Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 9, pp 10-19, September-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.309002
Available Online at https://www.jaiet.com

A Technique for Privacy-Preservation in Ubiquitous Healthcare Monitoring

[1]Chigozi Wali, [2]Onate Taylor, [3]Victor Emmah

[1,2,3]Department of Computer Science, Rivers State University, Port Harcourt, Nigeria
E-mail: [1]wali.chigozi@rsu.edu.ng, [2]onate.taylor@ust.edu.ng, [3]victor.emmah@ust.edu.ng

Abstract: Ubiquitous healthcare monitoring systems generate continuous streams of sensitive patient data from wearable sensors, mobile devices, and Internet of Medical Things environments, but existing privacy approaches often protect isolated stages of the data lifecycle while leaving analytical processing, adaptive parameter selection, and patient transparency insufficiently addressed. This paper developed a privacy-preserving model for ubiquitous healthcare monitoring systems by integrating sensitivity-guided data masking, adaptive differential privacy, unified lifecycle policy enforcement, and a Flask-based privacy transparency dashboard. The model classified health attributes as highly sensitive, moderately sensitive, or routine, masked attributes whose disclosure risk met the selected threshold, and applied context-aware differential privacy using epsilon values of 0.5 for highly sensitive attributes, 3.0 for moderately sensitive attributes, and 2.0 for routine attributes. A policy engine coordinated protection across collection, transmission, storage, and analysis stages, while the dashboard presented protection status, sensitivity summaries, privacy metrics, policy settings, and lifecycle audit records. The system was implemented in Python and evaluated using three public healthcare datasets: Diabetes Health, Heart Disease, and Physical Activity. Results showed that the proposed model achieved 100.00% re-identification resistance for Diabetes Health, 98.89% for Heart Disease, and 100.00% for Physical Activity, exceeding the 95% privacy target across all datasets. Analytical accuracy retention was 95.03%, 90.52%, and 93.88%, respectively, while relative mean absolute error remained below 10% for all datasets. Processing time stayed below two seconds per 1,000 records and peak memory consumption remained far below the 4 GB threshold. The findings demonstrate that combining data masking, adaptive differential privacy, policy enforcement, and dashboard transparency can provide strong privacy protection while preserving useful analytical value for healthcare monitoring data.

Keywords: Ubiquitous Healthcare Monitoring, Internet of Medical Things, Data Masking, Adaptive Differential Privacy, Privacy Policy Engine, Privacy Transparency Dashboard, Re-Identification Resistance.

I. INTRODUCTION

Ubiquitous healthcare monitoring has moved from hospital-based observation to continuous sensing through wearable devices, mobile applications, and Internet of Medical Things (IoMT) platforms. Earlier clinical monitoring required patients to be physically present for vital-sign measurement and medical data collection [1]. Wearable and IoMT devices later made remote monitoring possible by collecting heart rate, blood pressure, glucose, electrocardiogram, and activity data outside clinical settings [2]. Recent systems increasingly combine these data streams with artificial intelligence and machine learning for prediction, anomaly detection, and personalised health support [3]. This shift has improved the reach of healthcare monitoring, but it has also increased the amount of sensitive data exposed across collection, transmission, storage, and analysis.

Privacy preservation is therefore a practical requirement for healthcare providers, patients, researchers, and regulators. Privacy-preserving techniques allow health data to be collected and analysed while reducing exposure of sensitive patient information to unauthorised parties. Blockchain-based systems, for example, have reported 95% success rates in preventing unauthorised access while maintaining data utility [4]. Privacy controls and measurable evaluation metrics can also support compliance with HIPAA, GDPR, and emerging data localisation requirements [5]. For collaborative research, federated learning can reduce the need to transfer raw patient records, with reported reductions of up to 90% compared with centralised alternatives [6]. Patient-facing privacy is also important because many users remain unaware of how wearable health data may be shared or sold outside HIPAA protection [7].

Efforts to address privacy preservation in healthcare monitoring systems have produced several solution categories.

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 9, pp 10-19, September-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.309002
Available Online at https://www.jaiet.com

Traditional encryption schemes protect data at rest and in transit through symmetric and asymmetric cryptographic algorithms, providing confidentiality guarantees but requiring decryption for computational operations on the data [8]. Differential privacy mechanisms inject calibrated noise into health data or query responses, offering mathematical privacy guarantees with bounded information leakage while enabling statistical analysis without exposing individual records [9]. Blockchain-based approaches provide decentralised data management with immutable audit trails and fine-grained access control, with recent implementations achieving throughput of 1100 requests per second and response times of 125 milliseconds for healthcare IoT environments [4]. Federated learning frameworks enable collaborative model training across distributed health monitoring devices without centralising raw patient data, with privacy-preserving federated analytics demonstrating model performance within 5-10% of centralised baselines [10].

Despite these advances, existing solutions still leave important privacy issues unresolved. Conventional encryption protects data at rest and in transit, but sensitive records are often decrypted before analysis, creating exposure during processing [8]. Differential privacy provides formal protection, but many implementations rely on fixed privacy parameters that may over-protect routine data or under-protect sensitive measurements [9]. Privacy-preserving techniques are also often implemented as separate mechanisms, which can weaken protection across the data lifecycle [10]. In addition, many systems give patients limited visibility into how their health data are protected or used [7]. These limitations motivate an integrated privacy-preserving model that combines data masking, adaptive differential privacy, lifecycle policy enforcement, and dashboard-based transparency for ubiquitous healthcare monitoring.

