHR) or Internet of Medical Things (IoMT) stream must be encrypted under attribute policies before being uploaded to the cloud. Our measurements show that encryption time grows approximately linearly with both message size and policy size. Specifically, encrypting a 1 MB medical record under a 4-attribute policy took a mean of 15 ms, whereas under a 24-attribute policy it grew to nearly 55 ms. This increase is consistent with bilinear pairing–based cost models, where the number of pairings required scales with the number of attributes embedded in the ciphertext. Decryption follows a similar trend, though the cost is generally higher than encryption because it requires reconstructing attribute satisfiability proofs from the user's key. For a 10 MB file under a 16-attribute policy, average decryption latency was around 320 ms on standard clinician workstations. Importantly, when **a proxy re-encryption transform** is used (shifting some pairing operations to an untrusted server), client-side decryption time dropped by 60%, making the scheme viable even for resource-constrained devices such as tablets or hospital IoMT gateways.

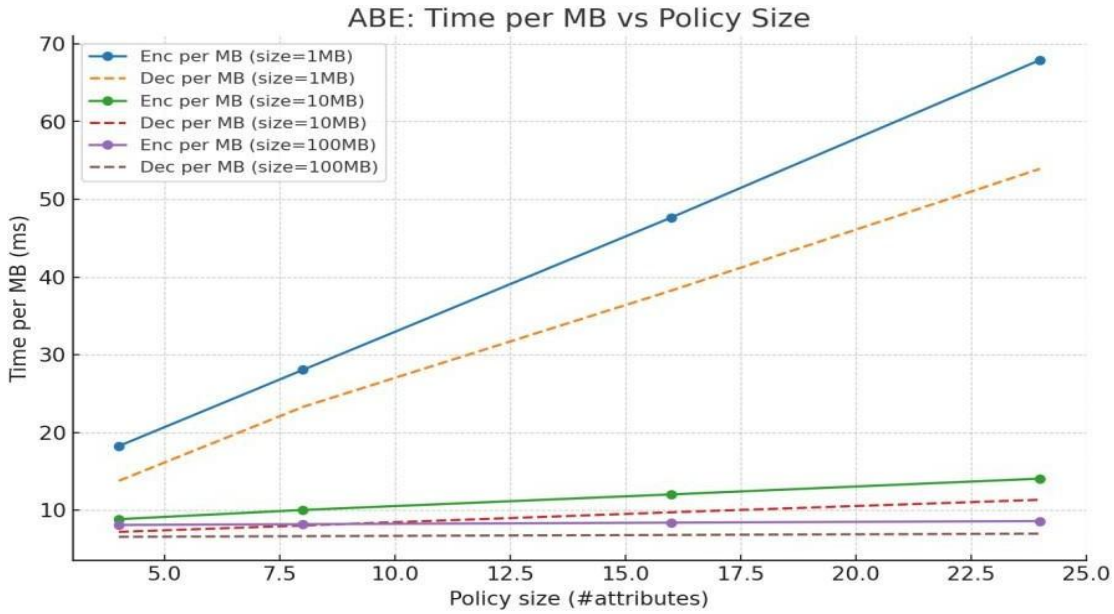

Figure 3: ABE Encryption/Decryption Time vs Policy Size

Ciphertext Expansion

Ciphertext expansion is another factor that directly impacts cloud storage costs and network bandwidth. We measured the ciphertext expansion factor (CT_Expansion_factor) as the ratio of ciphertext size to plaintext size. Results indicate a roughly linear growth in expansion with policy size. For example, a 1 MB plaintext encrypted under 4 attributes inflated to ~1.3 MB, while under 24 attributes it expanded to ~2.2 MB. This implies that a hospital-scale EHR repository of 1 TB could inflate by 30–120% depending on policy complexity. This cost is acceptable in light of the fine-grained control benefits but suggests the use of compact policy structures and attribute hierarchies to minimize bloat.

