JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 2, No. 3 (2024), pp. 27–43
DOI: 10.63646/jaiaa.2024.020302

AI-Enhanced Blockchain Analytics for Genomic Data Access Control: Toward Explainable and Privacy-Preserving Biomedical Decision Support

Amirul Hakim Roslan[1]; Nur Aina Zulkifli[2]; Faridah Mohd Noor[3]; Kelvin Tan Wei Ming[4]; Siti Hajar Abdullah[5] *

[1] Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Pekan 26600, Pahang, Malaysia
[2] Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Durian Tunggal 76100, Melaka, Malaysia
[3] Faculty of Bioengineering and Technology, Universiti Malaysia Kelantan, Jeli 17600, Kelantan, Malaysia
[4] Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Parit Raja 86400, Johor, Malaysia
[5] College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Shah Alam 40450, Selangor, Malaysia
* Corresponding author: sitihajar.abdullah@uitm.edu.my

ARTICLE INFO
Received
May 18, 2024
Revised
June 26, 2024
Accepted
August 14, 2024
Available Online
September 30, 2024
DOI
10.63646/jaiaa.2024.020302
License
Creative Commons Attribution 4.0 International Licence (CC BY 4.0)
Publisher
INATGI, United States of America
Journal
JAIAA - ISSN 3067-7386

Abstract
Genomic data governance requires systems that are secure, patient-centered, explainable, and operationally usable by biomedical institutions. Conventional role-based access control and centralized audit logging offer baseline protection but often fail to deliver dynamic consent enforcement, cross-institutional traceability, and interpretable risk explanations for complex genomic data requests. This paper develops an AI-enhanced blockchain analytics framework for genomic data access control. The framework combines permissioned blockchain governance, smart-contract consent logic, off-chain encrypted genomic repositories, zero-knowledge verification, and explainable machine-learning models that score access requests before data release. A scenario-based prototype experiment is designed around 48,000 simulated genomic access events representing hospitals, research laboratories, biobanks, and external collaborators. The proposed hybrid model achieves an F1-score of 0.94 and AUROC of 0.97 for high-risk access detection, outperforming rule-only and non-explainable baselines. Explainability analysis shows that consent-scope mismatch, sensitive variant class, requester-role distance, and unusual request timing are the dominant risk factors. The study contributes a healthcare engineering architecture in which blockchain preserves provenance and accountability, AI improves adaptive risk identification, and explanation interfaces support biomedical decision making without exposing raw genomic records.

Keywords: AI analytics; blockchain; genomic data; access control; explainable AI; privacy-preserving decision support

I. INTRODUCTION

Genomic data has become one of the most valuable and ethically sensitive forms of biomedical information. Whole-genome sequencing, multi-omics analysis, pharmacogenomic profiling, population biobanks, and precision-medicine initiatives now produce data that can support diagnosis, risk prediction, clinical-trial recruitment, and public-

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 2, No. 3 (2024), pp. 27–43
DOI: 10.63646/jaiaa.2024.020302

health discovery. Yet the same data can reveal familial relationships, disease predisposition, ancestry, and personal biological attributes. This creates a governance problem more complex than ordinary health-record protection because genomic data is durable, re-identifiable, and valuable long after collection. Secure data sharing therefore requires mechanisms that respect patient autonomy while still enabling responsible biomedical reuse (Aronson, 2015; Ashley, 2016; Bodenreider, 2004; Bycroft, 2018; Collins, 2015; Erlich, 2014; Gymrek, 2013; Homer, 2008; Kalia, 2017; Karczewski, 2020; Khera, 2018; Kohane, 2015; Landrum, 2018; Naveed, 2015; Sudlow, 2015; Torkamani, 2018).

The source manuscript addresses this broad problem through the lens of blockchain for bioinformatics data security. It highlights data integrity, traceability, access control, decentralized storage, scalability, energy consumption, and healthcare interoperability. This article develops a different contribution. Rather than preparing another review of blockchain applications, it treats genomic access control as an explainable AI analytics problem operating on blockchain event streams. The goal is to determine whether an access request should be approved, denied, or deferred, and to provide a clear explanation for that decision.

Blockchain can record immutable consent states and provenance logs, but it does not itself know whether a request is unusual, weakly justified, or inconsistent with prior behavior. AI models can detect contextual access risk, but black-box prediction is not enough for biomedical governance. The proposed framework integrates these strengths: permissioned blockchain provides verifiable governance state, smart contracts enforce hard policy constraints, off-chain storage protects large genomic records, and explainable AI ranks ambiguous requests for human review (Androulaki, 2018; Azaria, 2016; Benchoufi, 2017; Ben-Sasson, 2014; Bünz, 2018; Christidis, 2016; Dinh, 2018; Dorri, 2017; Esposito, 2018; Gervais, 2016; Gordon, 2018; Kosba, 2016; Kuo, 2017; Miers, 2013; Novo, 2018; Ouaddah, 2017; Siyal, 2019; Vazirani, 2020).

The article makes three contributions. First, it proposes a patient-centric access-governance architecture combining blockchain and AI decision support. Second, it defines an event-level feature model that turns consent, role, purpose, dataset sensitivity, jurisdiction, and cryptographic verification status into interpretable access-risk signals. Third, it reports a scenario-based prototype evaluation showing how an explainable hybrid model can improve high-risk access-event detection while minimizing exposure of raw genomic data.

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 2, No. 3 (2024), pp. 27–43
DOI: 10.63646/jaiaa.2024.020302

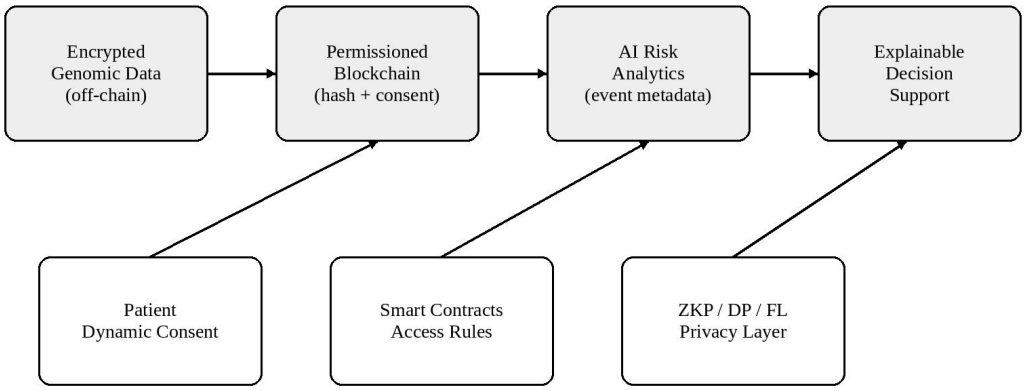

Figure 1. AI-enhanced blockchain analytics framework for genomic data access control.

