Jagua Publication

Journal of Applied Health Sciences and Medicine, 6(3):32–46, 2026. DOI: 10.58614/jahsm636

Journal of Applied Health Sciences and Medicine

Journal homepage: https://www.jpub.org/journal-details.php?journal-id=39

ISSN (E): 2583-1887
Journal of Applied Health Sciences and Medicine

Research Article

A Federated Epidemiological Modelling Architecture Leveraging Cloud Technology and Blockchain for Cancer Cell Growth Management

Supratim Bhattacharya [1*]

[1] *Techno India University, EM -4/1, Street Number 2, EM Block, Sector V, Bidhannagar, Kolkata, West Bengal 700091, India.*
[*] *Corresponding author: bhattacharya.supratim@gmail.com*

Article Info

Keywords: *Blockchain, Google Cloud Platform, Epidemiological Model, malignant cell growth, Decentralized architecture.*

Received: *27.02.2026;*
Accepted: *14.03.2026;*
Published: *20.03.2026*

Abstract

Cancer growth has a high correlation with the dynamic and complex changing interactions of malignant cells, different treatment responses and human immune systems. It is always difficult to make predictions and deliver timely and accurate prediction while also managing secure clinical data management. This novel study presents a federated architecture that assembles epidemiological modelling (Feedback-based SIR Model) along with cloud computing and blockchain technology. It also applies machine learning to improve the predictive capability of cancer cell growth along with managing clinical records. On top of that the framework applies blockchain technology with off-chain storage using the Inter Planetary File System (IPFS that ensures scalability, security and preserving & managing sensitive clinical records. Experimental assessment demonstrates that the feedback-based SIR model significantly surpasses conventional approaches SIR model in predictive accuracy and that the proposed blockchain – cloud architecture achieves an effective balance between security and system performance, providing a robust and scalable foundation for precision oncology, intelligent decision support and collaborative cancer research.

1. Introduction

Cancer continues to be the most complex and challenging diseases to predict, manage and monitor due to its heterogeneous nature, dynamic evolution, and dependence on multiple biological and environmental factors [1–3]. Accurate modelling of cancer cell growth and relapse is critical for early diagnosis [4–7], treatment optimization, and personalized decision-making. Traditional rule-based and statistical models often struggle to capture the nonlinear dynamics of tumour evolution and the feedback mechanisms between cancer cells, treatment response, and the immune system [4–6].

In current study, epidemiological models, originally designed to study infectious disease dynamics, have gained attention in cancer research due to their capability to capture population- wide transitions between biological states [8–12]. Models such as the Susceptible–Infectious–Recovered (SIR) framework can be effectively adapted to represent healthy cells, malignant proliferative cells, and treated or dormant cancer cells [5, 7]. Recent studies demonstrate that feedback-based extensions of compartmental models significantly enhance the accuracy of cancer growth and recurrence prediction by incorporating treatment resistance, immune suppression, and tumour microenvironment effects [13–15]. These models provide a mathematically grounded framework for simulating cancer progression over time.

Concurrent with recent advances in mathematical modelling, the growing digitization of healthcare has resulted in huge volumes of genomic, clinical and imaging data [16–19]. Cloud computing helps to achieve scalable computational resources to process large datasets

and extract real time analytics by incorporating machine learning driven prediction models for abnormal cell growth analysis and predictive assessment [19–21]. Cloud-native AI frameworks exhibit strong potential in enhancing the precision oncology by incorporating diversified medical records to guide clinical decision-making [22–24]. In certain scenario, Centralized processing and storage of sensitive clinical records raise substantial challenges in connection with security, privacy, integrity as well as regulatory compliance [25–27]. Blockchain technology stood upfront as an acceptable solution to mitigate these challenges by providing immutable, decentralized and transparent data governance mechanisms [28–30]. Recent studies shows that healthcare-oriented blockchain frameworks provide granular access control with secure and reliable data sharing across multiple institutions without any dependency on a centralized authority. Furthermore, the integration of on-chain and off-chain storage systems such as IPFS improves scalability while ensuring data confidentiality.

In spite of these advance technological, previous studies has often focused on either only disease prediction modelling or blockchain-based data security system or cloud-based storage management in isolation [31, 32]. The proposed architecture is an absence comprehensive framework that combine epidemiological cancer modelling with scalable, secure and intelligent data management infrastructure. This study is an end-to-end framework that integrates a feedback-based SIR epidemiological model for cancer cell growth, blockchain-enabled secure clinical data management and cloud-based machine learning analytics [30–32]. The proposed system ensures better cell growth prediction, ensuring a secure and confidential data handling that supports clinical decision-making in cancer cell growth prediction [30–35].

2. Problem Statement

The accelerated involvement related to digital technology in non-communicable diseases like cancer disease has resulted in huge volume of diversified clinical data, including patient records, tumour growth histories and different treatment outcomes. Though cloud platforms enable and points to scalable data storage along with advanced analytics but as a centralized architecture, it poses significant challenges related to data privacy, integrity, security and regulatory compliance. Existing studies show the limitations of capturing disease recurrence behaviour and the natural feedback mechanisms related to cell growth progression. This stays back in optimizing the overall performance and effectiveness in real-world clinical decision-making. Blockchain technology provides decentralized and tamper-resistant data management. But this on-chain data management is inefficient and infeasible when it comes to directly storing large-scale medical data. Moreover, most prior and existing studies mainly focusing on different areas like cancer modelling, secure data storage and predictive analytics as independent components, lacking a unified and comprehensive framework that integrates mathematical modelling with secure and scalable healthcare infrastructures.

Accordingly, it is an essential to develop a unique framework that

1. Accurately models malignant cell growth and relapse applying feedback-based epidemiological models
2. Ensures secure, privacy-protected and reliable management of clinical data and
3. Supports scalable data analytics and prediction using machine learning. To mitigate these challenges, it is essential to employ secured, data-driven and integrated precision oncology systems.

3. Objective

The primary objective of this study is to evaluate and design an integrated framework for secure prediction of cancer cell growth and clinical data management by leveraging epidemiological modelling, blockchain, cloud computing, and machine learning. The specific objectives are as follows:

1. To adapt a feedback-based SIR epidemiological model to represent cancer cell dynamics, including dormancy, proliferation and treatment resistance.
2. To develop a secure clinical data management mechanism using blockchain technology, ensuring data transparency, integrity and granular access control.
3. To employ off-chain storage (IPFS) for scalable and privacy-preserving storage of large clinical datasets, while maintaining blockchain-enabled traceability.
4. To integrate cloud computing infrastructure for scalable and flexible computation and real-time processing of oncological modelling and clinical datasets.

4. Related Work

Recent studies have progressively explored mathematical and computational models [36, 37] to better understand cancer progression and treatment dynamics. In a span of 3 to 4 years, several researchers extended classical compartmental and tumor–immune dynamic models to capture the non-linear behaviours of malignancy such as immune suppression, treatment response, and relapse. Mahlbacher et al and de Pillis et al. demonstrated that feedback-driven population-level tumor growth models significantly improve interpretability and stability compared to solely data-driven approaches [38]. However, while these models offer robust biological insight, they are typically validated under isolated simulation environments and lack integration with secure data management or clinical decision-support infrastructures [39].

