Check for updates

Engineering Reports

WILEY

Engineering Reports Open Access

RESEARCH ARTICLE OPEN ACCESS

Fraud Detection in Privacy Preserving Health Insurance System Using Blockchain Technology

Md. Mazharul Islam[1] | Mubasshir Ahmed[1] | Rajesh Palit[1] | Mohammad Shahriar Rahman[2] | Salekul Islam[1]

[1]Department of Electrical and Computer Engineering, North South University, Dhaka, Bangladesh | [2]Department of Computer Science and Engineering, United International University, Dhaka, Bangladesh

Correspondence: Salekul Islam (salekul.islam@northsouth.edu)

Received: 9 February 2025 | **Revised:** 21 June 2025 | **Accepted:** 15 July 2025

Funding: This work was supported by the Institute for Advanced Research (IAR), United International University, and the Office of Research (OR), North South University, under Grant UIU-IAR-02-2023-SE-41.

Keywords: anonymity | blockchain | fraud detection | health insurance claim | privacy preservation | smart contracts

ABSTRACT

In developed countries, around 90% of the population is covered by health insurance through public or private providers. However, fraudulent activities account for an estimated 3%–10% of total healthcare expenditures, resulting in financial losses exceeding $300 billion annually. These fraudulent practices erode trust among patients, healthcare providers, and insurers, further complicating the insurance claim process. Additionally, claim rejection rates due to fraudulent activities are estimated to range between 25% and 35%, which impacts its efficiency and trustworthiness and weakens the industry's reliability. The digitization of healthcare and the health insurance industry has amplified the need for robust and trustworthy systems that ensure data security and optimize the insurance claim process. To address these issues, this paper proposes a system that ensures patient anonymity through secure credentials and advanced fraud detection mechanisms. Privacy is preserved using cryptographic techniques such as secure hashing and anonymous credentials, which ensure that sensitive patient information remains confidential throughout the claim process. Smart contract algorithms are utilized in two scenarios: patient-submitted claims and healthcare provider-submitted claims, ensuring accurate processing and validation while detecting fraudulent activities such as duplicate claims, inflated medical bills, billing for unprovided services, falsifying patient records, and submitting claims for nonexistent treatments. The proposed system has been implemented and tested on a blockchain platform, demonstrating its effectiveness in preserving privacy and detecting fraud. Performance evaluations reveal its scalability and efficiency in managing increased user loads, offering a robust solution to modern health insurance challenges while fostering trust and operational efficiency among participants.

1 | Introduction

Maintaining good health and quality of life is essential for any human being. Healthcare systems ensure that everyone receives the necessary medical care and services to lead a healthy and quality life [1]. Proper and quality treatment is too expensive. Patients often face the challenge of managing the costs of treatments, medications, and necessary services including diagnostic tests, ultrasonography, and more. Health insurance providers step into help patients to face these challenges. With support from insurance service providers, patients are able to obtain medical services without significant financial pressure. Health insurance service providers are also beneficial from this [2]. The relationship between patients, healthcare providers, and

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2025 The Author(s). *Engineering Reports* published by John Wiley & Sons Ltd.

insurance companies forms the backbone of an operational and stable healthcare system, promoting both health services and economic growth.

The healthcare industry has been digitized over time. However, the increasing digitization of healthcare has brought new challenges, particularly in terms of protecting patient privacy. Sharing patient's private data and medical information with health insurance companies is essential for patients to obtain care and submit insurance claim [3] Concerns arise regarding the management, storage, and sharing of data. Ensuring patient anonymity plays a key role in protecting against breaches, identity theft, and unauthorized viewing of medical histories [4]. As healthcare data is highly personal, it is important to create systems that not only protect this information but also ensure that it is used securely and appropriately [5].

In addition to privacy concerns, healthcare insurance fraud has become a major issue, and the financial impact of healthcare fraud is staggering, costing the industry billions of dollars annually [6]. In developed nations, nearly 90% of individuals have access to health insurance, either through public programs or private providers [7], fraudulent activities account for an estimated 3%–10% of total healthcare expenditures [8]. The U.S. healthcare system, in particular, faces annual losses ranging from $505 billion to $850 billion, representing 9% to 19% of total healthcare spending [9]. Other regions, such as Europe and Asia, also face substantial healthcare fraud. In Southeast Asia, countries like Indonesia, Malaysia, and Singapore encounter similar challenges, with Indonesia's insuring around 89% of its population, yet still grappling with significant fraud issues that add to the financial strain on the public healthcare system [10]. These fraudulent practices not only result in financial losses exceeding $300 billion annually but also erode trust among patients, healthcare providers, and insurers, further complicating the insurance claim process. Additionally, claim rejection rates due to fraudulent activities are estimated to range between 25% and 35%, significantly impacting the efficiency and trustworthiness of the system and weakening the industry's overall reliability [11]. This places a financial burden on patients, who end up paying more due to the increased costs associated with fraudulent claims. Health insurance claims have been settled through manual reviews and audits [12]. To complete the insurance claims settlement process, patients need to submit claims with supporting documents, which are verified by insurance service providers. However, this manual approach is inefficient because of its time-consuming nature. Moreover, manual processes are limited in their ability to detect complex patterns of fraud, making them ineffective in addressing the growing challenges in the insurance industry [13].

