IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 11, November 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1211.14

Privacy-Preserving Health Data Sharing Using Secure MPC

Shruthi TS
Assistant Professor, Dept of CSE
KS Institute of Technology, Bengaluru, India
shruthits20@gmail com
https://orcid.org/0009-0008-6001-7177
Parvez Ansari, Raghusai Achuth, Manoja GV
Dept of CSE, KS Institute of Technology,
Bengaluru, India
work.seek2003@gmail.com, manojagvm@gmail.com
raghusaiachuth1729@gmail.com

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.12/Issue11/NVAE10093
Research Article| Open Access | Double-Blind Peer-Reviewed | Article ID: IJIRAE/RS/Vol.12/Issue11/NVAE10093
Received:22,October 2025,Revised:28,October 2025, Accepted:31, October 2025, Published Online: 21, November 2025.
https://www.ijirae.com/volumes/Vol12/iss-11/14.NVAE10093.pdf
Citation: Shruthi,Parvez,Raghusai,Manoja (2025), Privacy-Preserving Health Data Sharing Using Secure MPC , IJIRAE: International Journal of Innovative Research in Advanced Engineering, Volume 12, Issue 11 of 2025 pages 520-526
doi:>https://doi.org/10.26562/ijirae.2025.v1211.14
BibTeX Key: Shruthi@2025Privacy-Preserving
IJIRAE papers should be cited as IJIRAE (International Journal of Innovative Research in Advanced Engineering, AM Publications, India 2025, ISSN 2349-2163, https://doi.org/10.26562/ijirae.2025.v1211.14 The journal's official abbreviation is IJIRAE. Orcid: https://orcid.org/0009-0004-9398-7488

Abstract: Collaborative data analytics holds tremendous potential for healthcare research, but privacy regulations and ethical obligations limit data sharing between institutions. Traditional anonymization methods remain vulnerable to re-identification attacks, necessitating cryptographic techniques that enable computation without exposing raw data. We present a full-stack platform for privacy-preserving health data exchange that combines Secure Multi-Party Computation (SMPC), Homomorphic Encryption (HE), and Differential Privacy (DP). The system supports eighteen analytical tasks spanning descriptive statistics, regression, survival analysis, and federated machine learning. Comprehensive testing with simulated multi-institutional scenarios demonstrates that secure computations achieve accuracy within 0.02% of plaintext baselines while scaling linearly with dataset size. The platform integrates compliance features, real- time monitoring, and access control mechanisms aligned with HIPAA and GDPR requirements. Code and data are publicly available for reproducibility. This work bridges the gap between cryptographic theory and production healthcare systems, pro- viding a foundation for multi-institutional collaboration without compromising patient privacy.
Index Terms: Secure Multi-Party Computation, Homomorphic Encryption, Healthcare Analytics, Data Privacy, Differential Privacy, Federated Learning

I. INTRODUCTION

Healthcare institutions depend on data analytics for improving diagnosis, treatment protocols, resource allocation, and epidemiological modeling. High-quality, diverse datasets are essential for training accurate predictive models and sup- porting evidence-based clinical decisions. However, privacy regulations such as HIPAA in the United States and GDPR in the European Union impose stringent restrictions on sharing identifiable patient information. This creates tension between the need for collaborative analytics and the obligation to protect sensitive data. Traditional anonymization and de-identification techniques provide insufficient protection. Numerous studies have demonstrated successful re-identification attacks using auxiliary data sources, rendering these approaches inadequate for modern threat models. Cryptographic methods that enable joint computation without exposing raw data offer a more robust alternative. Secure Multi-Party Computation (SMPC) and Homomorphic Encryption (HE) permit computations over encrypted or secret-shared data while preserving confidentiality guarantees. This paper presents a deployable platform that integrates SMPC, HE, and optional Differential Privacy (DP) for privacy- preserving healthcare analytics. The system emphasizes Practical deployment through compliance logging, fine-grained access control, and real-time operational monitoring. Our contribution sex tend beyond cryptographic protocols to include full-stack implementation, regulatory alignment, and comprehensive validation through simulated multi-institutional testing scenarios.

IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 11, November 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1211.14

A. Motivation

Healthcare data silos significantly limit the potential of col- laborativeresearch,especiallywhenmultipleinstitutionscould benefit from pooling insights without exposing raw patient records. While privacy-preserving computation technologies have matured considerably, few systems integrate them into complete, deployable platforms ready for institutional use. Moreover, regulatory frameworks like HIPAA and GDPR demand more than just secure computation—they require comprehensive auditability, fine-grained access control, and operational transparency that most research prototypes over-look.

Contributions

The main contributions of this paper are: A full-stack, deployable platform that integrates SMPC, HE, and DP for privacy-preserving healthcare analytics.

- Support for 18 analytical tasks spanning descriptive statistics, regression, survival analysis, and federated machine learning.
- Extensive evaluation of accuracy, latency, scalability, and resource utilization with synthetic healthcare datasets.

TABLE I: Comparison of Privacy-Preserving Medical Data Sharing Schemes

Scheme	Security Primitives	Access Control	Data Authenticity	Data Encryption	Architecture Type	Data Storage	Smart Contracts	Intero perability
Lindell-Pinkas[1]	SMPC+DM	Limited	Yes	Symmetric	Distributed	Off-chain	No	Low
MedRec[2]	Blockchain	Yes	Yes	Symmetric	Permissionless	Off-chain	Yes	Moderate
BBDS[3]	Blockchain+ABE	Yes	Yes	Symmetric	Permissioned	Off-chain	Yes	High
MedShare[4]	Blockchain+IBE	Yes	Yes	Symmetric	Permissioned	Off-chain	Yes	High
MedBlock[5]	Blockchain+HE	Yes	Yes	Asymmetric	Permissioned	Off-chain	Yes	Moderate
BSPP[6]	HybridBlockchain	Yes	Yes	Symmetric	Hybrid	Off-chain	Yes	High
Dong-Lin[7]	SMPC+GC	Yes	Yes	Symmetric	Distributed	Off-chain	No	Moderate
MP-SPDZ[8]	SMPCFramework	Yes	Yes	Multiple	DistributedMPC	Off-chain	No	High
Sahinbas-Catak [9]	SMPC+IoT	Yes	Yes	Symmetric	Distributed	Off-chain	No	Moderate
Patel-Rao[10]	SMPC	Yes	Yes	Symmetric	DistributedMPC	Off-chain	No	High
vonMaltitz[11]	MPC	Yes	Yes	Symmetric	DistributedMPC	Off-chain	No	Moderate
PriCollab[12]	MPC	Yes	Yes	Symmetric	DistributedMPC	Off-chain	No	Moderate
PriCollab Analysis [13]	MPC+Blockchain	Yes	Yes	Symmetric	Hybrid	Off-chain	Yes	Moderate
OurPlatform	SMPC+HE+DP	Yes	Yes	Homomorp hic	DistributedMPC	Off-chain	No	High

- Integration of compliance and monitoring features aligned with HIPAA and GDPR requirements.
- Open-source implementation that demonstrates technical feasibility for multi-institutional health care collaboration.

II. RELATED WORK

Privacy-preserving healthcare analytics has evolved signif- icantly as researchers explore techniques including Secure Multi-Party Computation (SMPC), homomorphic encryption (HE), and differential privacy (DP).These methods address the fundamental challenge of enabling collaborative data analysis while protecting patient confidentiality. The theoretical foundations for privacy-preserving health- care analytics emerged over several decades, from Shamir's [14]secret sharing and Paillier's[15] homomorphic encryption to Dwork et al.'s [16] differential privacy and Gentry's [17] breakthrough in fully homomorphic encryption. Translating these primitives required significant engineering, leading to practical systems like the secure aggregation mechanisms developed for federated learning[18],[19] and flexible SMPC frameworks like MP-SPDZ [8]. In healthcare, specific applications include using SMPC for patient risk stratification [7], secure imputation of miss-ing clinical data [20], and managing data sharing across institutions [10]–[12]. Prior surveys, such as Jin et al. [21], have highlighted the need to bridge the gap between crypto- graphic research and deployable, interoperable systems. Our work builds on these contributions by emphasizing practical deployment, regulatory compliance, and end-to-end system integration.