In parallel, the adoption of cloud-based analytics [39, 40] and machine learning for cancer prediction has accelerated. Earlier studies reported the use of hybrid ML pipelines deployed on cloud platforms to process large-scale clinical datasets for prognosis and outcome prediction. While these approaches maintain a promising & strong predictive accuracy level, recent surveys pin point challenges related to model reproducibility, interpretability and centralized data governance [41]. Additionally, most cloud-native frameworks based on oncology analytics operate under the assumption of trusted centralized storage, pointing to criticalities around auditability, privacy and regulatory compliance when applied in federated healthcare ecosystems.

To address trust and data security, blockchain-based healthcare frameworks have attracted considerable attention over the last couple of years. Works published within that span propose blockchain-assisted electronic health record (EHR) sharing along with the concept of decentralized identity management and smart contract–based access control. Notably, studies embedding blockchain with off-chain storage

mechanisms such as IPFS exhibit improved scalability by storing only hashes and metadata on-chain while maintaining large clinical data repositories encrypted off-chain. These systems offer strong guarantees for data integrity, access auditing and provenance. However, most blockchain-based healthcare solutions primarily emphasizing on secure data exchange and interoperability, without incorporating predictive disease models or decision-support logic within the system workflow.

More recent studies attempt partial integration of analytical and trust management layers. Blockchain-enabled decision support systems [39–41] proposed in recent studies combine cloud analytics with immutable audit trails, but they typically depend on generic statistical or ML-based predictions [42–45] and do not integrate biologically grounded cancer growth models [46–48]. Additionally, epidemiological modelling embedded with blockchain-based security are often considered as independent components, with limited attention to how the correctness of the model outputs can be verified, audited, and protected against data tampering [49–53].

In summary, although recent studies demonstrate advances in cancer modelling, cloud-based predictive analytics, and blockchain-based healthcare security, these contributions largely remain unaddressed. There is a clear gap in end-to-end frameworks that jointly integrate feedback-aware epidemiological cancer models with cloud-scale analytics and blockchain–IPFS–based trust mechanisms. The present work addresses this gap by integrated cancer growth prediction, secure data management, and trustworthy decision support within a single and scalable architecture, thus advancing the state of the art in precision oncology decision-support systems.

5. System Architecture

5.1. User

From an end-user viewpoint, the system enables secure user registration and authentication, create new data entries, and access their own data through the application interface. From a report viewer perspective, authorized users are able to register and securely authenticate with the system and are permitted to view analytical outputs produced by the DSS without altering the underlying data. From an administrator point of view, the system enables secure user registration and authentication, enables managing and revoking access permissions for different user roles and enables updating or editing data to ensure proper governance, control, and system integrity.

5.2. Data Sources

- Patient clinical data and socio-demographic data.
- Tumour growth datasets in different timeline.

5.3. Overall DSS Framework

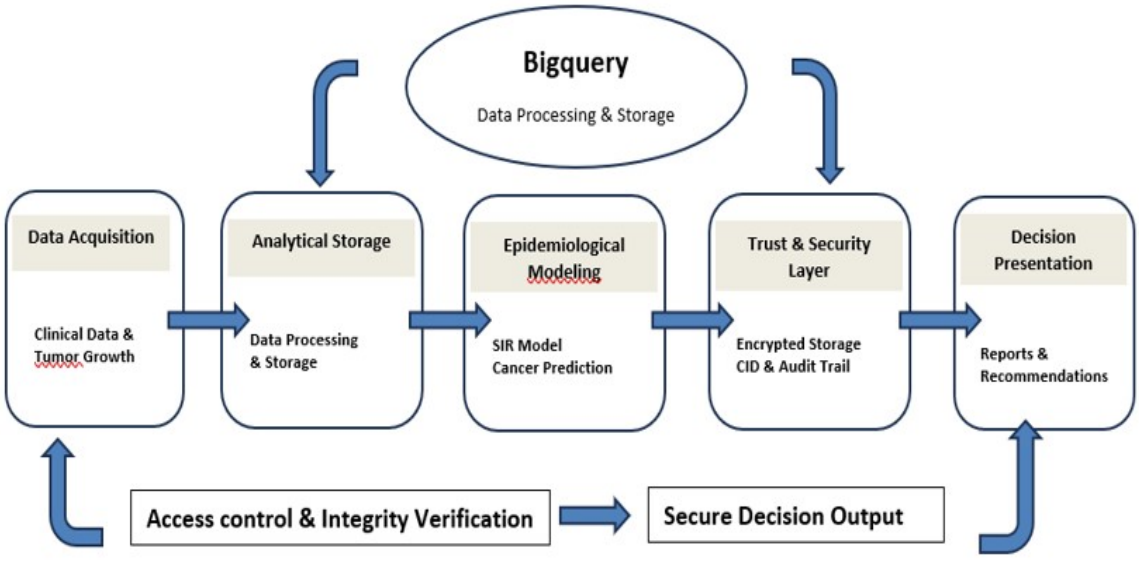


Figure 1: DSS Framework

BigQuery Data Layer

The BigQuery data layer serves as the main analytical storage component of the proposed DSS, providing scalable, high-performance computing of large-scale cancer-related datasets, including anonymized patient records, tumour growth time-series, treatment metadata and simulated epidemiological data. Data are ingested through batch and streaming pipelines and undergo preprocessing steps such as cleaning, normalization and feature extraction data readiness for analytics. Leveraging BigQuery's distributed, serverless architecture, estimation of parameters for the adapted epidemiological model, statistical analysis and parameter estimation for the adapted epidemiological model, with query results directly feeding into the modelling engine to enable dynamic and data-driven cancer growth prediction. Periodic snapshots of critical datasets are used to preserve data integrity and traceability and also outputs of the model are exported from BigQuery. Subsequently, the data are encrypted and stored in IPFS, with the corresponding content identifiers are securely recorded on the blockchain. Thus, the overall process ensures security, verifiability, and auditability, keeping scalable analytics intact.

IPFS-Based Evidence Layer

The proposed DSS model is incorporated with IPFS-based layer to ensure data integrity, traceability, and tamper resistance. This layer acts as a decentralized and immutable storage for critical input datasets as well as model outputs records instead of implementing complex computation process or applying dynamic querying. Snapshots of BigQuery datasets and model outputs are captured, encrypted and stored in the IPFS at prespecified intervals. For each snapshot, a unique ID is being produced which cryptographically checks on time security interference. The unique IDs are stored in the blockchain to create an un-tampered record. During the execution process of the proposed system, data integrity is verified by extracting the corresponding snapshot from IPFS and then comparing its hash with the CID that is already recorded on the blockchain ensuring overall accuracy of outputs that is derived from un-tampered dataset. The system provides a decentralized storage keeping evidence separately from data analysis which helps maintaining privacy and efficiency along with data protection. Its performance increases by applying cloud technology that builds trust and transparency in the decision support system.