The health insurance claim process faces a major issue due to fraudulent activities, which can be initiated by patients, healthcare service providers, or even health insurance providers [14]. Fraudulent activities weaken the integrity of the system. Patients try to exploit the weakened system by submitting false claims, healthcare providers inflate charges, and insurance providers unfairly deny valid claims. Existing systems for addressing these issues rely on rule-based engines and data-driven approaches to detect suspicious activities and ensure compliance. Privacy preservation methods typically involve encryption, access controls, and centralized databases to protect sensitive data [15]. While these systems provide some level of effectiveness, they often fail to address the dual challenges of privacy and fraud simultaneously. Furthermore, centralized systems remain vulnerable to breaches and manipulation, posing risks to patient confidentiality and eroding trust among stakeholders [16]. This underscores the need for more secure and integrated solutions.

Blockchain technology offers an innovative solution to these challenges by providing a decentralized, immutable ledger for recording transactions [17]. In the context of health insurance claims, blockchain ensures that patient data and claim records are tamper-proof, enhancing transparency and accountability across stakeholders. Its decentralized and cryptographically secured architecture has demonstrated transformative potential across sectors, including education, finance, and healthcare, by offering tamper-resistance and trust without intermediaries [18]. For example, blockchain has been effectively used in enterprise management systems to improve transparency, data security, and operational efficiency, as demonstrated by the BAIoT-EMS system, which integrates blockchain and augmented intelligence for managing small and medium-sized enterprises [19]. By integrating smart contracts, the system can automate the claim verification process and enforce predefined rules to detect and prevent fraudulent activities. As a decentralized approach, blockchain mitigates the risks associated with centralized systems, addressing both privacy concerns and fraud detection effectively [20].

Although blockchain and smart contracts provide a decentralized and immutable framework, they often lack the mechanisms to fully preserve patient anonymity and detect complex frauds across multiple entities. These limitations hinder their ability to address the dual challenges of privacy preservation and fraud prevention comprehensively. Additionally, existing systems rarely support seamless collaboration among multiple insurance providers, further complicating the insurance claim process. In such scenarios, innovative consensus mechanisms like B-LPoET offer an efficient solution by utilizing lightweight multithreading to reduce computational overhead and enhance transaction throughput [21].

This paper proposes a comprehensive solution to address the dual challenges of privacy preservation and fraud detection in health insurance claims. The proposed model enables both patients and healthcare providers to submit claims securely, ensuring patient anonymity while effectively detecting fraudulent activities. Figure 1 illustrates the architecture of the proposed privacy-preserving and fraud-resistant health insurance claim system. The model supports two parallel scenarios: patients and healthcare providers can both submit insurance claims.

To preserve privacy, the system ensures that patients' medical data remains anonymous from health insurance providers during the claim process. This is achieved using SHA-256-based anonymous credentials, which allow sensitive information to be encrypted and anonymized while enabling claim validation without revealing the underlying medical data. By maintaining anonymity, the system safeguards patient privacy and ensures compliance with data protection requirements. For fraud