A. Comparison with Related Systems

Following Jin et al.'s [21] survey, we position our platform relative to existing schemes. Table I compares architectural philosophies. Blockchain approaches [2]–[6] leverage de- centralized trust and immutable ledgers but incur consensus overhead. In contrast, our platform adopts a pure cryptographic approach, strategically combining Homomorphic Encryption (HE) for efficient simple aggregations with full SMPC for complex analytics. This hybrid strategy yields a lightweight, high-performance solution particularly appropriate for HIPAA- regulated environments, eliminating the complexity associated with block chain infrastructure while maintaining strong security guarantees. Beyond architectural choice, deployment readiness is cru- cial. Table II compares implementation characteristics. While most related work provides prototypes, few offer real-time coordination features essential for multi-institutional work- flows. Our platform

uniquely combines a prototype implementation, real-time Web Socket based coordination, and open- source availability, making it immediately deployable for privacy-preserving analytics.

TABLE II: Implementation Readiness Across Related Work

Work	Prototype	Real-time / Live	OpenCode
Lindell-Pinkas[1]	✓	–	–
MedRec[2]	✓	–	–
BBDS[3]	✓	–	–
MedShare[4]	✓	–	–
Dong-Lin[7]	✓	–	–
MP-SPDZ[8]	✓	–	✓
Sahinbas-Catak[9]	✓	–	–
vonMaltitz[11]	✓	–	–
Patel-Rao[10]	✓	–	–
PriCollab[12]	✓	–	–
PriCollabAnalysis[13]	✓	–	–
OurPlatform	✓	✓	✓

III. SYSTEM ARCHITECTURE

The proposed system follows a modular design that sep- arates orchestration, computation, data preparation, and user interaction concerns. Figure 1 illustrates the overall architecture. Key components include:

- Coordinator API: A Fast API backend orchestrating lifecycles, invitations, and role-based access control (RBAC).
- Computation Engine: Implements SMPC (Shamir secret sharing, $t = n - 1$) and opportunistic HE acceleration (Paillier).
- Data Preparation Layer: Validates inputs, applies fixed- point encoding, and generates cryptographic shares or ciphertexts locally.
- Client Applications: React/Next.js interfaces providing computation wizards and result dashboards.
- Audit and Monitoring Layer: Captures fine-grained events and generates compliance reports (HIPAA/GDPR aligned).

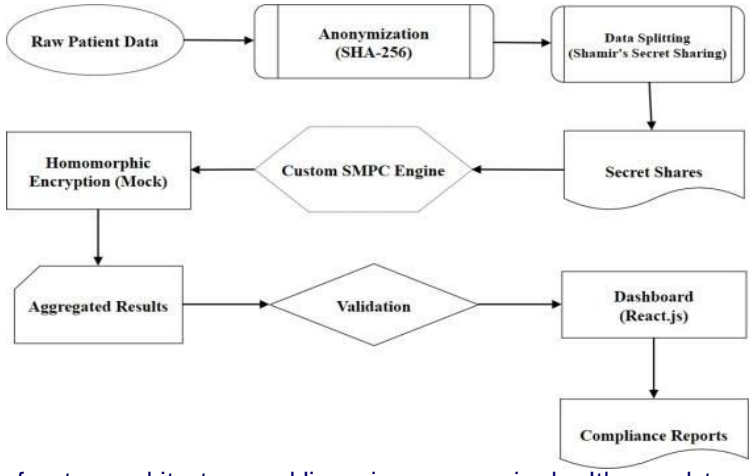

Fig.1: Overview of system architecture enabling privacy-preserving health care data exchange using secure multi-party computation and federated analytics.

A. DataFlow

The end-to-end workflow proceeds through four stages. First, an organizer creates a computation request and issues targeted invitations. Second, accepting institutions locally preprocess their data, apply fixed-point encoding, and produce secret shares or Paillier ciphertexts. Critically, no plaintext data leaves the institution. Third, the Coordinator orchestrates secure computation rounds, selecting HE for simple aggrega- tions and SMPC for complex analytics (regression, survival). Finally, the engine reconstructs only the final aggregate result (with optional differential privacy noise) and delivers it to authorized parties over secure channels, while all events are logged for audit.

IV. IMPLEMENTATION DETAILS

Our implementation prioritizes security, scalability, and ease of deployment. We chose Python's FastAPI for the asynchronous backend and React/Next.js for the responsive frontend.

A. Core Components

- Coordinator API: Oversees the entire computation life- cycle. It enforces RBAC via JWT authentication and ex- poses RESTful endpoints alongside WebSocket channels for live status updates.