Blockchain Trust Layer

In the proposed DSS, blockchain trust layer is a lightweight ledger with tamper-resistant that supports both transparency and accountability. It is not being used for data storage or for computation, rather it stores metadata which acts as IPFS content identifiers or dataset IDs or timestamps or model execution details. Smart contracts are used to enforce predefined access control policies that is capable of verifying access to only authorized users or system components. All the access requests and authorizations are permanently recorded to enable end-to-end auditability. During the execution of the DSS model, the blockchain is used to verify and validate the access and the integrity part by allowing the system to retrieve CIDs and later validate them against the encrypted IPFS snapshots. This ensures that analytical computations and the predictive power of the epidemiological model are derived from authentic, untampered data and if any discrepancies occur then immediate integrity alerts will be triggered. System robustness is being enhanced by segregating the trust management from data analytics and storage. This is done with the help of blockchain layer without significant computational overhead. This avoids storing personal and sensitive medical records on-chain and preserves privacy which clearly signifies how the system performs and where the data comes from. It exemplifies a strong base for a secure Decision Support System by improving trust and confidence in the overall outputs for cancer growth prediction and data management.

6. Methodology

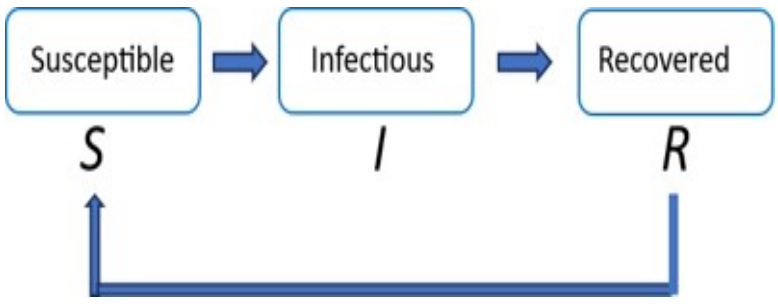
6.1. Data Processing Pipeline

The data processing pipeline transforms diversified cancer disease related datasets into more structured and analytics ready inputs for the proposed Decision Support System (DSS). The process starts with collecting medical records from validated sources with all personal and sensitive information removed or anonymized prior to uploading those datasets in cloud. After ingestion, the data is cleaned, preprocessing, perform normalization and avoid outliers to improve quality and consistency. Subsequently, relevant features including time-based features and demographic features are selected and transformed to support epidemiological modelling. To enable efficient analytical queries and large-scale statistical analysis, the transformed datasets are stored in the BigQuery data layer. The extracted output of the pipeline is directly injected to the epidemiological model. This guarantees that the predictive insights generated by the DSS are based on consistent, high-quality inputs and thereby enhancing the reliability and accuracy of decision outcomes.

6.2. Epidemiological Model Adaptation

The propose epidemiological model, the Feedback – based SIR model represent cancer cell in three different states:

- **S (Susceptible):** Healthy cells prone to mutation.
- **I (Infectious):** Mutated cancerous cells.
- **R (Recovered):** Dormant or treated cells.



In feedback-based SIR model, the recovered cells can be again back to the susceptible state due to like various factors like mutation, regrowth, after treatment effects etc.

Here is how this might happen.

6.3. Biological Interpretation

1. **Residual Cancer Cells:** Over the course of treatment some malignant cells may not be fully eliminated and can remain dormant. Because of environmental or systemic changes like immune system suppression or changes in the tumour microenvironment those

dormant cells can become susceptible again.
2. **Resistance Development:** Malignant cells that initially respond to treatment which may later become resistant and effectively becoming "susceptible" again contributing to the growth or spread of the disease.
3. **Mutations:** Genetic modification or changes in the recovered cells could behave like malignant again, causing them to be treated as in susceptible-like state and may restart the cancer disease progress.
4. **Microenvironment Factors:** Recovered cells can be influenced by nearby blood vessels and tissues which can further act as a cancer cell and can revert to the susceptible state.
5. **Immune System Dynamics:** A weak immune system after recovery, where in some malignant cells remain undetected and later start behaving as active malignant cell and again re-enter to susceptible phase.

The proper percentage of recovered cell feed back to the "susceptible" compartment in a cancer cell growth model depends on the specific biological context and treatment conditions. This proportion varies based on several factors, such as cancer type, effectiveness of treatment, patient's immune system and the overall condition of the tumour.

And his is how these contributions might be measured & quantified:

1. **Treatment Efficacy** (S_1) : Depending of the effectiveness of the treatment very few dormant or resistant cells results in a low percentage ($<5\%$) of recovered cells feed-back to susceptible state, compared to low or partial treatment efficacy where a higher percentage (20%-30%) of recovered cells might return to the susceptible state.
2. **Mutation Rate** (S_2) : Due to the genomic instability in cancer cells new changes may develop even after the treatment or when they seem to be already inactive. The rate of this mutation is based on the recovered cells re-enter the susceptible state, that might range between 10%-20%, depending on the cancer type.
3. **Immune System Effectiveness** (S_3) :A strong and robust immune system can control the modification rate of recovered cell. Depending on the immune this proportion may vary from to about 5%-25%.
4. **Tumour Microenvironment** (S_4) **::** Different contributing factors such as inflammation, blood vessels growth and reactivate dormant malignant cells contributes to 5%-15% of recovered cells becoming susceptible again.
5. **Cancer Type** (S_5) :
    - **Aggressive Cancers:** The feedback could be higher for highly aggressive cancers such as triple-negative breast cancer or glioblastoma, where 20%–40% of recovered cells revert back to the susceptible segment.
    - **Less Aggressive Cancers:** The contribution might be as low as 10% for slow-growing cancers such as prostate cancer.
6. **Relapse and Recurrence Data** (S_6) :
    - Study related to clinical dataset and its corresponding report enlighten the following:
    - The relapse rates for Breast Cancer would be around 20%-30% within next five years.
    - Also the relapse rates for Leukemia might be 10%-50% depending on different malignant subtypes.
    -

The Decision Support System can be modelled using available clinical and socio-demographic dataset implementing Dormancy Activation Rate (DAR), which is derived from empirically observed relapse rates, Mutation Rate (MR), which is estimated from genetic studies and the Immune Suppression Rate (ISR) that Measured from immune profiling.

So, the total susceptible population (S) can be calculated as:

$$S = S_1 + S_2 + S_3 + S_4 + S_5 + S_6$$

6.4. Blockchain-Based Access Control

The blockchain-based access control mechanism, within the proposed Decision Support System (DSS), is designed to ensure transparent and traceable management. User are first checked and authentication by the cloud identity management framework and then access mechanisms are control via smart contracts deployed on the blockchain. These smart contracts use role-based access control mechanism for each user role like clinicians, researchers, and auditors in relation to specific datasets and system functionalities. Each access request is validated against the rules stored in Blockchain. Both allowed and denied access are permanently recorded in an immutable ledger on the blockchain. The proposed system reduces unauthorized data access, enables accountability and enhances trust by decoupling authentication from authorization using Blockchain. It also does this without exposing sensitive clinical records or adding substantial computational overhead.