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

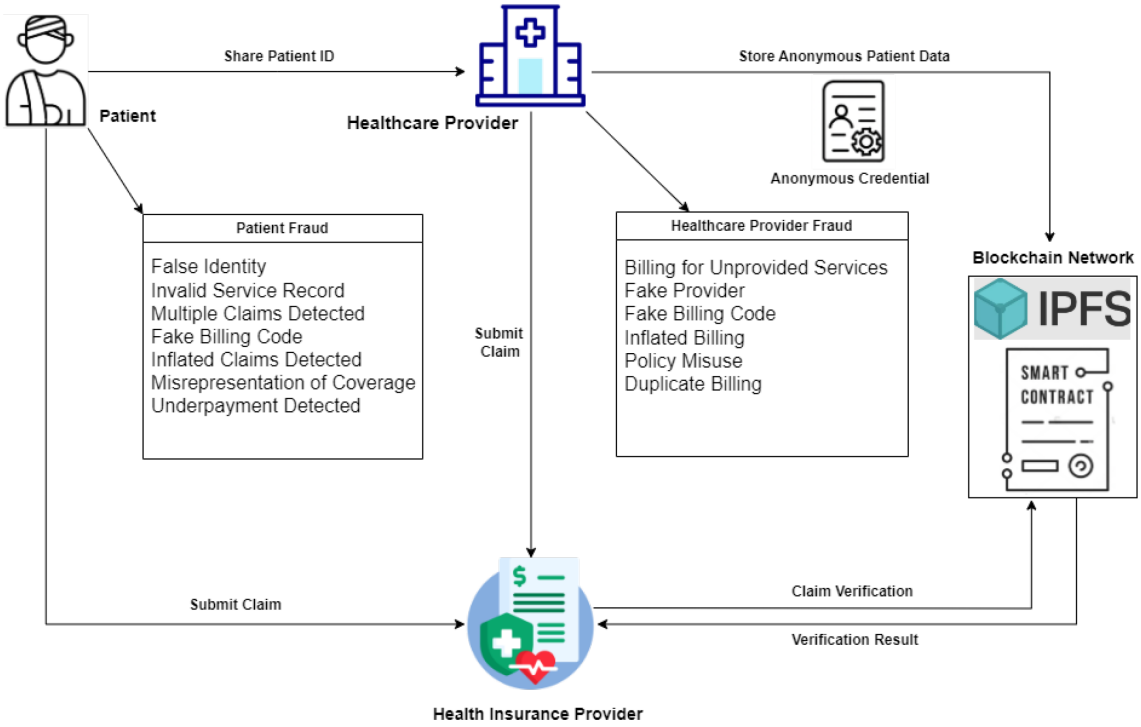

FIGURE 1 | Architecture of the proposed privacy-preserving and fraud-detection-enabled health insurance claim system.

detection, the model identifies activities such as false identity, duplicate claims, inflated charges, and policy misuse and so forth. Smart contract algorithms automate the validation of claims, enforcing predefined rules to analyze both patient-submitted and healthcare provider-submitted claims. These mechanisms provide transparency and accountability across all participants without compromising privacy. This approach not only addresses the critical need for privacy preservation but also fosters trust within the health insurance ecosystem. By enabling seamless interactions among patients, healthcare providers, and multiple insurance providers, the system offers a scalable and efficient solution to modern health insurance challenges. The key contributions and highlights of this paper are summarized as follows:

- **Privacy Preservation:** The proposed system ensures the anonymity of patient data through the use of anonymous credentials and secure hashing techniques, safeguarding sensitive information from unauthorized access and ensuring that patient privacy is maintained throughout the claim process.
- **Fraud Detection:** By using smart contracts, the system automates the detection and prevention of fraudulent activities, addressing misconduct from both patients and healthcare providers. The system effectively identifies and mitigates fraud scenarios such as duplicate claims, inflated charges, and policy misuse.
- **Integration with Multiple Insurers:** The system enables smooth interactions among patients, healthcare providers, and multiple health insurance providers, ensuring scalability, flexibility, and efficient management of insurance claims across diverse entities.
- **Implementation of Proposed Model:** The proposed model has been implemented on the Hyperledger fabric platform. Sensitive data from patients are securely stored in decentralized InterPlanetary File System (IPFS). A web-based user interface is also developed to interact with the blockchain platform, for example, submitting insurance claims. A detailed performance evaluation is also carried out to demonstrate the scalability of the solution.

The remainder of this paper is structured as follows: Section 2 discusses the foundational concepts and technologies used, focusing on privacy-preserving patient data, anonymous credentials, and common frauds in health insurance claims. Section 3 reviews the existing literature, categorizing studies on fraud detection, privacy-preserving techniques, and combined approaches. Section 4 outlines the proposed model, explaining its key components and methodology, including threat modeling, claim submission scenarios, and fraud detection mechanisms. Section 5 details the system implementation, highlighting the technologies used and the working process. Section 6 evaluates the system's performance through metrics such as data writing, claim validation, and fraud detection. Finally, Section 8 concludes the paper, summarizing contributions and proposing directions for future work.

2 | Preliminaries

The preliminaries section provides foundational concepts and necessary definitions for understanding data privacy preservation and fraud detection mechanisms in the healthcare insurance claim settlement process. The primary goal is to ensure the anonymity of the patient, preserve the privacy of the data, and

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

address the various forms of fraud that can occur during the claims process.

2.1 | Privacy-Preserving Patient Data

In today's modern healthcare system, ensuring the protection of patient data is a top priority [22]. When patients submit claims to insurers, they are often required to share a significant amount of personal and medical information, including details about their diagnoses, treatments, and other identifying data. This information, while necessary for claim verification and processing, is highly sensitive and, if improperly managed, poses substantial privacy risks. The need for healthcare providers and insurers to access this data creates multiple touch points where information can potentially be exposed, leading to a heightened risk of unauthorized access, data breaches, and misuse of sensitive personal data [23].