- Computation Engine: Implements Shamir Secret Shar- ing (t=n− 1) for SMPC and the Paillier cryptosystem for homomorphic encryption. It dynamically selects be- tween HE and SMPC based on protocol complexity for the eighteen supported analytical tasks (Table III).
- Data Preparation Module: Validates inputs against predefined schemas, applies fixed-point scaling (16-bit pre- cision),and generates cryptographic shares with bounded coefficients ([0, 10^6]) locally. All transformations are performed locally, ensuring plaintext data never leaves institutional boundaries.
- Audit System: Logs every action (actor ID, timestamp, operation type) for compliance reporting, supporting HIPAA and GDPR documentation.

B. Protocol Execution Flow

1) Request and Invitation: An initiating organization creates a request and selects invited institutions. Invitations are targeted, and all responses are recorded in the audit log.
2) Local Data Transformation: Participants encode their datasets using fixed-point arithmetic, then generate Cryptographic artifacts (Shamir shares or Paillier cipher texts) on-premises.
3) Secure Computation Rounds: The Coordinator or chest rates protocol execution. Aggregations use homomor- phic addition of ciphertexts, while complex analytics require multiple SMPC rounds exchanging polynomial shares.
4) Result Reconstruction and Release: Final aggregates are reconstructed using secure protocols (with optional Laplace noise for differential privacy) and transmitted over TLS-encrypted channels to authorized participants.
5) Visualization and Compliance: Participants access interactive dashboards for result analysis and all events are logged for compliance review.

C. Deployment and Design Insights

All services are containerized using Docker and Kubernetes. TLS 1.3 secures external communications. Performance is optimized through protocol batching, constant-time comparisons to mitigate timing side-channels, and bounded coefficient ranges. Fixed-point arithmetic with 16-bit precision ensures accurate handling of real-valued data. The deployment revealed that hybrid security (HE for simple operations ,SMPC for complex ones) significantly optimizes performance while maintaining strong guarantees.

D. Supported Analytics

Table III summarizes the eighteen analytical tasks supported across six domains. Basic statistical operations use hybrid security, while regression, survival analysis, and machine learning tasks require full SMPC due to their iterative nature.

TABLE III: Catalog of Supported Secure Analytics Operations

Category	Computation	Security	TypicalUseCase
Statistical	Sum,Mean,Variance	Hybrid	Descriptive metrics
Statistical	Correlation	Hybrid	Feature association
Statistical	Linear Regression	SMPC	Risk modeling
Survival	Kaplan–Meier	SMPC	Outcome analysis
ML	FederatedLogistic	SMPC	Classification
ML	Federated Random Forest	P	Ensemble modeling
ML	Anomaly Detection	SMPC	Outlier screening
Healthcare	Cohort Analysis	SMPC	Trialcohort selection
Healthcare	Drug Safety	SMPC	ADR detection
Epidemiology	Surveillance	SMPC	Population trends
Genomics	Secure GWAS	Hybrid	SNP association
Genomics	Pharmacogenomics	Hybrid	Drug–gene effects

Note: Hybrid security uses homomorphic encryption (HE) for additive ag-gregations with SMPC fallback. Pure SMPC applies to operations requiringcomplex multi-party interactions.

V. SECURITY ANALYSIS

This section examines the platform's security properties from cryptographic, operational, and regulatory perspectives.

A. Threat Model and Adversary Assumptions

We adopt a semi-honest (honest-but-curious) adversary model, which is appropriate for scenarios involving regulated institutions that are legally and ethically bound to execute the protocol correctly but may attempt passive information leakage. The adversary is assumed to correctly execute the protocol but attempts to infer information from observed messages. We assume the adversary cannot compromise the Coordinator node, corrupt more than t parties simultaneously, or break underlying cryptographic primitives. Defending against malicious adversaries (who arbitrarily deviate from the protocols) is planned for future releases, though it imposes significant computational overhead (≈ 2 − 5×).