This study develops a privacy-preserving model for ubiquitous healthcare monitoring systems. The model integrates a data masking module for sensitive health attributes, an adaptive differential privacy mechanism for sensitivity-based noise calibration, a policy engine for lifecycle enforcement, and a Flask-based transparency dashboard for presenting privacy status and audit information. The model is evaluated using re-identification resistance, analytical accuracy retention, relative mean absolute error, processing time, memory consumption, and dashboard functionality.

The study focuses on software-based protection for numerical health monitoring data, including vital signs, activity metrics, and physiological measurements from public datasets. It evaluates privacy effectiveness through re-identification resistance, utility through analytical accuracy retention, computational feasibility through processing time and memory use, and transparency through dashboard functionality. The work uses simulated ubiquitous monitoring environments rather than live clinical deployment or real patient data collection.

II. RELATED WORKS

This study is grounded in Privacy-Preserving Healthcare Monitoring Theory, Differential Privacy Theory, and Information-Theoretic Security. Privacy-Preserving Healthcare Monitoring Theory posits that sensitive health data can be collected, transmitted, analysed, and stored throughout the monitoring lifecycle while maintaining mathematical privacy guarantees that prevent unauthorised identification or information leakage [3]. The theory comprises data protection mechanisms, privacy-utility preservation, and lifecycle-consistent protection across all data handling stages [10]. Differential Privacy Theory provides the mathematical basis for bounded information leakage through epsilon and delta parameters, ensuring that computational outputs reveal statistically indistinguishable information whether an individual's data is included or excluded from a dataset [9]. Information-Theoretic Security extends cryptographic protection to privacy-preserving computation, with homomorphic encryption schemes enabling computation on protected health values without revealing plaintext beyond predetermined parameters [11].

Data masking and anonymisation techniques provide an important foundation for privacy-preserving healthcare systems. Data masking protects sensitive health attributes through substitution, suppression, or generalisation transformations that preserve data format and statistical properties while preventing identification of individual patients [8]. Anonymisation techniques such as k-anonymity, l-diversity, and t-closeness provide group-based protection by ensuring that individual records are not easily distinguishable from other records. However, anonymisation methods are limited in streaming health monitoring contexts because multidimensional anonymisation is difficult to apply to real-time data streams that require immediate processing, and stricter privacy parameters can produce substantial information loss in healthcare analytics [9].

Differential privacy has also been widely applied to healthcare analytics because it provides formal privacy guarantees through calibrated noise injection. Mudassar et al. [9] applied Laplace and Gaussian differential privacy mechanisms to healthcare datasets and showed that noise injection can preserve

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 9, pp 10-19, September-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.309002
Available Online at https://www.jaiet.com

data utility while limiting disclosure risk. Laplace mechanisms are suitable for discrete counting queries, while Gaussian mechanisms are useful for high-dimensional continuous health measurements. However, differential privacy for continuous health monitoring faces challenges because physiological streams may contain temporal correlations, repeated queries can exhaust the privacy budget, and high-dimensional health features may require larger epsilon values to preserve utility, thereby weakening privacy guarantees [5].

Blockchain-based privacy protection provides decentralised data management, immutable audit trails, distributed trust, and fine-grained access control through smart contracts. Aboshosha et al. [4] developed a blockchain-driven lightweight hashing system for healthcare IoT environments and reported 1100 requests per second throughput, 125-millisecond response time, 0.3-second average block creation time, and 78-88% maintained efficiency across increasing workloads. These results show the value of blockchain for auditability and distributed access control in health monitoring systems. However, blockchain approaches still face storage overhead, transaction latency, scalability concerns, and limited suitability for emergency scenarios requiring sub-second response [9].

Federated learning, homomorphic encryption, and secure multiparty computation provide additional privacy-preserving approaches for distributed healthcare analytics. Federated learning enables collaborative model training without centralising raw patient data, supporting multi-institutional health analytics without direct record pooling [6]. It nevertheless remains vulnerable to data heterogeneity, communication overhead, poisoning attacks, and privacy leakage from model updates [12]. Homomorphic encryption enables computation over encrypted health data, but CKKS-based implementations may consume much more processing time than plaintext equivalents and may exceed the memory capacity of low-resource edge devices [13]. Secure multiparty computation supports collaborative patient data evaluation without revealing local records [14]. Practical deployment still requires cryptographic expertise, institutional coordination, and additional infrastructure [15].

Data sensitivity and lifecycle policy enforcement are central to privacy-preserving ubiquitous healthcare monitoring. Health data include highly sensitive diagnostic indicators, moderately sensitive physiological measurements, demographic attributes, and routine activity metrics, and these categories require different protection strengths. Treating all attributes with a single privacy setting may either degrade utility for routine data or under-protect sensitive measurements. Lifecycle-based privacy protection also remains important because health data move through collection, transmission, storage, analysis, and archival stages. Fragmented protection mechanisms can create exploitable gaps at transition points, while unified policy enforcement can coordinate masking, encryption verification, storage integrity, and analysis-stage privacy controls across the lifecycle [10].