The current practice of sharing detailed medical information with insurers highlights the limitations in traditional privacy-preserving methods, which often do not account for the complexities of healthcare data exchange. Once data leaves the hands of healthcare providers, patients lose control over how it is stored, accessed, and used, especially as it passes through various intermediaries [24]. Therefore, there is an urgent need for advanced privacy-preserving mechanisms that minimize the extent of data shared and restrict access strictly to authorized entities. Techniques like data anonymization, encryption, and the use of decentralized systems such as blockchain and IPFS offer promising solutions. These technologies can help ensure that only essential information is shared, enhancing the security of patient data while still allowing insurers to perform necessary validations [25].

2.2 | Anonymous Credentials for Patient Privacy

To protect patient privacy in healthcare systems, ensuring anonymity is essential, especially when sensitive information is shared with multiple parties [26]. In this research, we aim to keep the identity of patients anonymous during health insurance claims, allowing only necessary data to be used for verification without revealing personal details. To achieve this, we utilize the SHA-256 algorithm, a secure hashing technique that transforms data into a unique, fixed-length string of characters.

The SHA-256 algorithm [27] is widely used for its security and reliability. When patient data are processed through SHA-256, it is converted into an irreversible hash that cannot be traced back to the original information. This means that while the health insurance provider can verify the authenticity of the data, the actual details of the patient's identity remain hidden. By using SHA-256, we ensure that patient information remains confidential, as only hashed data are shared, providing a layer of privacy that protects patients' identities even as their claims are processed [28]. This approach helps build a secure, privacy-preserving system where patients can confidently interact with healthcare and insurance providers without compromising their personal information.

2.3 | Frauds in Health Insurance Claims

Fraud detection in health insurance claims involves identifying and preventing deceptive activities that lead to wrongful financial gains by exploiting the insurance system [29]. Health insurance fraud can be perpetrated by various entities, including patients, healthcare providers, or even health insurance providers. These fraudulent activities not only result in substantial financial losses but also undermine trust in healthcare systems. Below are some common types of fraud in health insurance claims, categorized by the entities involved:

- **Patient Frauds**:
  1. Falsifying Medical Conditions: Patients misrepresent their health status to claim benefits or unnecessary treatments.
  2. Multiple Claims: Submitting multiple claims for the same treatment across different health insurance providers.
  3. Misrepresentation of Identity: Using another person's identity to access services or claim benefits.
  4. Inflated Claims: Exaggerating the severity of an illness or treatment needs for higher payouts.
  5. Policy Abuse: Patients misuse insurance policies, submitting claims that exceed policy limitations or using emergency services for minor ailments.
- **Healthcare Provider Frauds**:
  Billing for Unprovided Services: Charging insurers for services not rendered.
  Fake Patients: Creating fictitious patient records to bill insurers for fraudulent claims.
  Upcoding: Using inflated billing codes to claim reimbursement for more expensive services.
  Service Unbundling: Separately billing for services typically grouped into one procedure, increasing total claim amounts.
  Phantom Billing: Billing for services or items never provided to the patient.
  Self-Referral Fraud: Referring patients to services or entities in which the provider has a financial interest, increasing profits through unnecessary referrals.
- **Joint Frauds by Patients and Healthcare Providers**:
  Duplicate Billing: Colluding to submit multiple claims for the same service or procedure, either through different insurers or by modifying claim details.
  Fabricated Procedures: Performing unnecessary procedures or exaggerating treatment needs to claim higher reimbursements.
  Misrepresentation of Coverage: Misleading patients about their insurance coverage or submitting claims for services outside of coverage.
- **Health Insurance Provider Frauds**:
  Denying Legitimate Claims: Unjustifiably denying valid claims to avoid payouts, often citing minor discrepancies or documentation issues.

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Commission Fraud: Manipulating commissions or payments associated with claims for additional profit.

These categories illustrate various methods of fraud in health insurance claims, each requiring specific detection strategies. Understanding these fraud types can help healthcare systems and insurers implement more effective mechanisms to safeguard against fraud, protect patient privacy, and prevent financial losses.

3 | Literature Reviews

Research on privacy preservation and fraud detection in healthcare and insurance systems has made significant advancements, leveraging technologies like blockchain and cryptography to address the limitations of traditional methods. Below, key studies are reviewed, highlighting their contributions and relevance to the challenges of ensuring patient privacy and detecting fraud.

Chase and Lauter (2011) [30] introduced one of the earliest frameworks for an anonymous healthcare system. Their work focused on safeguarding patient privacy through advanced cryptographic techniques, enabling claim verification without revealing sensitive medical records. The proposed system utilized token-based authentication and delegated credentials to protect user identities while allowing secure data sharing for claim processing. This foundational study emphasized the importance of unlinkable transactions and privacy-preserving mechanisms, offering a model that influenced future research in healthcare data security. However, the reliance on token-based authentication and centralized trust introduced potential vulnerabilities to breaches and manipulation. This system did not address fraud detection, leaving a critical gap in its applicability to real-world healthcare systems.