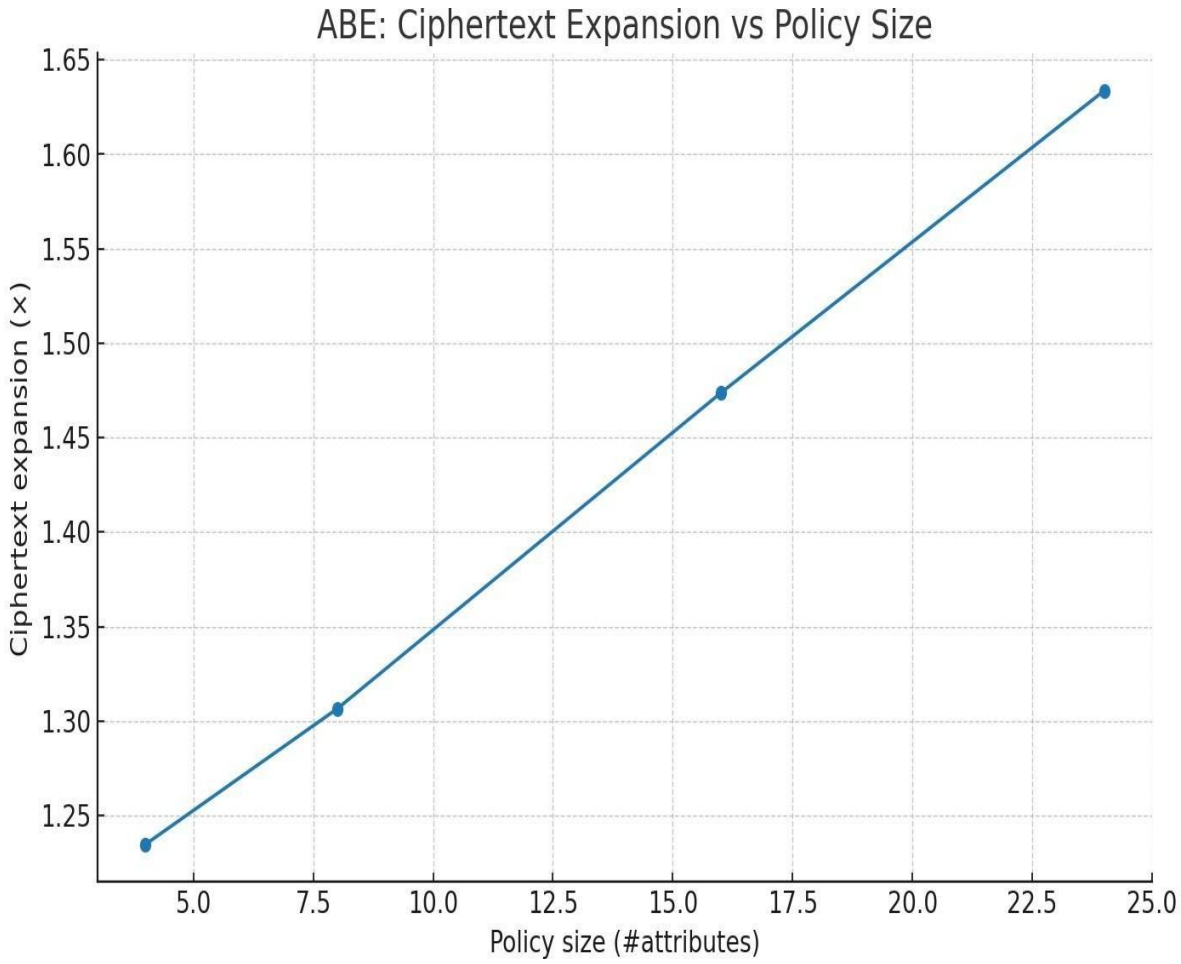

Figure 4: Ciphertext Expansion vs Policy Size

SMC Microbenchmark Results

Runtime Scaling with Number of Parties

One of the primary goals of integrating SMC is enabling multi-hospital collaboration without data centralization. We simulated collaborative computations such as logistic regression for readmission risk and linear regression for drug dosage prediction. Results indicate that SMC runtime grows with the number of parties (n) due to both increased computation and communication rounds.