Patient-facing transparency is another major concern in existing privacy-preserving healthcare systems. Brückner et al. [16] showed that user-driven consent and transparency dashboards can increase trust and engagement in digital health platforms, while Sifaoui and Eastin [7] highlighted that many consumers remain unaware of how wearable health data may be collected, shared, or sold outside HIPAA protection. Privacy evaluation literature also shows the need for measurable privacy and utility metrics, including re-identification risk, analytical accuracy retention, mean absolute error, processing time, memory consumption, and usability-oriented transparency assessment [17].

The reviewed literature reveals four limitations that guide this study: exposure during analytical processing [8], static privacy parameters [9], fragmented lifecycle protection [10], and limited patient-facing transparency [16]. These limitations necessitate an integrated model that combines masking, adaptive differential privacy, unified policy enforcement, and dashboard-based transparency within one healthcare monitoring workflow.

III. METHODOLOGY

3.1 Research Design

This study adopted Design Science Research (DSR) as the overarching methodology because it provides systematic procedures for developing novel artefacts, implementing computational systems, and empirically validating practical solutions through rigorous evaluation [18]. The DSR approach was appropriate because the study required controlled evaluation of datasets, privacy parameters, and performance metrics while measuring the effect of integrated privacy mechanisms on protection effectiveness and data utility [19]. The research followed the DSR process of problem identification, objective definition, artefact design and development, demonstration, evaluation, and communication. In this study, the process began with literature-based identification of privacy requirements in ubiquitous healthcare monitoring, then proceeded to model design, Python-based implementation, evaluation on public health datasets, and documentation through the privacy

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 9, pp 10-19, September-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.309002
Available Online at https://www.jaiet.com

transparency dashboard. Object-Oriented Design (OOD) was used as the software design methodology because the system comprises four functionally distinct components: the data masking module, adaptive differential privacy mechanism, unified privacy policy engine, and transparency dashboard [20]. The system adopted a modular layered architectural pattern in which the four privacy components were organised into processing layers with unidirectional data flow [21]. This structure supported separation of concerns across data masking, adaptive noise injection, policy coordination, and transparency visualisation.

3.2 System Analysis and Architecture

The baseline system analysed in this study was a blockchain-driven approach for health monitoring. It used symmetric encryption with lightweight hash functions for resource-constrained wearable devices, followed by blockchain-based distributed storage for immutable audit trails and decentralised access control. The baseline reported 1100 requests per second, 125-millisecond response time for 5500 operations, 0.3-second average block creation time, and 78-88% efficiency across increasing workloads [4]. These results demonstrate the value of blockchain for tamper-evident storage and distributed trust management. However, additional mechanisms are required for analysis-stage privacy, adaptive protection, lifecycle coordination, and patient visibility.

The proposed model is organised as the layered architecture shown in Figure 1. Health monitoring data enter through the data acquisition layer and pass to the data masking layer, where sensitive attributes are transformed while retaining their analytical format. The masked attributes are encrypted in the security layer and stored as encrypted payloads in the immutable storage layer. When records are retrieved, the adaptive privacy layer applies context-sensitive noise injection before protected analysis is performed in the computational layer. The presentation layer then displays analytical results together with privacy transparency information. The system is designed for deployment on standard computing hardware with 8 GB RAM and is intended for healthcare providers, patients, and data analysts working with privacy-preserving monitoring data.

3.3 Component and Functional Design

The proposed system translates the architecture into six implementable components. The SensitivityProfileBuilder assigns disclosure risk scores and maps attributes to sensitivity tiers. The AttributeMaskingService applies distribution-aware masking to attributes whose risk score meets the threshold. The PrivacyBudgetAllocator selects epsilon values for analytical queries. The LifecyclePolicyLedger records collection, transmission, storage, and analysis enforcement events. The UbiHealthPrivacyWorkflow coordinates dataset registration, attribute profiling, protected analysis, evaluation, and reporting, while the TransparencyDashboardService converts metrics, policy settings, and audit records into stakeholder-facing views.

The functional requirements were data masking, adaptive differential privacy, unified policy enforcement, and privacy transparency. The non-functional requirements were re-identification resistance above 95%, analytical accuracy retention above 90%, processing time below two seconds per 1,000 records, reproducibility through fixed random seeds, and execution on standard computing hardware.