B. Formal Security Properties

Under the semi-honest model, our SMPC protocol satisfies the standard simulation-based security definition. Key security guarantees include:

IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 11, November 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1211.14

- **Data Confidentiality:** Individual records remain en- crypted or secret-shared throughout computation.
- **Input Privacy:** No party learns information about others' inputs beyond what is logically deducible from the final aggregate output and their own input.
- **Threshold Security:** Any coalition of *t*or fewer par-ties gains no information about the underlying secrets (information- theoretic security for Shamir sharing with $t = n - 1$). We employ Shamir's (t,n)-threshold secret sharing over $F_p(p \approx 2^{256})$ for SMPC and Paillier HE (2048-bit keys) for additive aggregations. Practical instantiation uses16-bit fixed point precision, balancing accuracy with computational speed, and **bounded polynomial coefficients** ($[0, 10^6]$) to actively prevent numerical overflow during Shamir reconstruction. These engineering choices maintain provable security while achieving practical performance.

C. Attack Vectors and Counter measures

- Collusion Attacks: Mitigated by Shamir's information- theoretic security; $n \geq 3$ with$t = n-1$ is recommended, ensuring unanimous consent for result reconstruction.
- Statistical Inference Attacks: Countermeasures include optional Differential Privacy (Laplace/Gaussian mecha- nism with configurable $\varepsilon \in [0.1, 10]$), query rate limit- ing, audit logging, and minimum aggregation thresholds ($k \geq 10$).
- Side-Channel Attacks: Implementation vulnerabilities are mitigated by using constant-time comparison oper- ations, fixed-size message padding to 1024-byte bound- aries, and memory-hard operations.
- Network-Level Attacks: Man-in-the-middle and eaves- dropping are mitigated through TLS 1.3 with perfect forward secrecy.

D. Compliance with Healthcare Regulations

HIPAA Security Rule Alignment: The platform aligns with all three HIPAA safeguard categories: RBAC and audit trails for Administrative safeguards; HSM recommendations for Physical safeguards; and AES-256 encryption at rest, TLS 1.3 in transit, and cryptographic integrity controls for Techni- cal safeguards. Data minimization principles are inherently satisfied as only cryptographic shares (never plaintext PHI) are shared, meeting HIPAA's de-identification safe harbor provisions.

GDPR Compliance: The platform supports GDPR principles including Lawfulness, Transparency, Data Minimization (only aggregate outputs are computed), Purpose Limitation, Right to Erasure, and Data Portability. Crucially, cross-border data transfers are eliminated because raw data never leaves institutional boundaries.

VI. EVALUATION AND RESULTS

We implemented and validated the platform through comprehensive testing, simulating three healthcare organizations with independent data holdings. The platform was developed as a full-stack prototype. Testing utilized synthetic healthcare datasets (e.g., blood glucose, cardiovascular metrics) across dataset sizes ranging from 6to1600 samples distributed across three parties. Validation objectives included confirming computational accuracy, verifying system stability under concur- rent access, and ensuring compliance logging met regulatory audit requirements. The platform's web-based interface provides intuitive ac- cess to computation results through interactive dashboards, as illustrated in Figure 2 and Figure 3.

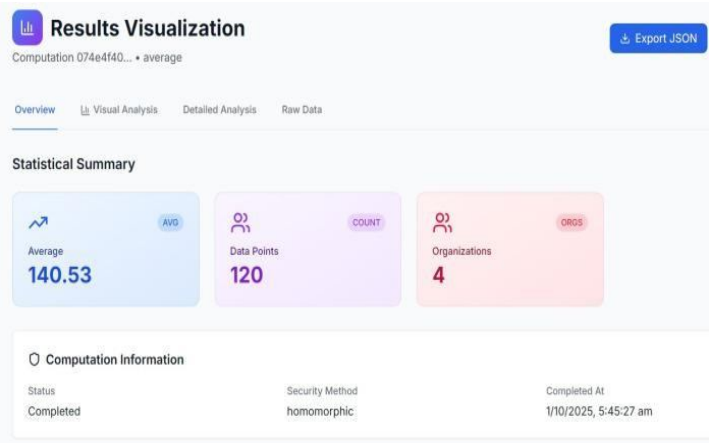

Fig. 2: Overview tab displaying statistical summary (Average=140.53, N=120 data points, 4 organizations) and compu- tation metadata (Status: Completed, Security: Homomorphic)

a) Experimental Setup and Reproducibility:

Experiments used Python3.11(Fast API, NumPy, Paillier cryptosystem)and Node.js 18 (React, Next.js, Chart.js). Fixed-point encoding with 16-bit precision was applied, and Shamir threshold was set to $t=n-1$.Hardware specifications: Inteli 7-9750H (6 cores, 2.6 GHz), 16GB DDR4 RAM. Source code and synthetic datasets are publicly available at GitHub repository.

IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 11, November 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1211.14

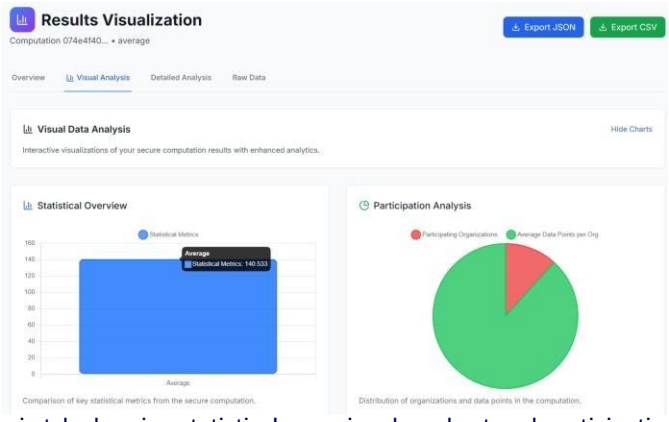

Fig. 3: Visual Analysis tab showing statistical overview bar chart and participation analysis pie chart.

A. Correctness and System Stability

We validated that the security mechanisms preserve analyt- ical accuracy by comparing secure outputs against plaintext baselines. Table IV presents the results. Basic aggregations achieved perfect or near-perfect accuracy (MAE ≤ 10^{-14}). More complex analytics (variance, correlation, regression) introduced minimal error, stemming from fixed-point encoding and matrix operations inherent to SMPC. Critically, all errors remained below **0.02% relative error**, which is acceptablefor clinical decision support. Extended testing confirmed high operationalstability,achieving99.9%uptimepost-deployment with 100% data submission success rates.

TABLE IV: Accuracy Comparison: Securevs. Plaintext Computations

Task	N	MAE	Std.Dev.	Rel. Error (%)	Remarks
Sum	6–1600	0.0000	0.0000	0.000	Perfect match
Mean	6–1600	<10−14	0.0000	0.000	FP precision limit
Count	6–1600	0.0000	0.0000	0.000	Perfect match
Variance	120–1600	2.0×10¯5	1.5×10¯6	0.002	Fixed-point rounding
Correlation	120–1600	1.1×10¯4	8.2×10¯6	0.008	Normalization drift
Regression	120–1600	2.4×10¯4	1.9×10¯5	0.015	Matrix ops precision

Note: MAE denotes Mean Absolute Error between secure and plaintextoutputs; N indicates sample size range. All measurements averaged over 10independent runs.

B. Latency and Scalability

Computation latency scaled approximately **linearly** with sample count, consistent with SMPC protocol communication complexity. Simple aggregations completed in under 0.5 sec- onds for N=1600 samples, while regression required 2.8 seconds due to matrix operations. The linear scaling confirms suitability for batch analytics on institutional-scale datasets.

C. Resource Utilization

System resource monitoring (Table V) showed moderate CPU utilization (25–40%) and peak memory consumption (45–60%) during share reconstruction. The network over-head was symmetric at 8–12 MB per computation round, demonstrating that the platform operates within the resource constraints of typical institutional servers without specialized hardware.

TABLE V: Operational Metrics Observed During Computation

Metric	Observed Value	Context
CPU Utilization	25–40%	During secure computation
Memory Utilization	45–60%	Peak during share reconstruction
Peak Memory	950–1400MB	For N=1600 samples
Network Sent	8–12 MB	Per computation round
Network Received	8–12 MB	Per computation round

Note: Measurements taken on Intel i7-9750H with 16GB RAM across three-party SMPC runs. Network metrics reflect total data exchange per roundincluding shares and protocol overhead.

VII. CONCLUSION AND FUTURE WORK

A. Conclusion

We have presented a deployable platform for privacy- preservinghealthcareanalyticsthat integratesSMPC,HE, and DP into a complete system architecture. Validation confirms that cryptographic protections introduce negligible accuracy loss (below 0.02%) while maintaining linear scalability and acceptable resource overhead. By integrating compliance log- ging, access control, and monitoring features aligned with HIPAA and GDPR, this work bridges the gap between cryptographic theory and production healthcare systems. The open-source implementation provides a foundation for multi- institutional collaboration without compromising patient privacy.