6.5. Data Integrity Verification

The data integrity verification process ensures that all analysis and decisions in the proposed DDS model output are based on real time data that are not been modified and untampered. At regular time intervals, processed datasets and epidemiological model outputs are extracted from the BigQuery. Later the extracted output is encrypted and stored in Inter Planetary File System (IPFS), where each copy gets a unique identifier. The unique IDs, dataset identifiers and timestamps are permanently stored in on-chain blocks. During the execution of DSS, the system retrieves unique ID extracted from the blockchain and verifies it by comparing the cryptographic hash of the similar fetched data snapshot from IPFS. If any data tampering occurs then verification fails which indicate possible data tampering, that leads to triggering integrity violation alert. This will prevent applying decision making with tampered dataset. The proposed system strongly protects integrity by combining decentralized storage with blockchain verification. It also ensures auditability with easy scalability and preserving the confidentiality of sensitive medical data.

7. Decision Support Workflow

7.1. Algorithmic Implementation

Algorithm 1: End-to-End Secure DSS Framework

Input

- Raw data streams D (sensor data / transactional data / external datasets)
- Decision query Q
- DSS model M

Output

- Verified decision output O
- Immutable audit and integrity proof

Initialization

1. Initialize Google BigQuery dataset BQ
2. Initialize IPFS node IPFS
3. Deploy blockchain smart contract SC
4. Configure GCP IAM and KMS for secure access

Phase I: Data Ingestion and Storage

1. Collect raw data D from data sources
2. Preprocess D (cleaning, normalization, aggregation)
3. Store processed data in BigQuery BQ
4. Assign dataset identifier dataset_id

Phase II: Dataset Snapshot and IPFS Storage

1. Periodically or event-triggered:
2. Export dataset snapshot S from BigQuery
3. Encrypt snapshot S $\rightarrow$ S_enc
4. Upload S_enc to IPFS
5. Receive Content Identifier CID

Phase III: Blockchain Integrity Registration

1. Compute metadata:
    - dataset_id
    - CID
    - timestamp T
2. Invoke smart contract SC store (dataset_id, CID, T)
3. Blockchain records immutable dataset proof

Phase IV: DSS Decision Execution

1. Receive decision query Q
2. Retrieve analytical data from BigQuery
3. Execute DSS model M on retrieved data
4. Generate decision output O

Phase V: Integrity Verification

1. Fetch registered CID from blockchain using dataset_id
2. Retrieve corresponding snapshot S_enc from IPFS
3. Decrypt S_enc $\rightarrow$ S
4. Verify hash(S) matches CID
5. If verification fails:
   Reject decision and raise alert
   Else:
   Approve decision output O

Phase VI: Audit and Logging

1. Record decision metadata:
    - dataset_id

- CID
- decision hash
- timestamp

2. Store audit log on blockchain
3. Return verified decision output O

End Algorithm

Algorithm 2: Blockchain-Based Access Control for DSS

Input

- User request R= ⟨user_id, dataset_id, action⟩
- Smart contract SC
- DSS service DSS

Output

- Access decision A ∈ Grant, Deny
- Immutable access log

Initialization

1. Deploy access control smart contract SC
2. Define user roles R = Admin, Analyst, Clinician, Auditor
3. Map users to roles using GCP IAM
4. Register authorized roles on blockchain

Access Control Procedure

1. Fetch access request R
2. Authenticate user via GCP IAM
3. If authentication fails:
   Deny access and terminate
4. Retrieve user's role r from IAM
5. Query smart contract SC.checkPermission(r, dataset_id, action)
6. If permission = FALSE:
   - Log access denial event on blockchain
   - Set A ← Deny
   - Terminate
7. Else:
   - Grant access to DSS service
   - Log access grant event on blockchain
   - Set A ← Grant

End Algorithm

Algorithm 3: Data Integrity Verification Using IPFS and Blockchain

Input

- Dataset identifier dataset_id
- Content Identifier CID
- IPFS network
- Blockchain smart contract SC

Output

- Integrity status V ∈ Valid, Invalid

Integrity Verification Procedure

1. Fetch registered CID_block from blockchain using dataset_id
2. Obtain encrypted dataset snapshot S_enc from IPFS using CID_block
3. If S_enc retrieval fails:
   Set V ← Invalid
   Raise availability alert
   Terminate
4. Decrypt S_enc → S
5. Compute hash H ← Hash(S)
6. Compare H with CID_block
7. If H = CID_block:
   Set V ← Valid
   Else:
   Set V ← Invalid
   Raise tampering alert