Algorithm 1:	**Integrated Privacy-Preserving Pipeline**
Input	health dataset, attribute schema, masking threshold, policy rules, epsilon tiers, analytical queries
Output	protected data, protected query results, privacy metrics, utility metrics, audit trail, dashboard outputs
1	Load the health dataset and remove records with missing values
2	Split the cleaned dataset into training and evaluation portions using a 70:30 split.
3	Classify attributes as highly sensitive, moderately sensitive, or routine using predefined sensitivity rules
4	Compute disclosure risk scores and identify attributes meeting the masking threshold
5	Apply format-preserving masking to protected attributes while retaining data structure for analysis
6	Enforce lifecycle rules for collection, transmission, storage, and analysis
7	Select the query epsilon value according to the relevant sensitivity tier
8	Apply adaptive differential privacy to protected analytical query outputs
9	Compare protected and unprotected query outputs to compute utility and error metrics.
10	Simulate linkage attacks to compute re-identification resistance
11	Record policy audit events and export dashboard reports, tables, figures, and JSON outputs

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 9, pp 10-19, September-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.309002
Available Online at https://www.jaiet.com

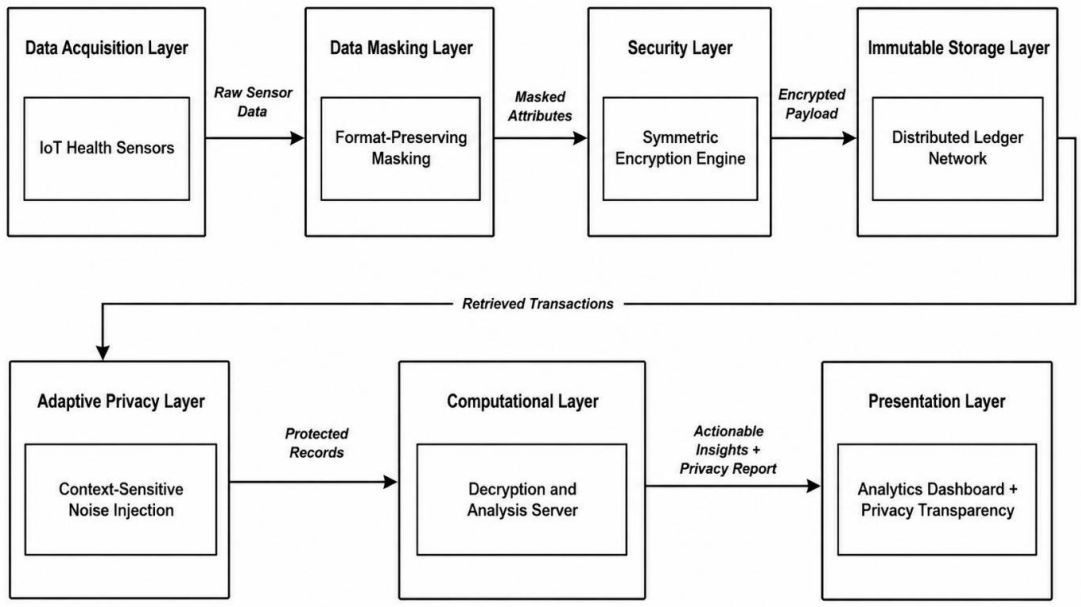

Figure 1: Architecture of the Proposed System

3.4 Implementation, Datasets, and Preprocessing

The model was implemented in Python 3.10.12 because the required privacy and web libraries are available for Python and because Python is widely used in health informatics research [22]. NumPy was used for numerical operations, Pandas for dataset loading and tabulation, diffprivlib for differential privacy mechanisms, scikit-learn for preprocessing and evaluation support, Flask for the web dashboard, SQLite for audit and preference storage, and Matplotlib and Plotly for result visualisation. All development and experiments were carried out on a standard laptop with an Intel Core i7 processor, 8 GB DDR4 RAM, 512 GB SSD, and Windows 11 Pro. No GPU or dedicated cryptographic hardware was used.

Three publicly available health monitoring datasets were obtained from the UCI Machine Learning Repository and Kaggle. They were selected because together they cover different record counts, attribute dimensionalities, sensitivity compositions, and healthcare domains. No original data were collected; all datasets were released under open-access licences permitting academic use.

Table 1: Health Monitoring Datasets for Experimental Evaluation

Dataset	Source	Records	Attributes	Sensitivity Mix	Domain
Diabetes Health Indicators	CDC BRFSS via Kaggle	70,692	21	High: 4, Moderate: 10, Routine: 7	Chronic Disease
Heart Disease	UCI Machine Learning Repository	303	14	High: 3, Moderate: 8, Routine: 3	Cardiovascular
Physical Activity Recognition	UCI Machine Learning Repository	10,299	46	High: 0, Moderate: 15, Routine: 31	Activity Monitoring

Each dataset was loaded from its CSV source using Pandas. Records containing missing values were removed before privacy mechanisms were applied. Attribute sensitivity classifications were assigned by matching column names against predefined category lists, producing a risk score vector for each dataset. No normalisation was applied before masking because the format-preserving transformation operates on values in their original clinical units. A 70:30 split was used for training and evaluation across all experiments, with random state fixed at 42.

3.5 Experimental Design and Evaluation Metrics

The selected experimental configuration used a masking threshold of 0.7, epsilon 0.5 for highly sensitive attributes, epsilon 3.0 for moderately sensitive attributes, epsilon 2.0 for

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 9, pp 10-19, September-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.309002
Available Online at https://www.jaiet.com

routine attributes, and random state 42. The proposed adaptive model was compared against two baselines: no privacy protection and static differential privacy with fixed epsilon 0.5.