B. Future Work

Performance for extremely large datasets (beyond tens of thousands of samples) remains a limitation due to cryptographic overhead. Furthermore, our current implementation assumes only semi-honest adversaries. Future work will address these gaps by exploring: (1) hardware acceleration using GPUs and Trusted Execution Environments (TEEs); (2) malicious-secure protocols with practical efficiency; (3) native FHIR/HL7 adapters for seamless clinical system integration; and (4) extended federated learning support for iterative model training.

ACKNOWLEDGMENTS

This work was conducted at K S Institute of Technology under the guidance of the Department of Computer Science and Engineering. The authors thank their faculty advisors for valuable feedback and guidance throughout the project development.

REFERENCES

1. Y.Lindell and B.Pinkas,“ Secure protocols for privacy-preserving data mining,” in Annual International Cryptology Conference, 2009.
2. A.Azaria, A.Ekblaw, T.Vieira, and A.Lippman, “Medrec: Using block chain for medical data access and permission management,” International Conference on Open and Big Data, 2016.
3. Q.Xia, E.B.Sifah, A.Smahi, S.Amofa, and X.Zhang, “Bbds: Block chain-based data sharing for electronic medical records,” in In-formation,2017.
4. Q.Xia, E.B.Sifah, K.O.Asamoah, J.Gao, X.Du, and M.Guizani,“ Medshare: Trust-less medical data sharing among cloud service providers via blockchain,” IEEE Access, 2017.
5. K.Fan, S.Wang, Y.Ren, H.Li, and Y.Yang, “Medblock: Efficient and secure medical data sharing via block chain,” Journal of Medical Systems,2018.
6. A.Zhang and X.Lin,“Towards secure and privacy-preserving datasharing in e-health systems via consortium block chain,” Journal of Medical Systems, 2018.
7. W.Dongand X.Lin,“Smpc for secure patient risks ratification,” Computers in Biology and Medicine,2020.
8. M.Keller,“Mp-spdz: Versatile frame work for secure computations, ”ACM Transactions on Privacy and Security,2020.
9. K.Sahinbas and F.O.Catak,“Smpciniot-based health care systems,” Sensors,2021.
10. R.Patel and U.Rao,“Smpc for cross-institutional data sharing,”Journal of Medical Systems, 2024.
11. M.vonMaltitz and T.Schneider,“Mpc in patient data analysis,” Journalof Biomedical Informatics, 2024.
12. K.Sunitha and M.Prasad, “Pricollab: Privacy-preserving collaboration among hospitals,” in International Conference on Data Science and Engineering,2024.
13. A.Tawfik and S.Shah,“Pricollab analysis: Smpc and block chain forehr analytics,”in IEEE International Conference on BigData, 2025.
14. A.Shamir,“How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.
15. P.Paillier, “Public-key crypto systems based on composite degree residuosity classes,” in EUROCRYPT. Springer, 1999, pp. 223–238.
16. C.D work, F.Mc Sherry, K.Nissim, and A.Smith,“Calibratingnoiseto sensitivity in private data analysis,” in Theory of Cryptography Conference (TCC).Springer, 2006, pp. 265–284.
17. C.Gentry,“Fully homomorphic encryption using ideal lattices,” in STOC,2009,pp.169–178.
18. K.Bonawitz, V.Ivanov, B.Kreuter, A.Marcedone,H.B.McMahan, S.Patel, D.Ramage, K.Segal, and K.Seth, “Practical secure aggregation for privacy-preserving machine learning,” in ACM SIGSAC Conferenceon Computer and Communications Security (CCS), 2017, pp. 1175–1191.
19. H.B.Mc Mahan, E.Moore, D.Ramage, S.Hampson, and B.A.y.Arcas,“Communication efficient learning of deep networks from decentralized data,” in AISTATS, 2017.
20. L.Jentsch and J.Mu¨ller, “Secure imputation of missing clinical data using smpc,” Journal of Biomedical Informatics, 2024.
21. H.Jin, Y.Luo, P.Li, and J.Mathew, “A review of secure and privacy-preserving medical data sharing,” IEEE Access,vol.7,pp.61 656–61 669,2019.