End Algorithm

7.2. DSS Execution Flow

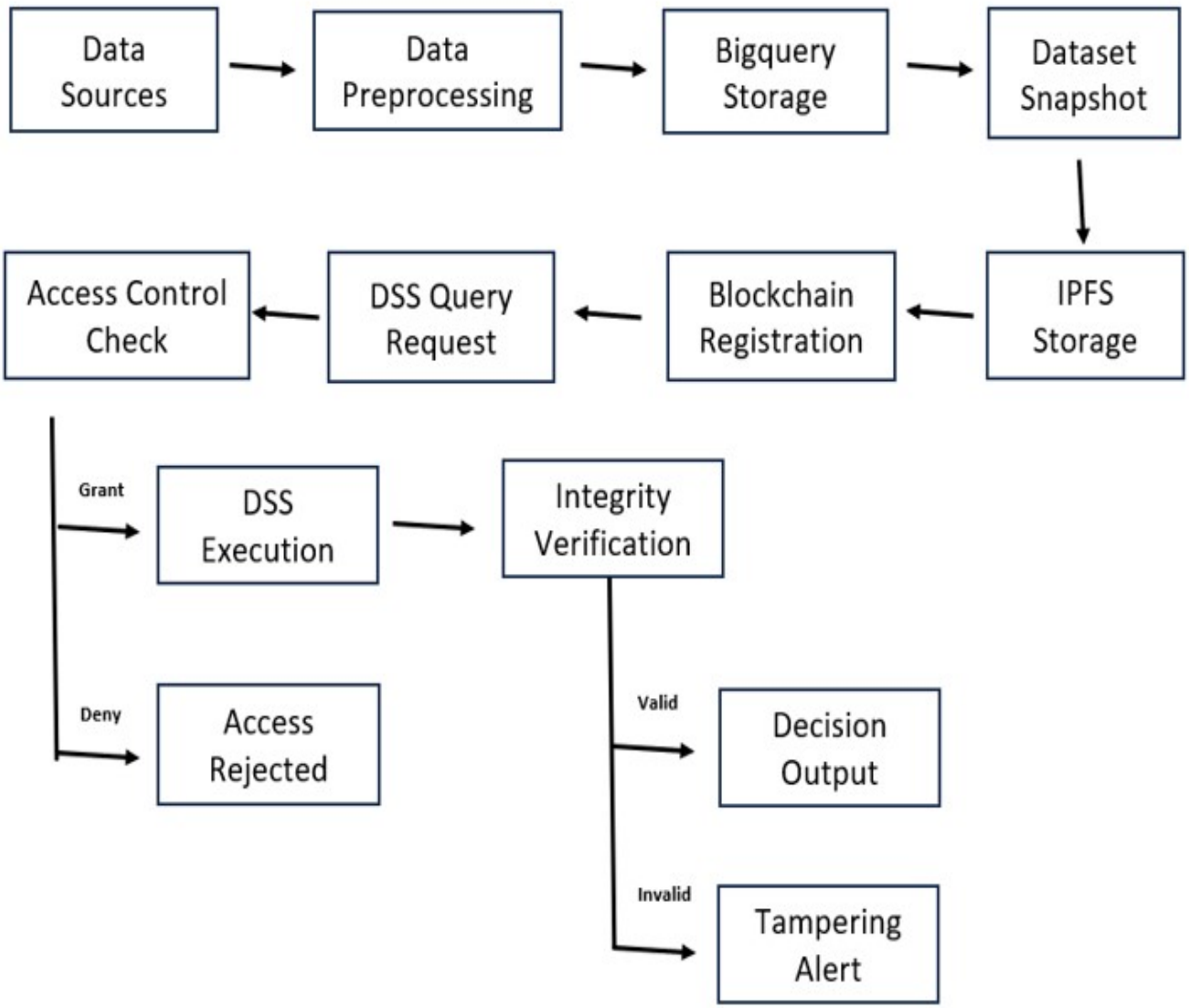


Figure 2: Flowchart – Secure DSS with Bigquery, IPFS, and Blockchain

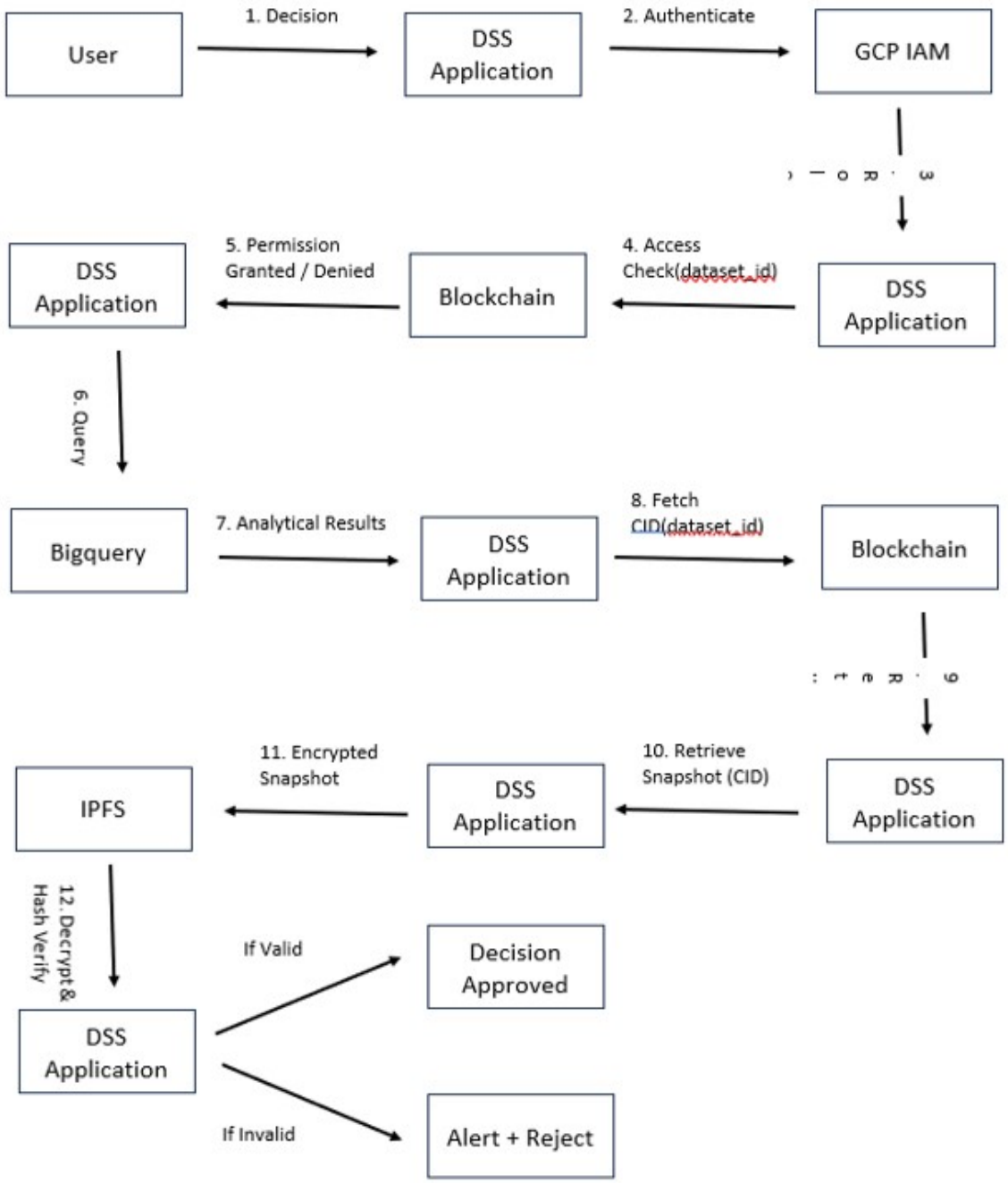


Figure 3: Sequence Diagram – Runtime DSS Operation

7.3. Experimental Setup and Evaluation

All experiments are run on Google Cloud Platform (GCP) with a reusable infrastructure orchestrated using Docker containers where the epidemiological model and the overall DSS orchestration services run on Compute Engine VMs with 4 vCPUs, 16 GB RAM and 100 GB SSD. IPFS nodes run on identical VMs to enable decentralized storage, while a permissioned blockchain network runs on dedicated VMs with moderated resources for execution of smart contracts and transactions verification, with secure HTTPS connections and authenticated service accounts. The evaluation uses anonymized cancer-related datasets comprises of time-series dataset of tumour growth, different treatment metadata comprising approximately 1.2 million records. Data is stored in BigQuery using a structured, partitioned and clustered schema optimised for analysis, including fields such as patient_id, timestamp, tumo_cell_count, treatment_type, growth_rate, recovery_rate, immune_response_index, and simulation_flag. Specific subsets of processed tables and subsequent results are saved as encrypted snapshots, stored in IPFS with unique IDs and recorded on the blockchain as integrity validation, checks and audits. All the log parameters, like Bigquery execution latency, model execution time, IPFS retrieval times, blockchain confirmation time etc. are collected centrally to perform comprehensive performance analysis and comparative evaluation between curent and proposed model configurations.

8. Results and Discussion

This section is about demonstrating the efficiency of the proposed framework by looking at certain parameters like predictive accuracy, system performance and trade-offs between security and performance.

The evaluation process is based on 3 key areas: They are

1. Comparison between feedback-based SIR model and conventional SIR model,
2. Data management using decentralized and on-chain storage, and
3. Cloud-based security mechanisms with its added processing overhead

8.1. Feedback-Based SIR Model vs Standard SIR Model

The proposed feedback-based SIR model was compared with the standard SIR model using cancer cell growth dataset in terms of predictive performance. Standard SIR model applied on epidemiological dataset achieved an overall predictive performance of 35%, in contrast, the feedback-based SIR model showed a significantly higher predictive performance of 62%. The improvement comes from the inclusion of feedback mechanisms that allow treated or dormant cells to transition back to the susceptible state, treating them vulnerable again, reflecting clinically observed recurrence patterns.