Table 2: Experimental Configurations

Configuration	Privacy Mechanism	Purpose
Baseline	No masking, no differential privacy	Unprotected reference for utility comparison
Static Privacy	Fixed epsilon = 0.5 for all attributes	Replicates non-adaptive differential privacy
Proposed Adaptive	Sensitivity-classified masking + adaptive epsilon	Evaluates the integrated model

The evaluation assessed privacy, utility, efficiency, and transparency. Re-identification resistance was measured as 1 - (successful linkages / total linkage attempts), with a target above 95%. Analytical accuracy retention was measured by comparing protected and unprotected mean, variance, range, and correlation query outputs, with a target above 90%. Relative mean absolute error measured normalised analytical distortion, with a target below 10%. Processing time was measured per 1,000 records, with a target below two seconds. Peak memory consumption was measured during pipeline execution, with a target below 4 GB. Dashboard functionality was assessed through implementation of protection status indicators, dataset sensitivity summaries, privacy evaluation results, lifecycle audit records, policy configuration views, and report outputs.

3.6 Ethical Considerations

This study used only publicly available health monitoring datasets from the UCI Machine Learning Repository and Kaggle. The datasets were released under open-access licences permitting academic use, and no primary data collection or direct interaction with human participants was conducted. All datasets were de-identified before public release. Reproducibility was supported through open-source libraries, fixed random seeds, documented privacy parameters, and documented sensitivity classifications.

IV. RESULTS & DISCUSSION

This section presents the results obtained from the selected adaptive configuration. Each public dataset was loaded, cleaned, split into 70:30 training and evaluation portions using random state 42, classified by sensitivity, masked where the risk score met the 0.7 threshold, processed through adaptive differential privacy, and compared against unprotected and static differential privacy outputs. Results are reported using sensitivity classification, privacy resistance, utility retention, query error, computational efficiency, lifecycle policy enforcement, and dashboard transparency evidence.

Table 3: Sensitivity Classification Summary

Dataset	Highly Sensitive	Moderately Sensitive	Routine	Protected Attributes
Diabetes Health	4	10	7	14
Heart Disease	3	8	3	11
Physical Activity	0	15	31	15

The sensitivity classification in Table 3 confirms that the model assigned risk levels according to the sensitivity structure defined in the methodology. With the masking threshold set at 0.7, highly sensitive and moderately sensitive attributes were protected, while routine attributes were left unmasked where appropriate. This supports the sensitivity-aware design of the model because diagnostic, physiological, demographic, and sensor-derived attributes were not treated as if they carried the same disclosure risk.

Table 4: Re-identification Resistance and Utility Results

Dataset	Baseline Resistance (%)	Static DP Resistance (%)	Adaptive Resistance (%)	Accuracy Retention (%)	Rel. MAE (%)
Diabetes Health	34.60	34.80	100.00	95.03	4.97
Heart Disease	0.00	0.00	98.89	90.52	9.48
Physical Activity	0.00	0.00	100.00	93.88	6.12

Table 4 shows that the proposed adaptive model exceeded the 95% re-identification resistance target across all datasets. Diabetes Health and Physical Activity achieved 100.00% resistance, while Heart Disease achieved 98.89%. The unprotected and static differential privacy baselines produced substantially weaker resistance, showing that output noise alone did not sufficiently reduce record-level linkability when sensitive attributes remained linkable. The same table also shows that analytical accuracy retention remained above the 90% target, with relative MAE below 10% across the three datasets. The comparative resistance pattern is visualised in Figure 2.

The Heart Disease result is particularly important because its evaluation set contained only 90 records after preprocessing,

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 9, pp 10-19, September-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.309002
Available Online at https://www.jaiet.com

making it more sensitive to privacy-preserving transformations than the larger Diabetes Health and Physical Activity datasets.

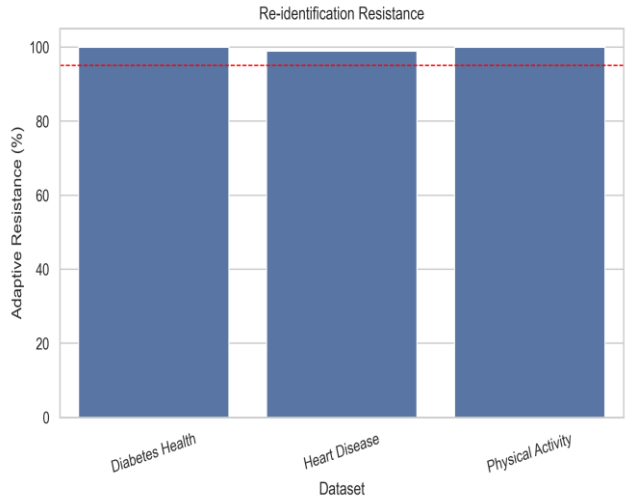

Figure 2: Re-identification resistance performance

Table 5: Overall Performance Against Efficiency Targets

Dataset	Records	Attributes	Total Time (s)	Time per 1000 Records (s)	Peak Memory (MB)
Diabetes Health	21,208	21	0.1540	0.0073	5.46
Heart Disease	90	14	0.0245	0.2722	0.04
Physical Activity	3,090	46	0.0794	0.0257	2.61

Table 5 shows that the model satisfied the computational efficiency requirement. Processing time remained below two seconds per 1,000 records for all datasets, while peak memory consumption remained far below the 4 GB threshold. These results indicate that the model can operate on standard computing hardware without specialised cryptographic hardware or GPU acceleration.