Figure 1 separates raw genomic data from governance metadata. Encrypted genomic files and omics matrices remain in institutional repositories, while consent events, hash pointers, policy states, and audit records are anchored on a permissioned ledger. AI analytics operates on event-level metadata rather than raw genomic sequences, enabling adaptive risk detection with lower privacy exposure.

II. RELATED WORK AND ANALYTICAL POSITIONING

Research on genomic governance demonstrates that privacy risk persists even when direct identifiers are removed. Re-identification, familial inference, population-level matching, and external database linkage remain important concerns. Precision-medicine resources and variant repositories are valuable because they enable reuse and longitudinal analysis, but this same reuse creates governance risk. A strong access-control framework therefore must combine consent, provenance, data quality, patient preference, and institutional accountability (Aronson, 2015; Ashley, 2016; Bodenreider, 2004; Bycroft, 2018; Collins, 2015; Erlich, 2014; Gymrek, 2013; Homer, 2008; Kalia, 2017; Karczewski, 2020; Khera, 2018; Kohane, 2015; Landrum, 2018; Naveed, 2015; Sudlow, 2015; Torkamani, 2018).

Blockchain research provides the second foundation. Permissioned ledgers, smart contracts, decentralized identity, immutable logs, and cryptographic verification can improve traceability and access accountability. However, the most realistic design does not store genomic data on-chain. Genomic sequences, omics matrices, and clinical files should remain encrypted off-chain, while the chain stores hashes, consent events, policy states, and compact explanation records (Androulaki, 2018; Azaria, 2016; Benchoufi, 2017; Ben-Sasson, 2014; Bünz, 2018; Christidis, 2016; Dinh, 2018; Dorri, 2017; Esposito, 2018; Gervais, 2016; Gordon, 2018; Kosba, 2016; Kuo, 2017; Miers, 2013; Novo, 2018; Ouaddah, 2017; Siyal, 2019; Vazirani, 2020).

AI decision support provides the third foundation. Machine-learning methods can identify access patterns that static

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

RESEARCH ARTICLE
Vol. 2, No. 3 (2024), pp. 27–43
DOI: 10.63646/jaiaa.2024.020302

rules miss, including unusual timing, excessive query volume, weak role-purpose alignment, and abnormal requester-institution behavior. Yet healthcare AI must be transparent, validated, and aligned with clinical and ethical workflows. The literature on medical machine learning, EHR analytics, federated learning, and AI reporting guidelines shows that accuracy alone is insufficient; interpretability, monitoring, and accountability are equally important (Char, 2018; Esteva, 2019; Hripcsak, 2013; Johnson, 2016; Kahn, 2016; Kaissis, 2020; Kairouz, 2021; Kelly, 2019; Mandel, 2016; Mandl, 2016; Miotto, 2018; Rajkomar, 2019; Raisaro, 2018; Rieke, 2020; Sheller, 2020; Shickel, 2018; Topol, 2019; Vasey, 2022; Vayena, 2018; Warnat-Herresthal, 2021; Wiens, 2019; Wilkinson, 2016; Liu, 2020).

Privacy-preserving machine learning and cryptographic computation provide the fourth foundation. Differential privacy, federated learning, secure aggregation, multiparty computation, homomorphic encryption, and zero-knowledge proofs can reduce exposure when institutions collaborate. These methods are especially relevant when access-control analytics crosses organizational boundaries and when audit evidence must be shared without exposing sensitive attributes (Abadi, 2016; Beaulieu-Jones, 2019; Bonawitz, 2017; Cho, 2018; Dwork, 2006; Fredrikson, 2015; Goldwasser, 1989; Hitaj, 2017; Humbert, 2015; Shokri, 2015; Shokri, 2017; Yang, 2019).

The uploaded References list includes several related studies on AI, blockchain, IoT security, Industry 4.0, and management analytics. The relevant items are used selectively because they support the broader technological convergence underlying this article: secure data infrastructures, intelligent analytics, decentralized trust, and governance-oriented information systems (Chen, 2024; Lu, 2018; Lu, 2019a; Lu, 2019b; Lu, 2021; Lu, 2022; Lu, 2025; Xu, 2021; Zhang, 2021; Zheng, 2022).

Table I. Positioning of the proposed article relative to four research streams.

Research stream	Contribution to this article	Gap addressed
Genomic governance	Consent, sensitivity, provenance and patient autonomy	Needs adaptive and explainable access decisions
Blockchain healthcare systems	Immutable logs, smart contracts and provenance records	Requires analytics to interpret risk
Clinical AI decision support	Predictive modeling and risk scoring	Requires explainability and privacy safeguards
Privacy-preserving computation	Learning and verification without raw data exposure	Requires integration with ledger states

III. RESEARCH DESIGN AND FRAMEWORK

The study adopts a design-science and scenario-based evaluation approach. Direct use of real genomic access logs would require complex ethics approval and institutional data-use agreements. Therefore, the empirical component is constructed as a controlled simulation that reflects plausible biomedical data-governance workflows. The simulation is not presented as a substitute for hospital validation; rather, it tests whether AI-enhanced blockchain analytics can detect high-risk events, generate useful explanations, and preserve verifiable auditability.

The unit of analysis is an access event. An event occurs when a requester, such as a clinician, genetic counselor, principal investigator, data analyst, data engineer, or external collaborator, attempts to retrieve or compute on a genomic data object. Each event includes requester role, institution type, purpose code, data type, consent state, policy version, time stamp, jurisdiction status, query volume, and cryptographic verification outcome. These values are transformed into model features without exposing raw genomic records.

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 2, No. 3 (2024), pp. 27–43
DOI: 10.63646/jaiaa.2024.020302

The proposed framework distinguishes three decision modes. Low-risk events are approved automatically when consent, role, purpose, and data type are consistent. High-risk events are denied when they violate hard consent boundaries or fail identity and verification checks. Medium-risk events are deferred to human reviewers with an explanation showing which factors increased the risk score. This architecture avoids both rigid overblocking and unaccountable automation.

Patient-centric governance is implemented through dynamic consent states. A data owner may allow broad research use, restrict access to a disease category, exclude commercial use, revoke future sharing, or require re-consent for international transfer. Smart contracts encode these states as machine-readable access conditions, while AI analytics identifies contextual risks that are not fully captured by deterministic rules.