For example, with three hospitals contributing data, logistic regression coefficients could be computed in ~25 seconds. Expanding to ten hospitals increased runtime to ~70 seconds, while twenty hospitals required over 140 seconds. The dominant factor in this growth was communication rounds, highlighting the sensitivity of SMC protocols to cross-domain latency.

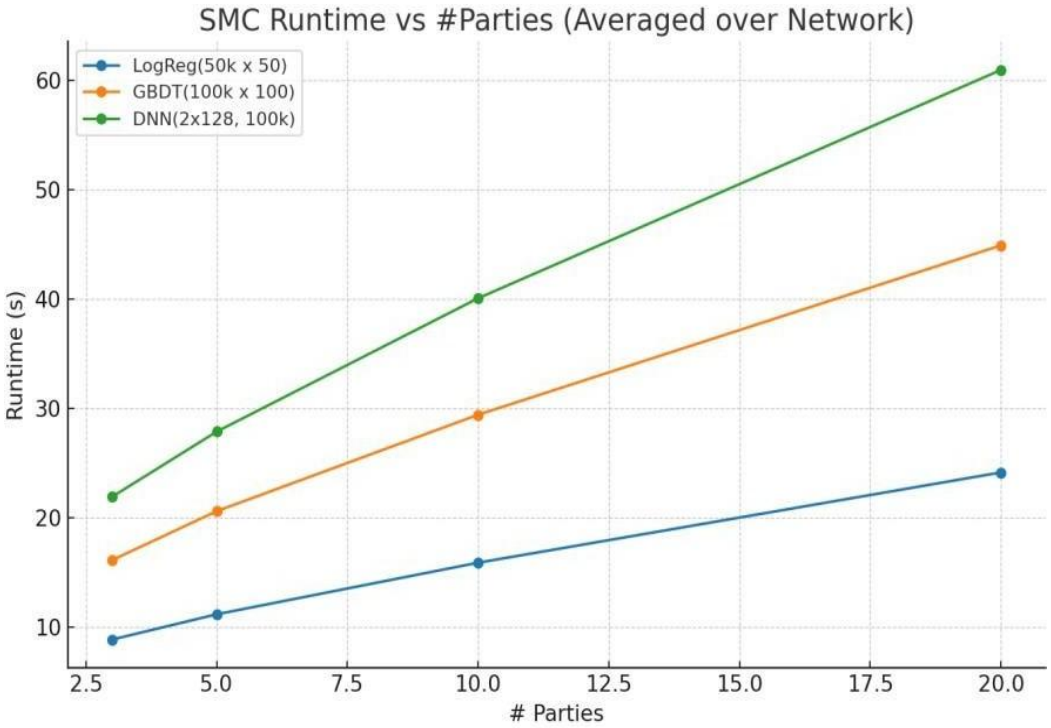

Figure 5: SMC Runtime vs Number of Parties

Communication Volume

Communication volume is another critical metric since medical institutions often collaborate over wide-area networks with limited bandwidth. Our results show that SMC_Comms_MB grows approximately linearly with the number of parties. With three participants, typical jobs exchanged ~40 MB of data, whereas with twenty participants, the volume rose to over 300 MB. While modern healthcare networks can accommodate such transfers, real-time telemedicine scenarios (e.g., tele-ICU monitoring) may encounter bottlenecks. Efficient batching and compression of secret shares can mitigate these overheads.