8.2. Data Storage Performance Analysis and Retrieval

The overall performance of the decentralized storage approach was evaluated by examining the relationship between file size and response time for both centralized and decentralized systems. The results demonstrate that response time increases with file size in decentralized storage, due to data retrieval from multiple sources and also it requires more coordination. Although decentralized approach is slower but it provides stronger data integrity and better fault tolerance, which are critical for clinical application. Compared to centralized storage, which responds faster for smaller files but it lacks security and immutability offered by the blockchain-enabled architecture.

8.3. Impact of Data Volume and Query Frequency of Blockchain

Scalability is evaluated by studying system response time across different Blockchain data volumes and different query rates. The result shows a strong positive correlation between data volume and response time. Similarly query rates is also proportional to response time because of simultaneous access and multiple validation operations. Despite of this increase, response times stayed within acceptable limits for clinical data access, indicating that the framework is suitability for real-world healthcare environments.

8.4. Cloud Computing and Security Overhead

The impact cloud-based authentication and corresponding security measure on system performance was studied by comparing processing times with authenticated and non-authenticated scenarios. Evaluation dictates that authentication takes additional time to process compared to non-authentication because of identity verification and access control checks. Authentication has some additional delay which is justified for the enhanced security mechanisms and regulatory compliance that it provides. Overall findings indicate that integrating strong security can be add without significantly affecting system responsiveness.

8.5. System Effectiveness

Results from the study indicate that the proposed framework effectively balances predictive accuracy, security and computational efficiency. Applying feedback-based SIR model improves cancer cell growth prediction. Along with that the blockchain embedded cloud framework ensures security, robustness and scalability. This integrated framework validates practical applicability of the proposed system as a decision-support tool for data driven cancer research.

Table 1: Malignant Cell Growth Prediction: Performance Comparison

Metric	Standard SIR Model	Feedback-Based SIR Model	Interpretation
Mean Absolute Error (MAE)	Higher	Lower	Indicates improved average prediction accuracy with feedback integration
Root Mean Square Error (RMSE)	Higher	Significantly lower	Demonstrates reduced sensitivity to large prediction deviations
Predictive Performance (%) Score	35%	62%	Shows substantial improvement in capturing cancer progression dynamics
Variance of Prediction Error	High	Reduced	Feedback model exhibits more stable predictions
95% Confidence Interval(CI) Width	Wider	Narrower	Reflects higher statistical reliability and robustness
Relapse/Dormancy Representation	Not captured	Explicitly modeled	Enables realistic cancer recurrence simulation
Model Stability Across Runs	Moderate	High	Consistent performance across multiple simulations

Table 2: System Performance Metrics of the Proposed Blockchain–Cloud Framework

Metric	**Centralized Storage System**	**Proposed Blockchain–IPFS System**	**Interpretation**
Average Data Upload Time	Lower	Slightly Higher	Additional overhead due to encryption, hashing and decentralized storage
Average Data Retrieval Time	Lower (small files)	Comparable (medium–large files)	Decentralization impact diminishes with larger data sizes
Scalability with Data Volume	Limited	High	IPFS enables horizontal scaling without centralized bottlenecks
On-Chain Data Size Growth	Not applicable	Minimal	Only hashes/identifiers stored on-chain
System Throughput	High	Moderate–High	Minor reduction due to blockchain validation
Response Time under High Query Load	Degrades rapidly	Stable	Blockchain ensures consistent access control
Fault Tolerance	Low	High	Distributed architecture prevents single-point failures
Data Integrity & Immutability	Moderate	Very High	Blockchain guarantees tamper resistance
Authentication Overhead	Not applicable	Present	Security trade-off remains within acceptable limits
Regulatory Compliance Support	Strong	Strong	Supports HIPAA/GDPR-style access control

Table 3: Impact of Cloud Authentication and Security Mechanisms on System Performance

Metric	**Without Authentication**	**With Cloud Authentication (IAM, Smart Contracts)**	**Interpretation**
Average Request Processing Time	Lower	Higher	Additional latency due to identity verification and access checks
Authentication Overhead	Not applicable	Present	Overhead introduced by token validation and permission checks
Response Time Variance	Low	Slightly Increased	Security layers add controlled variability
System Throughput	High	Moderate to High	Minimal degradation despite added security
Access Control Granularity	Coarse	Fine-grained	Role-based and policy-driven authorization
Unauthorized Access Prevention	Limited	Strong	IAM and smart contracts block invalid requests
Auditability & Traceability	Limited	Full	All access events are logged and verifiable
Compliance Readiness (HIPAA/GDPR)	Low	High	Supports regulatory requirements
Scalability under Concurrent Users	Moderate	High	Cloud IAM scales with user load
Security–Performance Trade-off	Favorable for speed	Balanced	Acceptable latency for improved security

8.6. Comparative Analysis

9. Conclusion and Future Directions

An Integrated framework is being proposed with a combination of epidemiological modelling, blockchain technology, cloud computing and machine learning. This framework is used to address different key challenges in cancer cell growth prediction and clinical data management. Feedback-based SIR model can able to accurately represents malignant cell behaviour including important biological processes like cell growth, dormancy, relapse, treatment resistance etc.

Experimental output enlighten that the proposed feedback-based SIR model performs better than the conventional SIR model in in terms of trend prediction, making it more suitability for those applications related to cancer prediction. Above that, blockchain technology is incorporated that guarantees secure, immutable and transparency for sensitive clinical data handling. The proposed off-chain storage, i.e. IPFS manages scalability and privacy. In order to control authorization mechanisms, smart contract is used that allows multiple institution to work together without compromising patient confidentiality. The proposed infrastructure also uses cloud-based infrastructure for scalable computation and smooth integration of machine learning models with real-time analytics and predictive capabilities. It also shows how modern technologies can work together to support precision oncology. Experimental results indicate that the imposed additional security incurred very minimal cost, making the system more practical from real-world healthcare environment perspective.

Table 4: Existing Models and the Proposed Framework

Feature / Metric	**Epidemiological Cancer Models**	**Blockchain-Based Healthcare Systems**	**ML-Based Cancer Prediction Models**	**Proposed Framework**
Representative Studies	Eftimie et al. (2021); Mahlbacher et al. (2022); de Pillis et al. (2023)	Sun et al. (2021); Hasselgren et al. (2022); Khan et al. (2023)	Ngiam & Khor (2021); Choudhury et al. (2022); Shickel et al. (2023)	This work
Core Objective	Tumor–immune interaction modeling	Secure clinical data sharing	Predictive accuracy	Epidemiological model+ prediction + security
Feedback / Relapse Modeling	Limited	Not applicable	Implicit	Explicit
Prediction Metrics (RMSE/MAE)	Rarely reported	Not reported	Accuracy/AUC focused	RMSE, MAE, CI
Model Interpretability	High	Not applicable	Low to Moderate	High
Data Security	None	Blockchain-based	Pipeline-dependent	Blockchain + IAM
Decentralized Storage	None	Partial	None	IPFS
Scalability	Moderate	High	High	High
Auditability	None	None	None	None
Clinical Deployment Readiness	Conceptual	Prototype	Dataset-validated	System-validated
Limitations Identified	No secure data handling	No prediction capability	Privacy & interpretability	Balanced trade-off

Future work aims to extend the framework by incorporating agent-based and spatial tumour models for better analysis on cell growth and adjacent environmental factors. Applying federated learning with Agentic AI techniques will further improve security and data management while allowing collaborative model applications across diversified institutions. Moreover, the proposed framework can be extended for other non-communicable diseases, making it a flexible solution for next-generation, data-driven public healthcare systems.