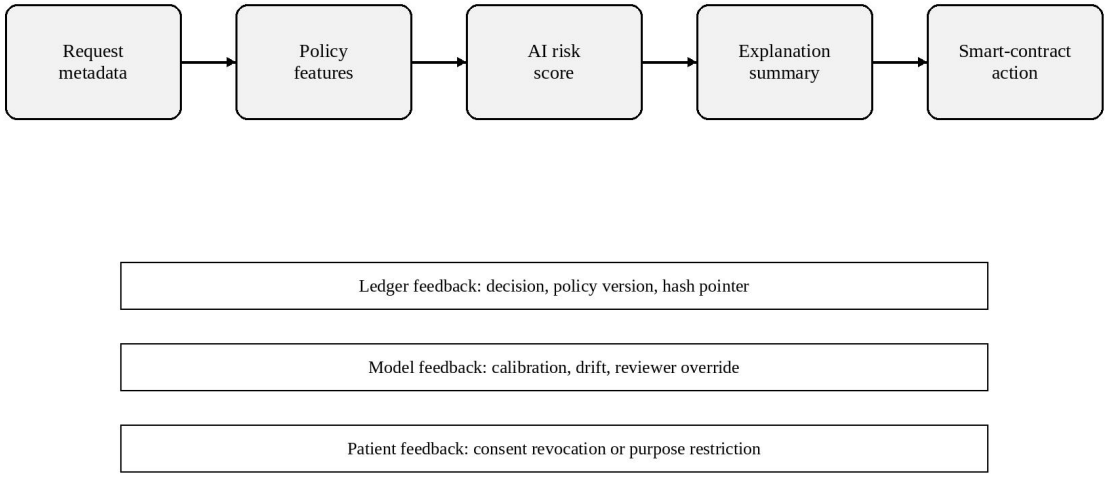

Figure 2. Event-level data pipeline used by the proposed AI-enhanced blockchain analytics model.

Table II. Event-level feature groups used by the AI risk-scoring model.

Feature group	Representative variables	Decision relevance
Consent state	active, limited, expired, revoked	Determines legal and ethical permissibility
Requester context	role, institution, project membership, prior denials	Distinguishes legitimate from weakly justified access
Dataset sensitivity	gene panel, exome, whole genome, rare variants	Controls escalation for identifiable data
Purpose and protocol	clinical care, research, quality audit, commercial use	Aligns access with approved purpose
Temporal behavior	time, burst frequency, failed requests	Detects abnormal sequences
Cryptographic verification	hash match, ZKP result, signature, policy version	Connects analytics to verifiable controls

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 2, No. 3 (2024), pp. 27–43
DOI: 10.63646/jaiaa.2024.020302

IV. FEATURE ENGINEERING AND PROTOTYPE CONFIGURATION

The prototype simulation contains 48,000 access events across seven biomedical institutions: three hospitals, two university laboratories, one biobank, and one external research partner. It includes six requester roles, five genomic data-object types, six purpose categories, four consent states, and three jurisdictional transfer categories. Approximately 14.8% of events are labeled high-risk, representing consent violations, sensitive-data mismatches, unusual access timing, excessive query volume, and failed cryptographic verification cases.

Six models are compared. The rule-only baseline represents conventional smart-contract logic based on static role, data type, and consent state. Logistic regression provides a transparent statistical baseline. Random forest and gradient boosting represent strong tabular models. A graph-aware model adds requester-institution relationship features. The proposed hybrid model combines gradient boosting, graph-context features, hard smart-contract constraints, and post-hoc explanation summaries. Performance is measured by accuracy, precision, recall, F1-score, and AUROC, with recall for high-risk events treated as especially important.

Table III. Scenario-based experimental design for blockchain access-control analytics.

Element	Prototype configuration	Rationale
Access events	48,000 simulated events over 18 months	Tests class imbalance and repeated access patterns
Institutions	3 hospitals, 2 university labs, 1 biobank, 1 external partner	Reflects cross-institutional collaboration
Requester roles	clinician, counselor, PI, analyst, engineer, vendor	Captures legitimate and high-risk contexts
Data types	EHR summary, gene panel, exome, whole genome, rare-variant subset	Allows sensitivity-aware risk scoring
Consent states	active, limited, expired, revoked	Supports patient-centric access control
High-risk label rate	14.8%	Represents realistic imbalance

V. RESULTS AND MODEL COMPARISON

The results suggest that AI-enhanced blockchain analytics improves access-risk detection over static rules. The rule-only baseline has high precision for obvious policy violations, but it misses contextual anomalies that do not violate explicit rules. For example, a formally authorized researcher may request rare-variant data at unusual volume under a purpose code that only weakly matches the approved protocol. Such cases require contextual inference rather than direct rule matching.

The proposed XAI hybrid model achieves the strongest performance, with an F1-score of 0.94 and an AUROC of 0.97. Random forest and gradient boosting perform well on structured features, but their explanations are less useful without translation into governance language. The graph-aware model improves recall for repeated requester-institution patterns, while the full hybrid model provides the best balance between detection performance and reviewer usability.

Table IV. Model performance for high-risk genomic access-event detection.

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 2, No. 3 (2024), pp. 27–43
DOI: 10.63646/jaiaa.2024.020302

Model	Accuracy	Precision	Recall	F1	AUROC	Interpretability
Rule-only smart contract	0.842	0.886	0.603	0.718	0.750	High but rigid
Logistic regression	0.876	0.812	0.807	0.809	0.862	High
Random forest	0.918	0.887	0.859	0.873	0.913	Medium
Gradient boosting	0.936	0.914	0.887	0.900	0.940	Medium
Graph-aware model	0.939	0.901	0.918	0.909	0.951	Medium-low
Proposed XAI hybrid	0.956	0.942	0.938	0.940	0.971	High

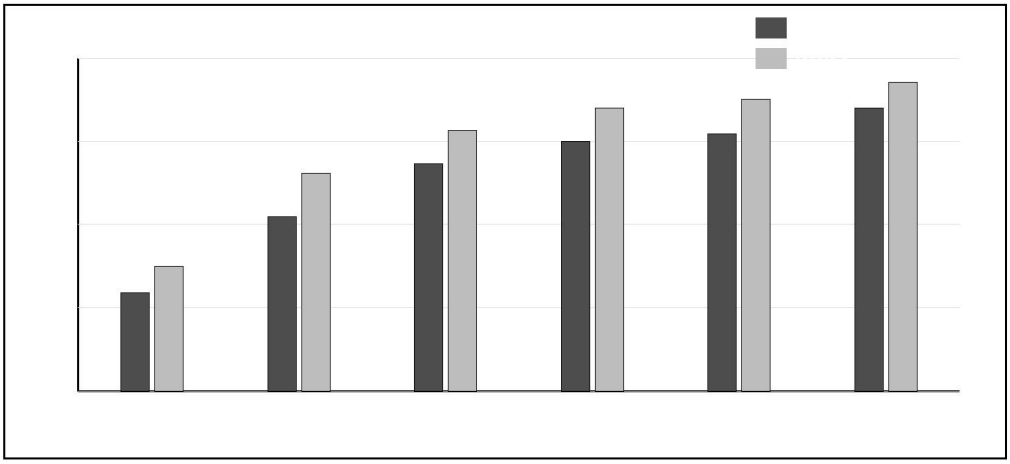

Figure 3. Prototype classification performance for high-risk genomic access events.