Zhang et al. (2016) [31] expanded on this by proposing the Fairness-Aware and Privacy-Preserving protocol, a system designed to ensure secure online insurance calculations while maintaining user privacy. The protocol employed certificateless signcryption to prevent data leakage during communications and incorporated mechanisms to detect fraudulent user behavior. By addressing both privacy and fairness, the study demonstrated the potential for integrating cryptographic tools to enhance transparency and integrity in insurance systems. However, it focused solely on user honesty without addressing fraudulent activities originating from healthcare providers or insurers, limiting its scope. Additionally, the computational burden of signcryption could pose scalability challenges.

He et al. (2018) [32] focused on blockchain technology to improve transparency and privacy in health insurance claims. Their system incorporated attribute-based access control to ensure that only authorized parties could access sensitive patient information. The blockchain framework also automated claim verification through smart contracts, streamlining workflows and enhancing trust among stakeholders. While effective in regulating data access, the system did not provide comprehensive fraud detection mechanisms, especially for complex fraud patterns involving collusion between multiple stakeholders. Hirtan et al. (2019) [33] further extended blockchain applications in e-health by proposing a dual blockchain architecture. This system maintained patient anonymity through a public mainchain while providing flexible access control using a private sidechain. However, the reliance on trusted nodes for managing the private sidechain raised concerns about potential centralization and limited scalability in high-volume environments. Together, these studies showcased blockchain's potential to address data security and privacy challenges in decentralized environments.

Li et al. (2022) [34] proposed EHRChain, a blockchain-based electronic health record system that integrated attribute-based encryption (ABE) and homomorphic cryptosystems. This approach enabled secure medical data sharing while ensuring fine-grained access control and privacy protection. The system also supported dynamic permission updates, making it adaptable to various use cases. However, the computational overhead of homomorphic encryption could hinder its adoption in large-scale healthcare systems. Similarly, Al Omar et al. (2021) [35] designed a blockchain-enabled healthcare platform for smart cities, focusing on managing electronic medical records and insurance policies securely. Their work combined Ethereum blockchain with cryptographic tools to ensure transparency and scalability, addressing the challenges of managing large datasets in urban healthcare settings. While it effectively managed large datasets, the system's dependency on a public blockchain introduced latency and cost concerns, limiting its efficiency in real-time operations.

Al Nuaimi et al. (2022) [36] developed a blockchain system for automating prescription drug insurance claims, leveraging smart contracts and IPFS for efficient data storage, and retrieval. The system streamlined claim processing while maintaining confidentiality and data integrity. Although the system streamlined claim processing, it lacked robust privacy-preserving mechanisms to prevent data exposure during storage and retrieval. Al Amin et al. (2024) [37] introduced a blockchain-based multisignature claim processing system that enhanced transparency and minimized fraud in health insurance. By requiring multistakeholder approval for claims, the system ensured accountability and reduced the risk of fraudulent activities. However, the framework did not focus on fraud detection, leaving vulnerabilities in cases of malicious behavior by healthcare providers or insurers.

These studies collectively highlight the progress in creating privacy-preserving and fraud-resistant systems for healthcare and insurance. However, limitations such as insufficient fraud detection, scalability challenges, reliance on centralized components, and incomplete privacy preservation underscore the need for more robust solutions. Building on these advancements, the proposed model integrates comprehensive privacy-preserving mechanisms and fraud detection strategies to address these gaps, providing a secure, scalable, and efficient solution for modern health insurance systems.

Building on these foundational works, existing research can be categorized into three areas: fraud detection, privacy-preserving techniques, and combined approaches that address both fraud detection and privacy preservation in health insurance claims. Fraud detection focuses on identifying anomalies and irregularities in health insurance claims that can compromise the integrity of the system. Privacy-preserving techniques aim to

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

secure sensitive patient data using advanced security methods. Combined approaches integrate these aspects to create comprehensive systems.

Fraudulent activities in healthcare insurance claims are a significant concern, leading to substantial financial losses for insurance providers and increased costs for consumers. Numerous research efforts have been dedicated to developing robust systems to detect and mitigate such fraud. The existing literature highlights diverse methodologies, including machine learning, data mining, and blockchain-based solutions, to tackle this challenge.

Table 1 provides a detailed comparative analysis of these methodologies, including their objectives, techniques, results, and limitations. It offers a comprehensive overview of existing approaches, highlighting key advancements and areas for improvement in healthcare fraud detection systems.