Scalability testing on increasing Diabetes Health record sizes from 100 to 50,000 records also remained within the efficiency target. Time per 1,000 records ranged from 0.3811 seconds at 100 records to 0.0025 seconds at 50,000 records, while peak memory rose only to 5.41 MB. This supports the feasibility of the masking and adaptive privacy pipeline for batch-based healthcare monitoring analysis. The privacy-utility behaviour across epsilon values is shown in Figure 3.

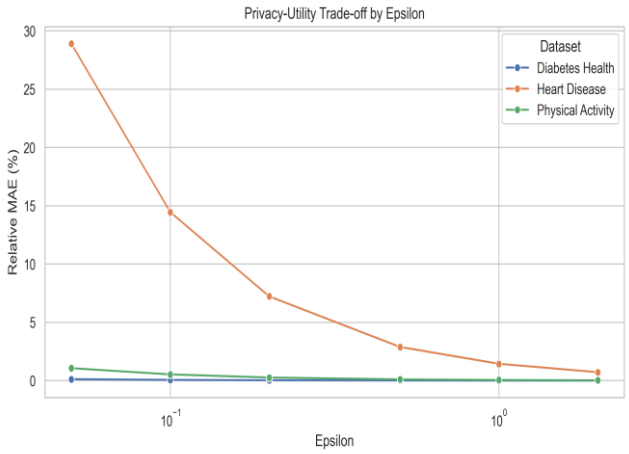

Figure 3: Privacy-utility trade-off

The trade-off confirms that epsilon selection strongly influenced analytical error. Lower epsilon values produced stronger perturbation and higher error, while higher epsilon values reduced error and improved utility. This pattern was most visible in the Heart Disease dataset, where relative MAE reduced from 28.9157% at epsilon 0.05 to 0.7229% at epsilon 2.00. The result supports the selected adaptive configuration because a single static epsilon would not provide the same balance across datasets and sensitivity categories.

Table 6: Mean Absolute Query Error by Statistic

Dataset	Correlation Error	Mean Error	Range Error	Variance Error
Diabetes Health	0.1584	0.0048	5.2502	0.0931
Heart Disease	0.2181	0.4249	5.0601	28.0110
Physical Activity	0.0128	0.0267	0.4582	0.0347

The query-level results in Table 6 show that privacy protection affected statistical operations differently. Mean queries produced low error across datasets, indicating that central tendency was preserved effectively. Variance and range queries produced larger errors, especially for Heart Disease, because these statistics are more sensitive to spread and extreme values in small clinical datasets. Correlation preservation was strongest for Physical Activity, which is important because wearable sensor analytics often depend on relationships among multiple sensor channels.

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 9, pp 10-19, September-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.309002
Available Online at https://www.jaiet.com

Table 7: Privacy Policy Configuration

Stage	Mechanism	Parameters	Conditions
Collection	Sensitivity Masking	threshold = 0.7	risk_score >= 0.7
Transmission	Transport Encryption Verification	AES-256 verification record	always
Storage	Blockchain Immutability Verification	ledger audit verification record	always
Analysis	Adaptive Differential Privacy	epsilon = 0.5 / 3.0 / 2.0	query context

Table 7 shows the lifecycle policy configuration used by the selected adaptive model. The policy engine enforced privacy controls across collection, transmission, storage, and analysis. Collection-stage enforcement applied sensitivity masking, transmission-stage enforcement verified transport encryption, storage-stage enforcement verified ledger audit integrity, and analysis-stage enforcement applied adaptive differential privacy. Audit records were generated for all datasets across the lifecycle stages, providing traceable evidence of policy enforcement. The dashboard interface used to expose these records and metrics is shown in Figure 4.