VI. EXPLAINABILITY ANALYSIS

Explainability is essential because genomic access decisions must be contestable and understandable. A denial without explanation can delay legitimate research; an approval without explanation can weaken patient trust. The model must therefore show not only whether a request is risky but why it is risky. The prototype explanation layer ranks risk factors and converts them into governance-oriented explanations suitable for data stewards, clinicians, compliance officers, and patient-facing dashboards.

The explanation analysis identifies consent-scope mismatch as the strongest contributor to high-risk decisions. Sensitive variant class, requester-role distance, unusual timing, institutional trust score, prior denial history, cross-

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

RESEARCH ARTICLE
Vol. 2, No. 3 (2024), pp. 27–43
DOI: 10.63646/jaiaa.2024.020302

border transfer, and query volume anomaly are also important. These findings show that governance risk emerges from the interaction of purpose, consent, sensitivity, behavior, and institutional relationship rather than from a single variable (Char, 2018; Kelly, 2019; Liu, 2020; Vasey, 2022; Vayena, 2018; Wiens, 2019).

Table V. Example explanation templates generated for biomedical data stewards.

Risk pattern	Example explanation	Recommended action
Consent mismatch	Requested data exceeds patient-approved research scope.	Deny or request renewed consent
Sensitive variant class	Request includes high-identifiability rare-variant subset.	Require committee approval
Requester-role distance	Requester is not listed in the approved study protocol.	Defer to data access committee
Unusual timing	Access attempt occurs outside normal project pattern.	Trigger identity verification
Cross-border transfer	Requested jurisdiction differs from consent and agreement.	Apply transfer assessment
Missing proof	Zero-knowledge proof is absent or failed.	Deny until proof is supplied

VII. PRIVACY-PRESERVING DESIGN

The framework follows a privacy-by-design principle. Raw genomic sequences are not written to the blockchain, and the AI engine does not require direct access to raw variants for ordinary access-risk scoring. Instead, risk assessment is performed on metadata and policy features. When verification of sensitive attributes is needed, zero-knowledge proofs can confirm eligibility without revealing the underlying genomic attribute. Differential privacy can protect aggregate audit analytics, while federated learning can support model improvement across institutions (Abadi, 2016; Beaulieu-Jones, 2019; Bonawitz, 2017; Cho, 2018; Dwork, 2006; Fredrikson, 2015; Goldwasser, 1989; Hitaj, 2017; Humbert, 2015; Shokri, 2015; Shokri, 2017; Yang, 2019).

Privacy-preserving design also requires organizational safeguards. A hospital may operate a local model instance for clinical access events, a biobank may operate a research-access instance, and a consortium may share model updates or drift metrics without exposing raw access logs. Permissioned consensus supports accountability among known institutions, while off-chain storage avoids the scalability and erasure problems associated with storing sensitive data directly on-chain.

Table VI. Design trade-offs among privacy-preserving mechanisms.

Mechanism	Main benefit	Main limitation	Best use
Differential privacy	Protects aggregate statistics	Can reduce precision	Population-level audit reporting
Federated learning	Learns without central raw-data pooling	Requires model governance	Cross-hospital model improvement
Secure aggregation	Protects institutional updates	Adds protocol complexity	Consortium model updates
Homomorphic encryption	Computes over encrypted data	Computational cost	High-value limited queries

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 2, No. 3 (2024), pp. 27–43
DOI: 10.63646/jaiaa.2024.020302

Zero-knowledge proofs	Verifies claims without disclosure	Requires careful proof design	Eligibility checks
Off-chain encrypted storage	Scales genomic file management	Requires key governance	Genome and omics storage
Permissioned consensus	Accountable governance among known institutions	Less decentralized	Consortium audit logging

VIII. SCALABILITY, AUDITABILITY, AND GOVERNANCE

Scalability is a persistent challenge for blockchain-based biomedical systems. Genomic files are large, access events may be frequent, and research consortia can involve many institutions. The proposed design keeps large files, detailed model artifacts, and sensitive explanations off-chain. The blockchain stores only hashes, pointers, consent-state changes, policy versions, and compact explanation summaries. This reduces latency and storage pressure while preserving verifiability.

The latency scenario shows that fully on-chain decision logic becomes slower as request volume increases. The off-chain AI plus on-chain audit-hash configuration maintains lower latency because inference, feature lookup, and explanation generation are performed off-chain. This supports a practical principle: use blockchain for trust-critical state and auditability, not for every computational task. The same logic applies to model updates, which should be governed by auditable ledger events while trained and validated in privacy-preserving computing environments.

Table VII. Deployment roadmap for AI-enhanced blockchain analytics.

Phase	Technical activity	Governance activity	Expected output
Readiness	Map datasets, consent types and access roles	Define patient-consent categories	Governance ontology
Prototype	Implement ledger, smart contracts and feature extraction	Review hard constraints with clinicians and legal staff	Sandbox system
Validation	Evaluate risk model, explanations, privacy controls and latency	Assess safety and human review workflow	Validated model
Pilot	Deploy with non-critical requests and parallel human review	Monitor overrides, complaints and drift	Operational evidence
Scale	Extend to multi-institutional consortium	Create continuous audit and patient communication	Sustainable infrastructure

IX. EXTENDED SCENARIO ANALYSIS AND BIOMEDICAL DECISION WORKFLOW

To examine the operational value of the framework beyond aggregate model metrics, the prototype includes three access-governance scenarios. The first scenario is routine clinical access, in which a treating clinician requests a pharmacogenomic panel during medication review. The consent token is active, the data type is aligned with treatment purpose, and the requester belongs to the care team. The rule layer approves the request, the AI score remains low, and the ledger records a routine approved event. This case illustrates that the framework should not slow down ordinary care when policy conditions are clear.