The fraud detection category addresses healthcare insurance fraud using methods like anomaly detection, clustering, machine learning, and blockchain. These methodologies enhance fraud detection by improving data integrity, automating processes, and ensuring transparency. However, challenges such as scalability, computational demands, and integration with legacy systems persist. The reviewed studies underscore the need for scalable, efficient, and privacy-preserving solutions to effectively tackle fraud detection and data security. A closer examination of the reviewed methods reveals that prior studies often suffer from high class imbalance, limited dataset generalizability, computational overhead, and insufficient handling of rare fraud patterns, factors that restrict their practical deployment and underscore the need for more scalable, efficient, and privacy-aware solutions.

The increasing digitization of healthcare data has amplified concerns about patient privacy. Privacy-preserving techniques aim to secure sensitive medical information against unauthorized access while ensuring data usability for legitimate purposes [43]. Blockchain technology has emerged as a popular solution, offering a decentralized ledger that secures data integrity and enables patient-controlled access. Techniques such as self-sovereign identity (SSI) and ABE have also been explored to enhance access control and safeguard patient privacy.

Despite these advancements, privacy-preserving systems often face challenges related to scalability and integration. Blockchain-based solutions, for instance, are associated with high computational costs and latency, especially when applied to real-time healthcare systems. Similarly, techniques like secure multiparty computation (SMPC) are effective in ensuring data confidentiality but can become computationally expensive as the number of parties involved increases. Table 2 provides a detailed summary of recent advancements in privacy-preserving healthcare systems, highlighting the objectives, methodologies, technologies, and limitations of various studies.

Combining privacy-preserving techniques with fraud detection mechanisms has gained significant attention as a means to address the dual challenges of data security and fraudulent activity in healthcare insurance claims. Blockchain and smart contracts are often at the core of these integrated approaches, providing both a secure data-sharing platform and automated fraud detection capabilities. However, existing integrated approaches frequently encounter limitations, including high computational costs, increased latency during real-time processing, and implementation complexities, all of which restrict their widespread adoption.

Table 3 presents a comparative analysis of recent studies that integrate privacy-preserving techniques with fraud detection mechanisms in healthcare systems, including our proposed model. Prior research has made notable strides using advanced methodologies such as blockchain, machine learning, cryptographic algorithms, and smart contracts, which have shown promise in mitigating healthcare insurance fraud while protecting patient privacy. Nevertheless, most existing approaches tend to focus on either fraud detection or privacy preservation in isolation. The limited number of integrated solutions often face significant challenges, including high computational overhead, limited scalability, and complex implementation.

Our proposed model addresses these limitations through a comprehensive framework that combines blockchain technology with IPFS-based decentralized storage, SHA-256-based anonymous credential generation, and smart contracts. This design ensures strong privacy preservation, efficient fraud detection, and enhanced scalability. The use of SHA-256 hashing and IPFS allows patient identities and sensitive medical data to remain anonymized and securely stored. Additionally, smart contracts automate the validation processes, minimizing manual intervention and improving the accuracy of fraud detection. Performance metrics have also been included to enable more effective benchmarking and facilitate a clearer comparison of each study's outcomes. Performance analysis further demonstrates the system's effectiveness, highlighting reduced latency, optimized resource utilization, and greater practicality for real-world deployment compared to existing solutions.

4 | Proposed Model

Our model integrates anonymity, blockchain, IPFS, and smart contracts to ensure secure and privacy-preserving healthcare insurance claims. The system involves three main entities: Patient, Healthcare Provider, and Health Insurance Provider. The focus of the model is to maintain the anonymity of patients while allowing both the patient and healthcare provider to submit claims to the insurance provider. Blockchain ensures that all interactions are transparent, immutable, and traceable, while IPFS secures off-chain storage of patient data. An overview of the roles of each entity, followed by detailed descriptions of the two scenarios: Claim by patient and claim by hospital are given below.

- Patient: The patient provides their Patient ID to the healthcare provider to receive services. In some cases, the patient can submit a claim directly to the insurance provider using a service token issued by the healthcare provider.
- Healthcare Provider: The healthcare provider generates an anonymous credential that includes the necessary details, such as the Patient ID, Service Token, and Timestamp, and stores this securely on the blockchain. The healthcare provider may also submit the claim on behalf of the patient.

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 1 | Comparative analysis of fraud detection techniques in healthcare insurance claims.