Article Information

Acknowledgments: The author would like to express his sincere gratitude to everyone who supported and contributed to this research work. We are especially thankful to our mentors and colleagues for their valuable guidance, insightful suggestions, and continuous encouragement throughout the study. We also acknowledge the institutions and organizations that provided the necessary resources and environment to conduct this research. Their support played an important role in the successful completion of this work.

Author Contributions: Supratim Bhattacharya - Conceptualization, Methodology, Data curation, Formal analysis, Writing – original draft, Writing – review & editing, Supervision.

Funding / Financial Support: The authors received no external funding.

Conflict of Interest: The author declares no competing interests.

Ethical Approval: Not applicable.

Informed Consent: Not applicable.

Data Availability Statement: Data available on reasonable request.

Clinical Trial Registration: Not applicable.

Disclaimer (Artificial Intelligence): The author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.), and text-to-image generators have been used during writing or editing of manuscripts.

Competing Interests: Authors have declared that no competing interests exist.

References

[1] J. Metzcar, Catherine R. Jutzeler, Paul Macklin, Alvaro Köhn-Luque, and Sarah C. Brüningk. A review of mechanistic learning in mathematical oncology. doi:10.3389/fimmu.2024.1363144, 2024.

[2] Lifeng Han, Marisabel Rodriguez Messan, Osman N. Yogurtcu, Ujwani Nukala, and Hong Yang. Analysis of tumor-immune functional responses in a mathematical model of neoantigen cancer vaccines. *Mathematical Biosciences*, 356:108966, 2023. ISSN 0025-5564. URL https://doi.org/10.1016/j.mbs.2023.108966.

[3] V. Bitsouni, M. Chaplain, and R. Eftimie. Mathematical Modelling of Cancer Invasion: The Multiple Roles of TGF-β Pathway on Tumour Proliferation and Cell Adhesion. *Mathematical Models and Methods in Applied Sciences*, 27(10):1929–1962, 2017. URL https://doi.org/10.1142/S021820251750035X.

[4] A. Rehman, S. Naz, and I. Razzak. Leveraging big data analytics in healthcare enhancement: Trends, challenges and opportunities. arXiv preprint arXiv:2004.09010, 2020.

[5] D. Kiaei and H. Tourajizadeh. Non-Linear Control of Cancer Model, Considering the Drug Resistance Using Feedback Based Chemotherapy Approach. In *2022 13th International Conference on Information and Knowledge Technology (IKT)*, pages 1–7, Karaj, Iran, 2022. IEEE. doi: 10.1109/IKT57960.2022.10039006.

[6] T. Lysaght, H. Y. Lim, V. Xafis, and K. Y. Ngiam. AI-assisted decision-making in healthcare. *Asian Bioethics Review*, 11(3):299–314, 2019.

[7] R. Kirkscey. Health Apps for Older Adults: A Method for Development and User Experience Design Evaluation. *Journal of Technical Writing and Communication*, 51(2):199–217, 2020. URL https://doi.org/10.1177/0047281620907939.

[8] W. Materi and D. S. Wishart. Computational systems biology in cancer: modeling methods and applications. *Gene Regul Syst Bio*, 1: 91–110, September 2007. PMID: 19936081. PMCID: PMC2759135.

[9] Jigna J. Hathaliya and Sudeep Tanwar. An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*, 153:311–335, 2020. ISSN 0140-3664. URL https://doi.org/10.1016/j.comcom.2020.02.018.

[10] H. B. Mahajan et al. Integration of Healthcare 4.0 and blockchain into secure cloud-based EHR systems. *Applied Nanoscience*, 13(3): 2329–2342, 2023.

[11] J. Paul et al. Privacy-preserving collective learning with homomorphic encryption. *IEEE Access*, 9:132084–132096, 2021.

[12] L. Hirtan, P. Krawiec, C. Dobre, and J. M. Batalla. Blockchain-based approach for e-health data access management. In *Proceedings of the IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, 2019.

[13] M. Taleka, K. Makkithaya, and N. V. G. Blockchain-based decentralized identifiers for EHR authentication. *Cogent Engineering*, 9, 2022. doi:10.1080/23311916.2022.2035134.

[14] K. Ngiam and Y. Khor. *Big data and AI in oncology*. Nature Medicine, 2021.

[15] R. Saha et al. Privacy ensured e-healthcare for fog-enhanced IoT applications. *IEEE Access*, 7:44536–44543, 2019. doi:10.1109/ACCESS.2019.2908664.

[16] D. Placido, B. Yuan, J. X. Hjaltelin, et al. A deep learning algorithm to predict risk of pancreatic cancer from disease trajectories. *Nat Med*, 29:1113–1122, 2023. doi:10.1038/s41591-023-02332-5.

[17] G. Srivastava, R. M. Parizi, and A. Dehghantanha. *Blockchain Cybersecurity, Trust and Privacy*. Springer, Cham, Switzerland, 2020. doi:10.1007/978-3-030-38181-3_9.

[18] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar*, pages 310–317, 2020. doi:10.1109/ICIoT48696.2020.9089570.

[19] Yunhee Kang, Jaehyuk Cho, and Young B. Park. An empirical study of a trustworthy cloud common data model using decentralized identifiers. *Applied Sciences*, 11(19):8984, September 2021. doi: 10.3390/app11198984.

[20] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and E. Hossain. A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes. *IEEE Access*, 8:118433–118471, 2020. doi:10.1109/ACCESS.2020.3004790.

[21] S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty. Interoperability and Synchronization Management of Blockchain-Based Decentralized e-Health Systems. *IEEE Transactions on Engineering Management*, 67(4):1363–1376, 2020. doi: 10.1109/TEM.2020.2989779. Article 9112689.

[22] S. Routray and R. Ganiga. Secure storage of electronic medical records on IPFS using blockchain. In *Proc. ICECCT, 2021*, pages 1–9, 2021. doi: 10.1109/ICECCT52121.

[23] S. Cao, X. Zhang, and R. Xu. Blockchain-assisted secure storage in cloud-based eHealth systems. *IEEE Network*, 34(2):64–70, 2020.

[24] Jin Sun, Lili Ren, Shangping Wang, and Xiaomin Yao. A blockchain-based framework for electronic medical records sharing with fine-grained access control. doi:10.1371/journal.pone.0239946, October 2020.

[25] S. S. Raj. IoT and big data analytics for healthcare with cloud computing. *Journal of Information Technology and Digital World*, 1(1): 9–18, 2019. doi:10.36548/jitdw.2019.1.002.