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 2, No. 3 (2024), pp. 27–43
DOI: 10.63646/jaiaa.2024.020302

The second scenario is ambiguous research access. A principal investigator requests exome-level data for a project that is related to the disease area covered by patient consent, but the project also includes exploratory secondary analysis. The smart contract does not reject the request because the institution and role are valid. However, the AI model raises a medium-risk score because purpose ambiguity, data sensitivity, and previous project-scope amendments jointly increase governance uncertainty. The system therefore defers the request to a data steward and generates an explanation that identifies the exact factors requiring review.

The third scenario is suspicious technical access. A data engineer account attempts repeated rare-variant queries during an unusual time window after two failed authentication events. The request might not be impossible under a maintenance role, but the combination of query sensitivity, timing, prior denial history, and weak protocol relationship produces a high-risk score. In this case, the framework recommends temporary denial, identity verification, and security review. The example shows how the AI layer can complement smart contracts by detecting patterns that are behavioral rather than merely legal.

The scenario analysis also clarifies how false positives and false negatives should be interpreted. A false positive is not only a statistical error; it may delay a legitimate clinical or research workflow. A false negative is more serious because it may expose sensitive genomic data beyond consent conditions. For this reason, the prototype favors high recall for high-risk access events and uses human review for borderline cases. This design accepts some reviewer workload in exchange for stronger privacy protection and greater patient trust.

From a biomedical engineering perspective, the decision-support interface should display five elements: the requested dataset, the active consent condition, the model risk score, the top explanation factors, and the recommended governance action. A reviewer should also be able to compare the current request with similar historical requests. This design turns the AI model into a practical governance assistant rather than a standalone authority. The final decision remains with the institutionally accountable reviewer except in cases where a hard smart-contract rule mandates rejection.

The prototype further shows that explanation stability is as important as prediction accuracy. If the model gives different explanations for similar cases, reviewers may lose confidence even when performance metrics remain high. The framework therefore monitors explanation drift by tracking whether the top-ranked factors for comparable access patterns remain consistent over time. Sudden shifts in explanation profiles can indicate model drift, policy changes, new attack patterns, or changes in requester behavior.

The proposed architecture can also support institutional benchmarking. Hospitals and biobanks can compare aggregate access-risk patterns without revealing patient data. For instance, a consortium may observe that cross-border requests have higher deferral rates or that certain purpose categories frequently require clarification. Differentially private reporting can turn these observations into governance dashboards while reducing exposure of individual-level access history. Such dashboards can guide staff training, consent-form revision, and data-sharing policy improvement.

Finally, the scenario analysis highlights why governance design must precede technology deployment. If consent categories are poorly defined, if institutional roles are ambiguous, or if data-sensitivity labels are inconsistent, even a technically strong AI-blockchain architecture will produce weak decisions. The quality of the framework depends on the quality of the governance ontology. Therefore, implementation should begin with multidisciplinary definition of data classes, access purposes, consent states, and escalation rules before model training or smart-contract deployment.

X. DISCUSSION AND IMPLICATIONS

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 2, No. 3 (2024), pp. 27–43
DOI: 10.63646/jaiaa.2024.020302

The findings support the argument that AI and blockchain are complementary. Blockchain contributes immutable governance records, shared provenance, decentralized auditability, and deterministic smart-contract enforcement. AI contributes contextual risk interpretation, anomaly detection, and explanation of non-obvious request patterns. Used separately, each technology has limitations. Blockchain without analytics can produce excellent records of poor decisions. AI without blockchain can produce predictions without trusted consent history or auditable provenance.

The framework also changes the role of patients. In many systems, patients provide consent once and then lose visibility into downstream reuse. A patient-centric system should support dynamic preferences, revocation, purpose restrictions, and understandable summaries. Blockchain can anchor consent-state changes, while AI can flag requests that deviate from those preferences. Patient-centric design, however, should not shift all responsibility to patients. Institutions remain responsible for explaining choices, preventing misuse, and ensuring fair access to the benefits of genomic research.

Theoretically, the article contributes a layered model of explainable genomic data governance. It clarifies the boundary between deterministic policy enforcement and probabilistic decision support. Practically, it recommends off-chain encrypted storage, permissioned blockchain governance, smart-contract consent rules, AI-based contextual risk scoring, human review of borderline cases, and explanation summaries written in governance language. This design can guide early-stage pilots before real patient data is introduced.

XI. LIMITATIONS AND FUTURE RESEARCH

The study has limitations. First, the empirical component uses scenario-based simulation rather than real institutional genomic access logs. Future research should validate the framework using de-identified access-event metadata under ethics approval. Second, the model evaluates access-risk detection rather than downstream clinical or research outcomes. Prospective studies should examine reviewer workload, patient trust, false-denial costs, false-approval harms, and the effect of explanations on decision quality.

Third, the framework assumes that institutions can agree on shared identity, consent, and data-sensitivity standards. In practice, such agreement is difficult because legal requirements differ by jurisdiction and consent categories may not align neatly with research purposes. Future work should develop ontology-based consent mapping, cross-jurisdictional policy translation, and formal verification of smart contracts. Additional research should also evaluate privacy-preserving mechanisms in operational genomic workflows rather than treating them as interchangeable safeguards.

XII. CONCLUSION

This article developed an AI-enhanced blockchain analytics framework for genomic data access control. It reframes blockchain-based bioinformatics security as an explainable and privacy-preserving biomedical decision-support problem. The architecture combines permissioned blockchain governance, smart-contract consent enforcement, off-chain encrypted genomic storage, zero-knowledge verification, and AI-based access-risk scoring. A scenario-based prototype suggests that the hybrid model can outperform rule-only and non-explainable baselines in detecting high-risk access events.

The main contribution is not only technical performance. The study shows how blockchain and AI can be organized into a layered governance infrastructure: blockchain preserves trust-critical state and auditability, while AI interprets contextual risk and provides explanations for human review. This design supports patient-centric control without placing raw genomic records on-chain and without relying on black-box automated decision-making.

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 2, No. 3 (2024), pp. 27–43
DOI: 10.63646/jaiaa.2024.020302

Acknowledgement

The authors acknowledge feedback from colleagues in health informatics, biomedical engineering, information systems, and data governance. The study is a design-science and scenario-based article and does not involve real patient data.

Funding

The authors received no financial support for the research, authorship, or publication of this article.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability

No patient-level genomic data were used. Prototype values and evaluation tables are based on scenario-based simulation for methodological demonstration.

Author Contributions

A.H.R. conceptualized the study and wrote the first draft. N.A.Z. developed the blockchain governance model. F.M.N. designed the biomedical privacy and consent components. K.T.W.M. prepared the AI analytics and explainability analysis. S.H.A. supervised the study and coordinated the final manuscript.