Ref.	Objective	Methodology	Studied parameters	Frauds covered	Results	Limitations
[38]	Detecting fraudulent activities using cost-sensitive learning for medical insurance claims.	Feature engineering based on temporal covariates with functional principal component analysis.	Medicare claims, class imbalance.	Upcoding, duplicate claims, phantom billing.	Cost-sensitive approach saved around 55% of potential fraud-related costs.	High class imbalance, limited generalization to non-Medicare claims.
[39]	Developing a big data-based model for early fraud detection in healthcare insurance.	Use of Recurrent Neural Networks (RNN) with hyperparameter optimization through Bayesian models.	Anomaly detection based on patient, claim, and provider.	Phantom billing, duplicate claims, billing for unprovided services.	Achieved 88.09% accuracy in detecting provider fraud, with improved precision and recall.	High computational cost and complexity, especially for large datasets.
[40]	Using data mining techniques to detect healthcare insurance fraud based on association rules and clustering.	Unsupervised learning: Association rule mining combined with classifiers like CBLOF, Isolation Forest.	Patient, service, provider interaction.	Billing for unprovided services, identity theft, overcharging.	CBLOF achieved the highest silhouette score (0.114), outperforming other anomaly detection algorithms.	Lower accuracy in unsupervised methods, difficulty handling outliers and rare fraud patterns.
[41]	Applying data-centric AI approaches to Medicare fraud detection using enriched datasets.	Medicare fraud classification with feature engineering, data labeling, cross-validation.	Medicare claims from Part B, D, DMEPOS datasets.	Upcoding, service unbundling, billing for unprovided services.	Enhanced fraud detection by adding 58 new features, improving performance over traditional datasets.	Potential overfitting when using enriched feature sets, privacy concerns in deanonymizing large datasets.
[42]	Efficient handling of data imbalance in health insurance fraud detection using meta-reinforcement learning.	Meta-RL using RL2 and VariBAD algorithms for imbalance mitigation.	Data imbalance, fraud ratio, task distribution.	Identity theft, duplicate claims, fraudulent billing.	Achieved high G-mean (98.99%) and F-measure (98.96%) for VariBAD at 10% imbalance.	High computational cost, sensitive to task distribution, scalability issues.

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 2 | Comparative analysis of privacy-preserving techniques in healthcare insurance claims.

Refs.	Objective	Methodology	Privacy mechanisms	Use cases	Results	Limitations
[44]	To design a privacy-preserving healthcare system using blockchain.	Hybrid blockchain model combining public and private chains.	Blockchain, Smart Contracts	Secure sharing of medical records, insurance claims.	Improved security and reduced fraud with patient control over data.	High computational cost.
[45]	To create a multi-authority access control system for healthcare data.	Attribute-Based Encryption, Secure Multiparty Computation.	Attribute-Based Encryption, Multiparty Computation	Access control for healthcare data sharing.	Enhanced access control with distributed data management.	Limited scalability for large datasets.
[46]	To develop an AI-driven machine learning approach for privacy-preserving fraud detection in US healthcare billing and insurance.	AI-driven machine learning with reinforcement learning for data security.	Differential Privacy, Federated Learning, Homomorphic Encryption.	Healthcare billing, insurance claims, risk management.	High accuracy in anomaly detection and reduced false positives.	High computational complexity, data imbalance sensitivity, high resource consumption.
[47]	To develop a high-security, privacy-preserving blockchain-based system for automating and managing laboratory health tests.	Open-source blockchain architecture with smart contracts, decentralized identity (DID) management.	Zero-Knowledge Proofs (ZKP), Homomorphic Encryption, Smart Contracts.	Laboratory test management, healthcare data privacy.	High security, privacy preservation, scalability.	High computational overhead, complex implementation, potential latency issues.
[48]	To ensure secure and privacy-preserving sharing of personal health records.	Self-Sovereign Identity (SSI), Secure Multi-party Computation (SMPC).	Secure Multi-party Computation, SSI	Secure health record sharing.	Secure access control and delegation of access rights.	High complexity in multiparty delegation.

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 3 | Comparative analysis of combined fraud detection and privacy-preserving techniques in healthcare insurance claims.