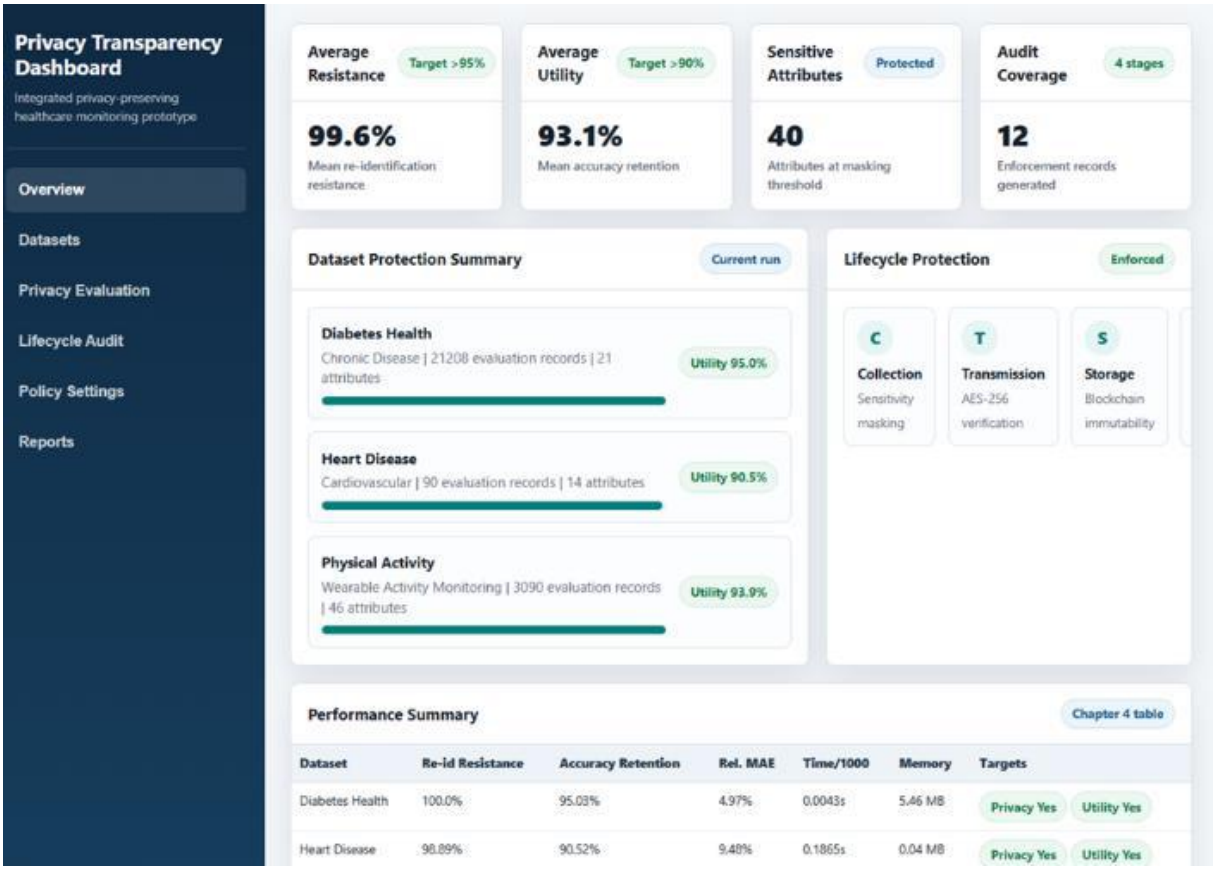

Figure 4: Privacy transparency dashboard overview

The implemented Flask dashboard provided the transparency component of the model. It presented protection status, dataset sensitivity, privacy evaluation results, lifecycle audit records, policy settings, and generated reports through a structured interface. The dashboard converted backend privacy operations into visible privacy indicators for intended patients, healthcare providers, and data analysts.

The results position the proposed model beyond the blockchain-driven baseline and the isolated privacy techniques reviewed earlier. The baseline provides storage integrity and access-control benefits, but it does not by itself protect analysis-stage outputs or explain privacy status to users. The proposed model adds masking before analysis, adaptive differential privacy during query execution, lifecycle policy enforcement,

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 9, pp 10-19, September-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.309002
Available Online at https://www.jaiet.com

and dashboard transparency. Its sensitivity-based epsilon selection also performed better than the static differential privacy baseline, which used one privacy budget for all attributes. Taken together, the results show that the model retained analytical utility while improving re-identification resistance, enforcing lifecycle policies, and making privacy status visible through the dashboard.

V. CONCLUSION

This paper presented a privacy-preserving model for ubiquitous healthcare monitoring systems. The model combines sensitivity-guided data masking, adaptive differential privacy, lifecycle policy enforcement, and dashboard-based transparency. By classifying health attributes according to disclosure risk and assigning privacy parameters by sensitivity level, the model avoids applying a uniform level of protection to diagnostic, physiological, demographic, and routine activity data.

Evaluation on the Diabetes Health, Heart Disease, and Physical Activity datasets showed that the model improved privacy protection while preserving analytical usefulness. Re-identification resistance reached 100.00%, 98.89%, and 100.00%, while analytical accuracy retention remained between 90.52% and 95.03%. Relative MAE stayed below 10% for all datasets, and processing time remained below two seconds per 1,000 records. The results suggest that sensitivity-aware masking and adaptive epsilon selection can support privacy-preserving analysis without prohibitive computational cost on standard hardware.

The policy and dashboard components add a governance layer to the technical privacy mechanisms. The policy engine recorded enforcement actions across collection, transmission, storage, and analysis, while the Flask dashboard displayed protection status, sensitivity summaries, privacy metrics, policy settings, lifecycle audit records, and generated reports. This makes the model relevant not only for privacy-preserving computation, but also for monitoring and communicating how health data are protected.

The study is limited by its use of public secondary datasets and batch-based experimental evaluation rather than real-time deployment with live IoMT streams. Future work should extend the model through operational blockchain or distributed-ledger integration, evaluate real-time wearable and IoMT streams, measure privacy budget consumption and dashboard responsiveness during continuous monitoring, and conduct usability evaluation with patients, clinicians, and healthcare data analysts.

REFERENCES

[1] Pantelopoulos, A., & Bourbakis, N. G. (2010). A survey on wearable sensor-based systems for health monitoring and prognosis. *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, 40(1), 1-12.