Use of AI Tools

Language editing and document-formatting support tools may have been used during manuscript preparation. All conceptual framing, technical interpretation, and final academic responsibility remain with the authors.

REFERENCES

Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 308-318). https://doi.org/10.1145/2976749.2978318

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolic, M., ... Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference. https://doi.org/10.1145/3190508.3190538

Aronson, S. J., & Rehm, H. L. (2015). Building the foundation for genomics in precision medicine. Nature, 526(7573), 336-342. https://doi.org/10.1038/nature15816

Ashley, E. A. (2016). Towards precision medicine. Nature Reviews Genetics, 17(9), 507-522. https://doi.org/10.1038/nrg.2016.86

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25-30). https://doi.org/10.1109/OBD.2016.11

Beaulieu-Jones, B. K., Wu, Z. S., Williams, C., Lee, R., Bhavnani, S. P., Byrd, J. B., & Greene, C. S. (2019). Privacy-preserving generative deep neural networks support clinical data sharing. Circulation: Cardiovascular Quality and Outcomes, 12(7), e005122. https://doi.org/10.1161/CIRCOUTCOMES.118.005122

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

Benchoufi, M., & Ravaud, P. (2017). Blockchain technology for improving clinical research quality. Trials, 18(1), 335. https://doi.org/10.1186/s13063-017-2035-z

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. In 2014 IEEE Symposium on Security and Privacy (pp. 459-474). https://doi.org/10.1109/SP.2014.36

Bodenreider, O. (2004). The Unified Medical Language System (UMLS): Integrating biomedical terminology. Nucleic Acids Research, 32(Database issue), D267-D270. https://doi.org/10.1093/nar/gkh061

Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., Ramage, D., Segal, A., & Seth, K. (2017). Practical secure aggregation for privacy-preserving machine learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1175-1191). https://doi.org/10.1145/3133956.3133982

Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., & Maxwell, G. (2018). Bulletproofs: Short proofs for confidential transactions and more. In 2018 IEEE Symposium on Security and Privacy (pp. 315-334). https://doi.org/10.1109/SP.2018.00020

Bycroft, C., Freeman, C., Petkova, D., Band, G., Elliott, L. T., Sharp, K., Motyer, A., Vukcevic, D., Delaneau, O., O'Connell, J., Cortes, A., Welsh, S., Young, A., Effingham, M., McVean, G., Leslie, S., Allen, N., Donnelly, P., & Marchini, J. (2018). The UK Biobank resource with deep phenotyping and genomic data. Nature, 562(7726), 203-209. https://doi.org/10.1038/s41586-018-0579-z

Char, D. S., Shah, N. H., & Magnus, D. (2018). Implementing machine learning in health care-addressing ethical challenges. New England Journal of Medicine, 378(11), 981-983. https://doi.org/10.1056/NEJMp1714229

Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Y. (2024). Applications of blockchain in Industry 4.0: A review. Information Systems Frontiers, 26(5), 1715-1729. https://doi.org/10.1007/s10796-022-10248-7

Cho, H., Wu, D. J., & Berger, B. (2018). Secure genome-wide association analysis using multiparty computation. Nature Biotechnology, 36(6), 547-551. https://doi.org/10.1038/nbt.4108

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

Collins, F. S., & Varmus, H. (2015). A new initiative on precision medicine. New England Journal of Medicine, 372(9), 793-795. https://doi.org/10.1056/NEJMp1500523

Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K.-L. (2018). Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering, 30(7), 1366-1385. https://doi.org/10.1109/TKDE.2017.2781227

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (pp. 618-623). https://doi.org/10.1109/PERCOMW.2017.7917634

Dwork, C. (2006). Differential privacy. In Automata, Languages and Programming (pp. 1-12). Springer. https://doi.org/10.1007/11787006_1

Erlich, Y., & Narayanan, A. (2014). Routes for breaching and protecting genetic privacy. Nature Reviews Genetics, 15(6), 409-421. https://doi.org/10.1038/nrg3723

Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K.-K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing, 5(1), 31-37. https://doi.org/10.1109/MCC.2018.011791712

Esteva, A., Robicquet, A., Ramsundar, B., Kuleshov, V., DePristo, M., Chou, K., Cui, C., Corrado, G., Thrun, S., & Dean, J. (2019). A guide to deep learning in healthcare. Nature Medicine, 25(1), 24-29. https://doi.org/10.1038/s41591-018-0316-z

Fredrikson, M., Jha, S., & Ristenpart, T. (2015). Model inversion attacks that exploit confidence information and basic

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

countermeasures. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 1322-1333). https://doi.org/10.1145/2810103.2813677

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 3-16). https://doi.org/10.1145/2976749.2978341

Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. SIAM Journal on Computing, 18(1), 186-208. https://doi.org/10.1137/0218012

Gordon, W. J., & Catalini, C. (2018). Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. Computational and Structural Biotechnology Journal, 16, 224-230. https://doi.org/10.1016/j.csbj.2018.06.003

Gymrek, M., McGuire, A. L., Golan, D., Halperin, E., & Erlich, Y. (2013). Identifying personal genomes by surname inference. Science, 339(6117), 321-324. https://doi.org/10.1126/science.1229566

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences-A scoping review. International Journal of Medical Informatics, 134, 104040. https://doi.org/10.1016/j.ijmedinf.2020.104040

Hitaj, B., Ateniese, G., & Perez-Cruz, F. (2017). Deep models under the GAN: Information leakage from collaborative deep learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 603-618). https://doi.org/10.1145/3133956.3134012

Homer, N., Szelinger, S., Redman, M., Duggan, D., Tembe, W., Muehling, J., Pearson, J. V., Stephan, D. A., Nelson, S. F., & Craig, D. W. (2008). Resolving individuals contributing trace amounts of DNA to highly complex mixtures using high-density SNP genotyping microarrays. PLoS Genetics, 4(8), e1000167. https://doi.org/10.1371/journal.pgen.1000167

Hripcsak, G., & Albers, D. J. (2013). Next-generation phenotyping of electronic health records. Journal of the American Medical Informatics Association, 20(1), 117-121. https://doi.org/10.1136/amiajnl-2012-001145

Humbert, M., Ayday, E., Hubaux, J.-P., & Telenti, A. (2015). Reconciling utility with privacy in genomics. In Proceedings of the 13th Workshop on Privacy in the Electronic Society (pp. 11-20). https://doi.org/10.1145/2808138.2808145