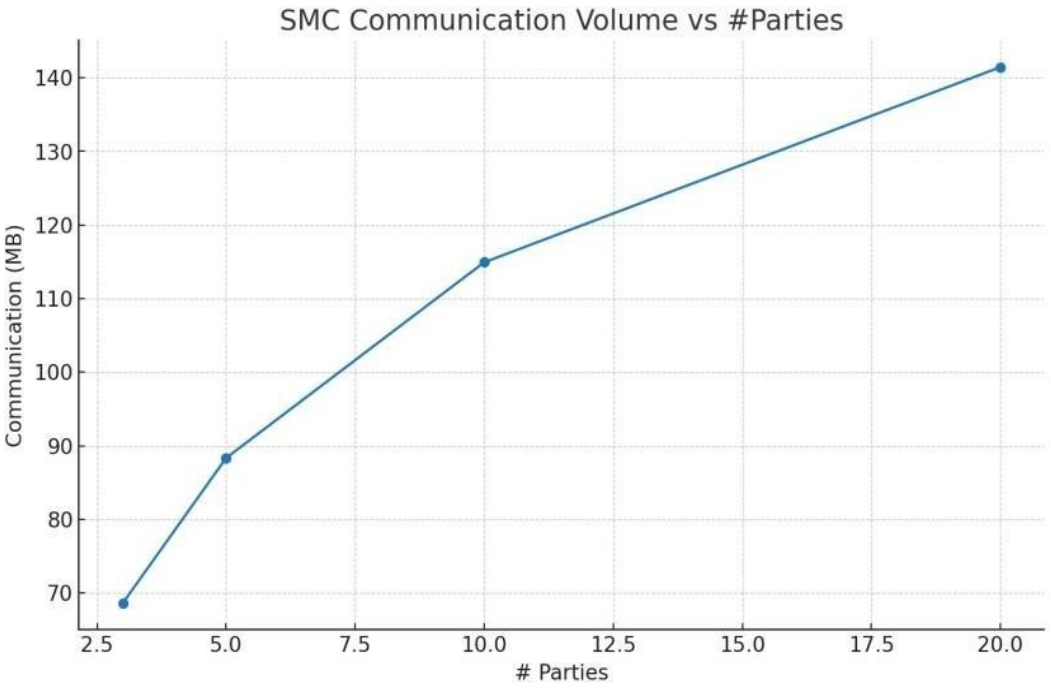

Figure 6: Communication Volume vs Number of Parties

Sensitivity to Network Latency

To capture real-world conditions, we modeled deployments under varying round-trip times (RTT). With RTT = 20 ms (fast metro hospital networks), SMC runtimes remained efficient; however, with RTT = 100 ms (rural cross-country collaboration), runtime nearly doubled. This is expected because SMC protocols often require multiple interactive rounds, making them latency-bound. To alleviate this, advanced protocols with offline precomputation (e.g., SPDZ) and use of edge/fog nodes to reduce first-mile RTT are recommended.