[2] Dias, D., & Cunha, J. P. S. (2018). Wearable health devices: Vital sign monitoring, systems and technologies. *Sensors*, 18(8), Article 2414. https://doi.org/10.3390/s18082414

[3] Nabha, R., Laouiti, A., & Samhat, A. E. (2025). Internet of Things-based healthcare systems: An overview of privacy-preserving mechanisms. *Applied Sciences*, 15(7), Article 3629. https://doi.org/10.3390/app15073629

[4] Aboshosha, B. W., Zayed, M. M., Khalifa, H. S., & Ramadan, R. A. (2025). Enhancing Internet of Things security in healthcare using a blockchain-driven lightweight hashing system. *Beni-Suef University Journal of Basic and Applied Sciences*, 14(1), Article 56. https://doi.org/10.1186/s43088-025-00644-8

[5] Shenoy, D., Bhat, R., & Prakasha, K. K. (2025). Exploring privacy mechanisms and metrics in federated learning. *Artificial Intelligence Review*, 58(8), Article 223. https://doi.org/10.1007/s10462-025-11170-5

[6] Haripriya, A. P., Khare, N., & Pandey, V. (2025). Privacy-preserving federated learning for collaborative medical data mining in multi-institutional settings. *Scientific Reports*, 15(1), Article 12482. https://doi.org/10.1038/s41598-025-97565-4

[7] Sifaoui, A., & Eastin, M. S. (2024). "Whispers from the Wrist": Wearable Health Monitoring Devices and Privacy Regulations in the U.S.: The Loopholes, the Challenges, and the Opportunities. *Cryptography*, 8(2), 26.

[8] Irshad, R. R., Sohail, S. S., Hussain, S., Madsen, D. O., Zamani, A. S., Ahmed, A. A. A., Alattab, A. A., Badr, M. M., & Alwayle, I. M. (2023). Towards enhancing security of IoT-enabled healthcare system. *Heliyon*, 9(11), Article e22336. https://doi.org/10.1016/j.heliyon.2023.e22336

[9] Mudassar, B., Tahir, S., Khan, F., Shah, S. A., Shah, S. I., & Abbasi, Q. H. (2024). Privacy-preserving data analytics in Internet of Medical Things. *Future Internet*, 16(11), Article 407. https://doi.org/10.3390/fi16110407

[10] Kalodanis, K., Feretzakis, G., Anastasiou, A., Rizomiliotis, P., Anagnostopoulos, D., & Koumpouros, Y. (2025). A privacy-preserving and attack-aware AI approach for high-risk healthcare systems under the EU AI Act. *Electronics*, 14(7), 1385.

[11] Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2017). Homomorphic encryption for arithmetic of approximate

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 9, pp 10-19, September-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.309002
Available Online at https://www.jaiet.com

numbers. *Advances in Cryptology-ASIACRYPT* 2017, 409-437.

[12] Fang, M., Cao, X., Jia, J., & Gong, N. (2023). Local model poisoning attacks to Byzantine-robust federated learning. *USENIX Security Symposium*, 1605-1622.

[13] Kumar, S., Gupta, R., & Singh, A. (2023). Configurable encryption and decryption architectures for CKKS-based homomorphic encryption. *Sensors*, 23(17), 7389.

[14] Ballhausen, H., Corradini, S., Belka, C., Bogdanov, D., Boldrini, L., Bono, F., Goelz, C., Landry, G., Panza, G., Parodi, K., Talviste, R., Tran, H. E., Gambacorta, M. A., & Marschner, S. (2024). Privacy-friendly evaluation of patient data with secure multiparty computation in a European pilot study. *npj Digital Medicine*, 7(1), Article 275. https://doi.org/10.1038/s41746-024-01293-4

[15] Naresh, V. S., Raju, A. V., & Rao, O. S. (2025). Secure multiparty computation for privacy-preserving machine learning in healthcare: A comprehensive survey. *WIREs Computational Statistics*, e70046.

[16] Brückner, S., Dridi, A., Deshmukh, A., Kirsten, T., Lauber-Rönsberg, A., Riedel, R., Hetmank, S., Welzel, C., & Gilbert, S. (2025). A user-driven consent platform for health data sharing in digital health applications. *npj Digital Medicine*, 8(1), Article 699. https://doi.org/10.1038/s41746-025-02147-3

[17] Kaabachi, B., Despraz, J., Meurers, T., Otte, K., Halilovic, M., Kulynych, B., Prasser, F., & Raisaro, J. L. (2025). A scoping review of privacy and utility metrics in medical synthetic data. *npj Digital Medicine*, 8, 60.

[18] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75-105. https://doi.org/10.2307/25148625

[19] Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302

[20] Booch, G., Rumbaugh, J., & Jacobson, I. (2007). The unified modelling language user guide (2nd ed.). *Addison-Wesley*.

[21] Sommerville, I. (2016). Software engineering (10th ed.). *Pearson*.

[22] Van Rossum, G., & Drake, F. L. (2009). Python 3 reference manual. *CreateSpace*.

Citation of this Article:

Chigozi Wali, Onate Taylor, & Victor Emmah. (2026). A Technique for Privacy-Preservation in Ubiquitous Healthcare Monitoring. *Journal of Artificial Intelligence and Emerging Technologies (JAIET).* 3(9), 10-19. Article DOI: https://doi.org/10.47001/JAIET/2026.309002

***** End of the Article *****