Johnson, A. E. W., Pollard, T. J., Shen, L., Lehman, L.-W. H., Feng, M., Ghassemi, M., Moody, B., Szolovits, P., Celi, L. A., & Mark, R. G. (2016). MIMIC-III, a freely accessible critical care database. Scientific Data, 3, 160035. https://doi.org/10.1038/sdata.2016.35

Kahn, M. G., Callahan, T. J., Barnard, J., Bauck, A. E., Brown, J., Davidson, B. N., Estiri, H., Goerg, C., Holve, E., Johnson, S. G., Liaw, S.-T., Hamilton-Lopez, M., Meeker, D., Ong, T. C., Ryan, P., Shang, N., Weiskopf, N. G., Weng, C., Zozus, M. N., & Schilling, L. (2016). A harmonized data quality assessment terminology and framework for the secondary use of electronic health record data. eGEMs, 4(1), 1244. https://doi.org/10.13063/2327-9214.1244

Kaissis, G. A., Makowski, M. R., Rückert, D., & Braren, R. F. (2020). Secure, privacy-preserving and federated machine learning in medical imaging. Nature Machine Intelligence, 2(6), 305-311. https://doi.org/10.1038/s42256-020-0186-1

Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira, R. G. L., Eichner, H., El Rouayheb, S., Evans, D., Gardner, J., Garrett, Z., Gascón, A., Ghazi, B., Gibbons, P. B., ... Zhao, S. (2021). Advances and open problems in federated learning. Foundations and Trends in Machine Learning, 14(1-2), 1-210. https://doi.org/10.1561/2200000083

Kalia, S. S., Adelman, K., Bale, S. J., Chung, W. K., Eng, C., Evans, J. P., Herman, G. E., Hufnagel, S. B., Klein, T. E., Korf, B. R., McKelvey, K. D., Ormond, K. E., Richards, C. S., Vlangos, C. N., Watson, M., Martin, C. L., & Miller, D. T. (2017). Recommendations for reporting of secondary findings in clinical exome and genome sequencing, 2016 update. Genetics in Medicine, 19(2), 249-255. https://doi.org/10.1038/gim.2016.190

Kelly, C. J., Karthikesalingam, A., Suleyman, M., Corrado, G., & King, D. (2019). Key challenges for delivering clinical impact with artificial intelligence. BMC Medicine, 17, 195. https://doi.org/10.1186/s12916-019-1426-2

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

Karczewski, K. J., Francioli, L. C., Tiao, G., Cummings, B. B., Alföldi, J., Wang, Q., Collins, R. L., Laricchia, K. M., Ganna, A., Birnbaum, D. P., Gauthier, L. D., Brand, H., Solomonson, M., Watts, N. A., Rhodes, D., Singer-Berk, M., England, E. M., Seaby, E. G., Kosmicki, J. A., ... MacArthur, D. G. (2020). The mutational constraint spectrum quantified from variation in 141,456 humans. Nature, 581(7809), 434-443. https://doi.org/10.1038/s41586-020-2308-7

Khera, A. V., Chaffin, M., Aragam, K. G., Haas, M. E., Roselli, C., Choi, S. H., Natarajan, P., Lander, E. S., Lubitz, S. A., Ellinor, P. T., & Kathiresan, S. (2018). Genome-wide polygenic scores for common diseases identify individuals with risk equivalent to monogenic mutations. Nature Genetics, 50(9), 1219-1224. https://doi.org/10.1038/s41588-018-0183-z

Kohane, I. S. (2015). Ten things we have to do to achieve precision medicine. Science, 349(6243), 37-38. https://doi.org/10.1126/science.aab1328

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In 2016 IEEE Symposium on Security and Privacy (pp. 839-858). https://doi.org/10.1109/SP.2016.55

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220. https://doi.org/10.1093/jamia/ocx068

Landrum, M. J., Lee, J. M., Benson, M., Brown, G. R., Chao, C., Chitipiralla, S., Gu, B., Hart, J., Hoffman, D., Hoover, J., Jang, W., Katz, K., Ovetsky, M., Riley, G., Sethi, A., Tully, R., Villamarin-Salomon, R., Rubinstein, W., & Maglott, D. R. (2018). ClinVar: Improving access to variant interpretations and supporting evidence. Nucleic Acids Research, 46(D1), D1062-D1067. https://doi.org/10.1093/nar/gkx1153

Lu, Y. (2018). Blockchain and the related issues: A review of current research topics. Journal of Management Analytics, 5(4), 231-255. https://doi.org/10.1080/23270012.2018.1516523

Lu, Y. (2019a). Artificial intelligence: A survey on evolution, models, applications and future trends. Journal of Management Analytics, 6(1), 1-29. https://doi.org/10.1080/23270012.2019.1570365

Lu, Y. (2019b). The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 15, 80-90. https://doi.org/10.1016/j.jii.2019.04.002

Lu, Y. (2021). Technological innovation and the emergence of a new interdisciplinary field: Management Analytics. Nanotechnologies in Construction, 13(3), 181-192. https://doi.org/10.15828/2075-8545-2021-13-3-181-192

Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 1876-1907. https://doi.org/10.1080/17517575.2021.2008513

Lu, Y. (2025). The current status and developing trends of Industry 4.0: A review. Information Systems Frontiers, 27(1), 215-234. https://doi.org/10.1007/s10796-021-10221-w

Mandel, J. C., Kreda, D. A., Mandl, K. D., Kohane, I. S., & Ramoni, R. B. (2016). SMART on FHIR: A standards-based, interoperable apps platform for electronic health records. Journal of the American Medical Informatics Association, 23(5), 899-908. https://doi.org/10.1093/jamia/ocv189

Mandl, K. D., & Kohane, I. S. (2016). No small change for the health information economy. New England Journal of Medicine, 375(6), 680-681. https://doi.org/10.1056/NEJMp1601381

Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous distributed E-cash from Bitcoin. In 2013 IEEE Symposium on Security and Privacy (pp. 397-411). https://doi.org/10.1109/SP.2013.34

Miotto, R., Wang, F., Wang, S., Jiang, X., & Dudley, J. T. (2018). Deep learning for healthcare: Review, opportunities and challenges. Briefings in Bioinformatics, 19(6), 1236-1246. https://doi.org/10.1093/bib/bbx044

Naveed, M., Ayday, E., Clayton, E. W., Fellay, J., Gunter, C. A., Hubaux, J.-P., Malin, B. A., & Wang, X. (2015). Privacy in the genomic era. ACM Computing Surveys, 48(1), 1-44. https://doi.org/10.1145/2767007

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

RESEARCH ARTICLE
Vol. 2, No. 3 (2024), pp. 27–43
DOI: 10.63646/jaiaa.2024.020302

Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2), 1184-1195. https://doi.org/10.1109/JIOT.2018.2812239

Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. Computer Networks, 112, 237-262. https://doi.org/10.1016/j.comnet.2016.11.007

Rajkomar, A., Dean, J., & Kohane, I. (2019). Machine learning in medicine. New England Journal of Medicine, 380(14), 1347-1358. https://doi.org/10.1056/NEJMra1814259

Raisaro, J. L., Tramèr, F., Ji, Z., Bu, D., Zhao, Y., Carey, K., Lloyd, D., Sofia, H., Baker, D., Flicek, P., Shringarpure, S., Bustamante, C. D., Wang, S., Jiang, X., & Hubaux, J.-P. (2018). Protecting privacy and security of genomic data in i2b2 with homomorphic encryption and differential privacy. BMC Medical Genomics, 11(Suppl 4), 30. https://doi.org/10.1186/s12920-018-0395-1

Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., Bakas, S., Galtier, M. N., Landman, B. A., Maier-Hein, K., Ourselin, S., Sheller, M., Summers, R. M., Trask, A., Xu, D., Baust, M., & Cardoso, M. J. (2020). The future of digital health with federated learning. npj Digital Medicine, 3, 119. https://doi.org/10.1038/s41746-020-00323-1

Sheller, M. J., Edwards, B., Reina, G. A., Martin, J., Pati, S., Kotrotsou, A., Milchenko, M., Xu, W., Marcus, D., Colen, R. R., & Bakas, S. (2020). Federated learning in medicine: Facilitating multi-institutional collaborations without sharing patient data. Scientific Reports, 10, 12598. https://doi.org/10.1038/s41598-020-69250-1

Shickel, B., Tighe, P. J., Bihorac, A., & Rashidi, P. (2018). Deep EHR: A survey of recent advances in deep learning techniques for electronic health record analysis. IEEE Journal of Biomedical and Health Informatics, 22(5), 1589-1604. https://doi.org/10.1109/JBHI.2017.2767063

Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 1310-1321). https://doi.org/10.1145/2810103.2813687

Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership inference attacks against machine learning models. In 2017 IEEE Symposium on Security and Privacy (pp. 3-18). https://doi.org/10.1109/SP.2017.41

Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography, 3(1), 3. https://doi.org/10.3390/cryptography3010003

Sudlow, C., Gallacher, J., Allen, N., Beral, V., Burton, P., Danesh, J., Downey, P., Elliott, P., Green, J., Landray, M., Liu, B., Matthews, P., Ong, G., Pell, J., Silman, A., Young, A., Sprosen, T., Peakman, T., & Collins, R. (2015). UK Biobank: An open access resource for identifying the causes of a wide range of complex diseases of middle and old age. PLoS Medicine, 12(3), e1001779. https://doi.org/10.1371/journal.pmed.1001779

Topol, E. J. (2019). High-performance medicine: The convergence of human and artificial intelligence. Nature Medicine, 25(1), 44-56. https://doi.org/10.1038/s41591-018-0300-7

Torkamani, A., Wineinger, N. E., & Topol, E. J. (2018). The personal and clinical utility of polygenic risk scores. Nature Reviews Genetics, 19(9), 581-590. https://doi.org/10.1038/s41576-018-0018-x

Vazirani, A. A., O'Donoghue, O., Brindley, D., & Meinert, E. (2020). Implementing blockchains for efficient health care: Systematic review. Journal of Medical Internet Research, 22(2), e12439. https://doi.org/10.2196/12439

Vasey, B., Nagendran, M., Campbell, B., Clifton, D. A., Collins, G. S., Denaxas, S., Denniston, A. K., Faes, L., Geerts, B. F., Ibrahim, M., Liu, X., Mateen, B. A., Mathur, P., McCradden, M. D., Morgan, L., Ordish, J., Rogers, C., Saria, S., Ting, D. S. W., ... McCulloch, P. (2022). Reporting guideline for the early-stage clinical evaluation of decision support systems driven by artificial intelligence: DECIDE-AI. Nature Medicine, 28(5), 924-933. https://doi.org/10.1038/s41591-022-01772-6

Vayena, E., Blasimme, A., & Cohen, I. G. (2018). Machine learning in medicine: Addressing ethical challenges. PLoS Medicine, 15(11), e1002689. https://doi.org/10.1371/journal.pmed.1002689

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.

JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 2, No. 3 (2024), pp. 27–43
DOI: 10.63646/jaiaa.2024.020302

Warnat-Herresthal, S., Schultze, H., Shastry, K. L., Manamohan, S., Mukherjee, S., Garg, V., Sarveswara, R., Händler, K., Pickkers, P., Aziz, N. A., Ktena, S., Tran, F., Bitzer, M., Ossowski, S., Casadei, N., Herr, C., Petersheim, D., Behr, J., Kern, F., ... Schultze, J. L. (2021). Swarm Learning for decentralized and confidential clinical machine learning. Nature, 594(7862), 265-270. https://doi.org/10.1038/s41586-021-03583-3

Wiens, J., Saria, S., Sendak, M., Ghassemi, M., Liu, V. X., Doshi-Velez, F., Jung, K., Heller, K., Kale, D., Saeed, M., Ossorio, P. N., Thadaney-Israni, S., & Goldenberg, A. (2019). Do no harm: A roadmap for responsible machine learning for health care. Nature Medicine, 25(9), 1337-1340. https://doi.org/10.1038/s41591-019-0548-6

Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., da Silva Santos, L. B., Bourne, P. E., Bouwman, J., Brookes, A. J., Clark, T., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C. T., Finkers, R., ... Mons, B. (2016). The FAIR Guiding Principles for scientific data management and stewardship. Scientific Data, 3, 160018. https://doi.org/10.1038/sdata.2016.18

Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452-10473. https://doi.org/10.1109/JIOT.2021.3060508

Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 10(2), 1-19. https://doi.org/10.1145/3298981

Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224. https://doi.org/10.1016/j.jii.2021.100224

Zheng, X. R., & Lu, Y. (2022). Blockchain technology: Recent research and future trend. Enterprise Information Systems, 16(12), 1939895. https://doi.org/10.1080/17517575.2021.1939895

Liu, X., Rivera, S. C., Moher, D., Calvert, M. J., & Denniston, A. K. (2020). Reporting guidelines for clinical trial reports for interventions involving artificial intelligence: The CONSORT-AI extension. BMJ, 370, m3164. https://doi.org/10.1136/bmj.m3164

ISSN: 3067-7386 © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author. See: https://inatgi.in/index.php/jaiaa/index for more information.