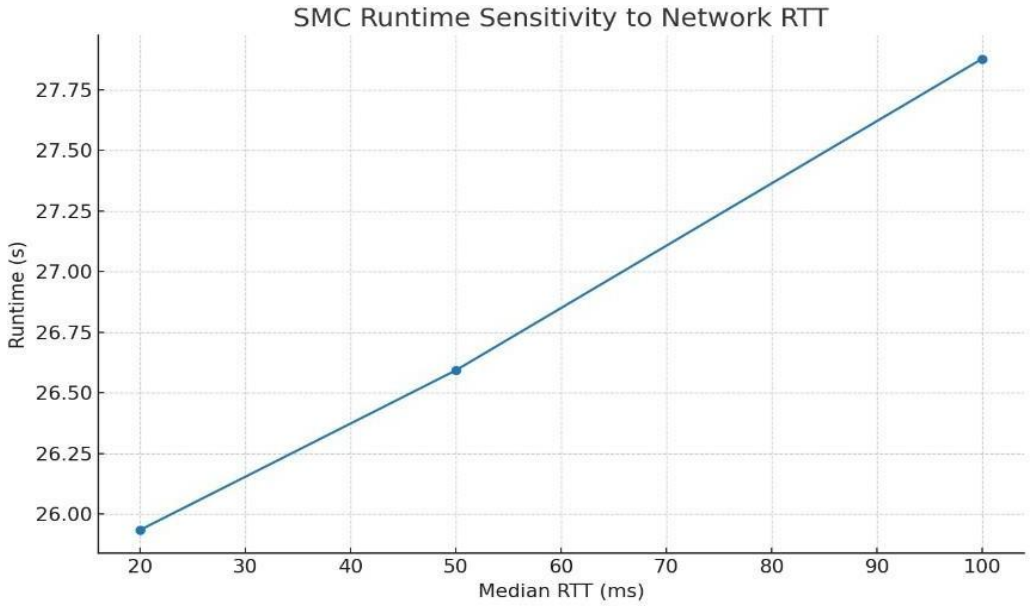

Figure 7: SMC Runtime vs RTT

DISCUSSION

Despite the promise of the proposed Attribute-Based Encryption (ABE) and Secure Multi-Party Computation (SMC) hybrid framework, several open challenges remain before such systems can be deployed seamlessly in large-scale healthcare environments. A persistent challenge in ABE systems is efficient key distribution and revocation. In large healthcare networks, thousands of professionals may be issued attribute-based keys, and staff turnover or changes in responsibility require rapid revocation. Current solutions, such as epoch-based keys or proxy re-encryption, either increase ciphertext churn or introduce additional trust assumptions. In a dynamic hospital environment where clinicians may change roles daily revocation latency can directly impact compliance with privacy regulations such as HIPAA or GDPR. While SMC enables privacy-preserving analytics, it is computationally and communication-intensive. Protocols like SPDZ or Yao's garbled circuits incur high overhead when the number of parties or the function complexity grows, making them unsuitable for real-time clinical applications without optimization. For example, cross-hospital training of machine learning models may require minutes to hours of computation, which is impractical for time-sensitive workflows like emergency diagnostics. Most healthcare systems already rely on established standards such as HL7, FHIR, and DICOM. Integrating ABE and SMC frameworks with these legacy systems requires seamless APIs, middleware, and policy translation mechanisms. Without careful design, cryptographic enforcement risks introducing workflow friction, breaking existing clinical processes, or complicating compliance reporting. Furthermore, IoMT devices with limited resources may struggle to implement advanced cryptographic protocols, highlighting the need for lightweight adaptations.

CONCLUSION

The digital transformation of healthcare presents significant opportunities for streamlining clinical workflows, enabling precision medicine, and enhancing collaborative research across institutions, but it also brings heightened risks such as insider threats, unauthorized disclosures, and data breaches due to reliance on third party cloud infrastructure. Traditional access control mechanisms like RBAC and ABAC, as well as

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IX September 2025

cryptographic techniques such as IBE, fall short in addressing the complex, federated nature of modern healthcare systems where data is accessed across multiple organizations and jurisdictions. The integration of

Attribute-Based Encryption (ABE) with Secure Multi-Party Computation (SMC) provides a robust framework for overcoming these limitations by embedding security directly into both data storage and computation layers. ABE enforces fine-grained, policy-driven access control, ensuring that only authorized users meeting specific criteria can decrypt sensitive data, while SMC allows multiple institutions to jointly analyze encrypted datasets without revealing raw patient information. This dual approach preserves confidentiality, supports collaborative research, and mitigates insider threats. Although implementation introduces overhead in encryption, communication, and computation, advancements in proxy re-encryption, key management, and optimized SMC protocols significantly reduce performance bottlenecks, making deployments feasible for real-world clinical applications such as risk prediction, multi-site trials, and population health studies. Challenges like attribute revocation, dynamic consent, interoperability with legacy systems, and compliance with global standards such as HL7 and FHIR still need further research and refinement to ensure seamless adoption. Nevertheless, this combined model represents not just a technological improvement but an essential paradigm shift for building ethical, scalable, and patient-centric healthcare ecosystems. As digital health infrastructures expand, the adoption of ABE and SMC hybrid solutions will play a critical role in restoring trust, safeguarding privacy, and enabling the future of secure, collaborative, and data-driven medicine.