[26] Adeoluwa Atanda. Cloud Computing in Healthcare Industry: A Systematic Literature Review. *Global Journal of Information Technology Emerging Technologies*, 13(2):64–71, November 2023. doi:10.18844/gjit.v13i2.8867.

[27] A. Sajid and H. Abbas. Data privacy in cloud-assisted healthcare systems: State of the art and future challenges. *Journal of Medical Systems*, 40(6):1–15, June 2016. doi:10.1007/s10916-016-0509-2.

[28] S. Immaculate Shyla and S. S. Sujatha. Efficient secure data retrieval on cloud using multi-stage authentication and optimized blowfish algorithm. *Journal of Ambient Intelligence and Humanized Computing*, 13(3):1–13, January 2022. doi: 10.1007/s12652-021-02893-8.

[29] A. Hoseinpour Dehkordi, M. Alizadeh, P. Derakhshan, P. Babazadeh, and A. Jahandideh. Understanding epidemic data and statistics: A case study of COVID-19. *J Med Virol*, 92(7):868–882, July 2020. doi: doi:10.1002/jmv.25885. PMID: 32329522. PMCID: PMC7264574. Epub 2020 Apr 25.

[30] J. Wang et al. High temperature and high humidity reduce COVID-19 transmission. 2020.

[31] S. Mittal. Exploratory data analysis of COVID-19 in India. doi:10.17577/IJERTV9IS040550., 2020.

[32] R. Gupta and S. K. Pal. Trend analysis and forecasting of COVID-19 outbreak in India. doi:10.1101/2020.03.26.20044511., 2020.

[33] R. S. Yadav. Mathematical modeling of SIR model for COVID-19. 2020.

[34] M. Jakhar et al. COVID-19 epidemic forecasting using SIR model. 2020.

[35] S. Moein et al. Inefficiency of SIR models in epidemic forecasting. 2020.

[36] M. Mehrtak, S. SeyedAlinaghi, M. MohsseniPour, T. Noori, A. Karimi, A. Shamsabadi, M. Heydari, A. Barzegary, P. Mirzapour, M. Soleymanzadeh, F. Vahedi, E. Mehraeen, and O. Dadras. Security challenges and solutions using healthcare cloud computing. *J Med Life*, 14(4):448–461, July–August 2021. doi: 10.25122/jml-2021-0100. PMID: 34621367. PMCID: PMC8485370.

[37] S. Khan, M. Khan, M. A. Khan, M. A. Khan, L. Wang, and K. Wu. A Blockchain-Enabled AI-Driven Secure Searchable Encryption Framework for Medical IoT Systems. *IEEE Journal of Biomedical and Health Informatics*, 38, December 2022. doi:10.1109/JBHI.2025.3538623.

[38] I. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, and K. N. Qureshi. Health-ID: A blockchain-based decentralized identity management for remote healthcare. *Healthcare*, 9(6):712, 2021. doi:10.3390/healthcare9060712.

[39] P. K. Ghosh, A. Chakraborty, M. Hasan, K. Rashid, and A. H. Siddique. Blockchain Application in Healthcare Systems: A Review. *Systems*, 11:38, 2023. doi:10.3390/systems11010038.

[40] R. Akkaoui, X. Hei, and W. Cheng. EdgeMediChain: A hybrid edge–blockchain framework for health data exchange. *IEEE Access*, 8: 113467–113486, 2020.

[41] Cristina Regueiro, Iñaki Seco, Santiago de Diego, Oscar Lage, and Leire Etxebarria. Privacy-enhancing distributed protocol for data aggregation based on blockchain and homomorphic encryption. *Information Processing Management*, 58(6):102745, 2021. doi:10.1016/j.ipm.2021.102745. ISSN 0306-4573.

[42] L. Syed et al. Smart healthcare framework using IoMT and big data analytics. *Future Generation Computer Systems*, 101:136–151, 2019.

[43] S. Bhattacharya, J. Poray, and P. Debnath. A bigdata analytics framework on the impact of non communicable diseases in kolkata. In *2020 International Conference on Computer, Electrical Communication Engineering (ICCECE). IEEE*, pages 1–8, 2020. https://doi.

[44] B. Behara, M. Delrobaei, and N. Afraz. Trusted Blockchain-Based Clinical Decision and Medication Management System for Movement Disorders. *IEEE Access*, 13:139404–139418, 2025. doi:10.1109/ACCESS.2025.3596693.

[45] V. Mani, P. Manickam, Y. Alotaibi, S. Alghamdi, and O. I. Khalaf. Hyperledger Healthchain: Patient-Centric IPFS-Based Storage of Health Records. *Electronics*, 10:3003, 2021. doi:10.3390/electronics10233003.

[46] S. Mandal, S. Bhattacharya, and J. Poray. Towards a decision support system by the study of cell malfunctions for breast cancer. In *2016 International Conference on Computer, Electrical Communication Engineering (ICCECE). IEEE. 2017;. ICCECE.2016.8009583*, pages 1–7, 2017.

[47] S. Bhattacharya, J. Poray, and P. Debnath. The Impact of Big Data Analytics on Risk Management and Decision Making: International conference on Recent Trends in Artificial Intelligence, IOT, Smart Cities Applications (ICAISC-2020). *SSRN Electronic Journal*, pages 1–7, 2020. doi:10.2139/ssrn.3758051.

[48] S. Bhattacharya, S. Goswami, P. Chowdhury, P. Pal, and J. Poray. Data Analytics for Pandemic: A Covid-19 Case Study in Kolkata, Book - Artificial Intelligence Solutions for Cyber-Physical Systems. *Auerbach Publications*, pages 404–418, 2024.

[49] Sreepal Reddy Bolla. Enhancing Healthcare Analytics with Federated Learning and Cloud Technologies for Improved Patient Outcomes. *Int J Intell Syst Appl Eng*, 13(1):346–352, April 2025.

[50] R. Geva, A. Gusev, Y. Polyakov, L. Liram, O. Rosolio, A. Alexandru, N. Genise, M. Blatt, Z. Duchin, B. Waissengrin, D. Mirelman, F. Bukstein, D. T. Blumenthal, I. Wolf, S. Pelles-Avraham, T. Schaffer, L. A. Lavi, D. Micciancio, V. Vaikuntanathan, A. A. Badawi, and S. Goldwasser. Collaborative privacy-preserving analysis of oncological data using multiparty homomorphic encryption. *Proc Natl Acad Sci U S A*, 120(33), August 2023. doi:10.1073/pnas.2304415120.

[51] World Health Organization. Digital Health and Oncology Systems. WHO Press, 2024.

[52] C. H. Cheng and S. S. Shi. Artificial intelligence in cancer: applications, challenges, and future perspectives. *Mol Cancer*, 24(1):274, October 2025. doi: 10.1186/s12943-025-02450-3. PMID: 41168799. PMCID: PMC12574039.

[53] A. Verma et al. Cloud-Based Decision Support Systems For Managing Healthcare Operations And Financial Risks. *International Journal of Scientific Research Engineering Trends*, 9(2), March–April 2023. URL http://doi.org/10.5281/zenodo.18229034.