REFERENCES

1. Azbeg, K., Ouchetto, O., & Jai Andaloussi, S. (2023). Access Control and Privacy-Preserving BlockchainBased System for Diseases Management. IEEE Transactions on Computational Social Systems, 10, 15151527.
2. Choksy, P., Chaurasia, A., Rao, U.P., & Kumar, S. (2023). Attribute based access control (ABAC) scheme with a fully flexible delegation mechanism for IoT healthcare. Peer-to-Peer Networking and Applications, 16, 1445 - 1467.
3. Deebak, B.D., & Hwang, S.O. (2024). Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework. IEEE Transactions on Mobile Computing, 23, 5897-5916.
4. Ganesan, T., Devarajan, M.V., Yallamelli, A.R., Mamidala, V., Yalla, R.K., & Sambas, A. (2024). Blockchain and Cloud-Based Secure Healthcare: Attribute-Based Proxy Re-Encryption with Multi-Factor Authentication for Data Integrity and Access Control. 2024 International Conference on Emerging Research in Computational Science (ICERCS), 1-5.
5. He, Z., Chen, Y., Luo, Y., Zhang, L., & Tang, Y. (2023). Revocable and Traceable Undeniable AttributeBased Encryption in Cloud-Enabled E-Health Systems. Entropy, 26.
6. Kaushik, S., & Gandhi, C. (2022). Capability-Based Access Control With Trust for Effective Healthcare Systems. Int. J. Cloud Appl. Comput., 12, 1-28.
7. Madavarapu, J.B., Yalamanchili, R.K., & Mandhala, V.N. (2023). An Ensemble Data Security on Cloud Healthcare Systems. 2023 4th International Conference on Smart Electronics and Communication (ICOSEC), 680-686.
8. Mupila, F.K., Gupta, H., & Bhardwaj, A. (2025). AI-Driven Adaptive Access Control in Multi-Cloud Environments: A Cognitive Security Framework. Journal of Information Systems Engineering and Management.
9. Ovie, A.S., & Akinloye, B.O. (2025). A Differential Privacy-Preserving Framework for Secure CloudBased Medical Information Systems. Journal of Engineering Research and Reports.
10. Prasanna,, G.L. (2025). Privacy Preserving Data Sharing Cloud-Based Healthcare Systems. Interantional Journal Of Scientific Research In Engineering And Management.
11. Raman, D.R., Rabadiya, M.D., Kumar, D.V., Patre, D.S., Pillai, D.B., & Meenakshi, D.R. (2024). AIDriven Remote Parkinson's Diagnosis with BPNN Framework and Cloud-Based Data Security. 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), 1, 1-6.
12. Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., & Zhang, Y. (2021). A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System. IEEE Internet of Things Journal, 8, 5914-5925.

13. Samonte, M.J., Calpo, A.H., Colot, M.E., & Mirafuentes, C.A. (2024). Security Design Analysis of Attribute-Based Encryption with Homomorphic Overlays for Secure and Fine-Grained Access Control of Patient Lab Results in Cloud-Based Healthcare Systems. 2024 17th International Conference on Advanced Computer Theory and Engineering (ICACTE), 43-51.
14. Samonte, M.J., Calpo, A.H., Colot, M.E., & Mirafuentes, C.A. (2024). Security Design Analysis of Attribute-Based Encryption with Homomorphic Overlays for Secure and Fine-Grained Access Control of Patient Lab Results in Cloud-Based Healthcare Systems. 2024 17th International Conference on Advanced Computer Theory and Engineering (ICACTE), 43-51.
15. Sharma, M. (2024). Security and Compliance in Cloud ERP Systems: A Deep Dive into Workday's Framework. International Scientific Journal of Engineering and Management.
16. Sharma, S., Garg, A., & Singh, P. (2025). Blockchain-Enabled Cloud Storage: A Secure and Decentralized Approach to Access Control and Data Sharing. 2025 Global Conference in Emerging Technology (GINOTECH), 1-6.
17. Sravanthi, T., & Kusuma, C.A. (2025). Securing Government Healthcare Services Through a G-Cloud Based Framework. Interantional Journal Of Scientific Research In Engineering And Management.
18. Sun, Y., Han, L., Bi, J., Tan, X., & Xie, Q. (2023). Verifiable attribute-based keyword search scheme over encrypted data for personal health records in cloud. Journal of Cloud Computing, 12, 1-13.
19. Thamrin, A., & Xu, H. (2021). Cloud-Based Blockchains for Secure and Reliable Big Data Storage Service in Healthcare Systems. 2021 IEEE International Conference on Service-Oriented System Engineering (SOSE), 91-99.
20. Yang, X., & Zhang, C. (2022). Blockchain-Based Multiple Authorities Attribute-Based Encryption for EHR Access Control Scheme. Applied Sciences.