Refs.	Objective	Methodology	Privacy Mechanisms	Fraud detection Techniques	Frauds Covered	Performance Metrics	Contribution	Limitations
[49]	Detect insurance fraud with data privacy in medical claims.	Blockchain with TLS-N, Ethereum smart contracts.	PPDP, TLS-N with generalization.	Smart contracts for proof, authenticity verification.	Fake documents, identity theft, double billing.	Transaction Speed, Scalability, Data Integrity	Enhanced privacy, reduced fraudulent claims.	High computation, privacy challenges.
[50]	Analyze and propose AI & blockchain for fraud detection.	Blockchain with AI (supervised, unsupervised), smart contracts.	Encryption, pseudonymization, IPFS.	ML algorithms with blockchain for fraud detection.	Medical identity theft, policy abuse.	Accuracy, Real-time Detection, Computational Efficiency	Improved transparency, real-time detection.	Computational needs, legacy issues.
[51]	Develop federated learning-based system for privacy & fraud detection.	Federated Learning in fog-cloud; FL-BETS for fraud detection.	AES, SHA-256, local/global training.	Federated ML for fraud pattern recognition.	Identity fraud, double billing, overbilling.	Latency, Energy Efficiency, Accuracy, Fault Tolerance	Lower delay, energy use, higher accuracy.	Complexity, latency in networks.
[52]	Use smart contracts for fraud detection with blockchain platform selection.	Decision map for blockchain selection; smart contracts.	Smart contracts, private access, encryption.	Smart contract algorithms for fraud scenarios.	Commission fraud, billing manipulation.	Processing Efficiency, Fault Tolerance, Scalability	Optimized fraud detection, efficient processing.	Limited testing, data intensity.
[53]	Enhance fraud detection with provider profiling and labeling via MultiTree.	Weighted MultiTree for profiling; DAG-based WMT.	Anonymization in profiling, MultiTree.	MultiTree for profiling, community detection.	Duplicate billing, fabricated procedures.	Profiling Accuracy, Cost Efficiency, Scalability	Higher accuracy, reduced profiling costs.	Dependency on structured data.
Our Model	To provide comprehensive privacy preservation and fraud detection in health insurance claims.	Blockchain integrated with IPFS, Smart Contracts, and anonymous credential generation (SHA-256).	SHA-256 hashing, anonymous credentials, decentralized data storage (IPFS), encryption.	Smart contract-based rule enforcement, cross-validation of claims with blockchain-stored data.	Identity theft, billing fraud, inflated claims, duplicate claims, fake providers, policy misuse, underpayment, and so forth.	Measurement of Throughput, Latency, Resource Utilization	Effective fraud detection with robust privacy protection, improved scalability.	Higher latency observed with extremely large concurrent user loads, assumption of trusted healthcare providers.

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

- Health Insurance Provider: The insurance provider receives claims from either the patient or the healthcare provider and verifies them using smart contracts on the blockchain. Once verified, the insurance provider processes the payment if the claim is valid.

4.1 | Threat Model

The proposed system is designed to ensure patient anonymity. This approach ensures that no other entities, including the health insurance provider, can directly access or modify sensitive patient information. The healthcare provider generates anonymous credentials that encapsulate patient details in a secure, encrypted format, maintaining privacy throughout the claim process. Additionally, all communication between entities occurs through secure channels using SSL (Secure Sockets Layer) to prevent unauthorized access or tampering during data transmission [54].

In this system, we assume that there are no external attackers attempting to compromise its operations. This assumption simplifies the security requirements and enables a focused approach to managing risks originating from internal entities. The absence of external threats allows the system to emphasize secure communication and robust data handling mechanisms between the patient, the healthcare provider, and the health insurance provider.

However, internal attacks remain a significant concern, as dishonest behavior or fraud can originate from any of the entities involved [55]. Patients may misuse anonymous credentials to submit false or duplicate claims. Healthcare providers may attempt to fabricate claims for services not rendered or create fraudulent patient records. Similarly, health insurance providers can act unfairly by rejecting valid claims or manipulating claim processing.

4.2 | Security and Privacy

The proposed system is designed to ensure the following critical security and privacy properties:

- **Pseudonymity:** Patients in our system are identified through anonymous credentials. This ensures that actual identities remain hidden and that healthcare data cannot be associated with particular individuals without proper authorization.
- **Privacy:** Sensitive patient data are anonymized with cryptographic credentials, and are stored inside off-chain via IPFS, ensuring decentralized and tamper-resistant storage. Healthcare providers have access to full patient data during treatment, while health insurance providers only access anonymized claim data, preventing direct access to sensitive patient information. This separation ensures privacy throughout the claim verification process.
- **Integrity:** The system ensures data integrity by validating that patient information, service records, and claims remain consistent throughout the life cycle. Any modification or mismatch is flagged, ensuring that only original, unaltered data are accepted, reflecting the actual medical services provided.
- **Accountability:** Every transaction is recorded and traceable, ensuring that all interactions with patient data are traceable and auditable.
- **Security:** Data are stored securely to prevent any kind of unauthorized access or alteration.

4.3 | Claim Submission

The claim submission process in the proposed system is designed to ensure privacy, security, and efficiency. It facilitates interactions between patients, healthcare providers, and health insurance providers while maintaining the anonymity of sensitive patient data. The system supports two distinct scenarios for submitting claims: one where the patient directly submits the claim and another where the healthcare provider submits the claim on behalf of the patient. Both scenarios leverage blockchain and IPFS to securely store and manage data, and smart contracts to validate claims. Below, we describe each scenario in detail.

4.3.1 | Scenario 1: Submission of a Claim by the Patient

In this scenario, the patient takes the initiative to submit the insurance claim directly to the insurance provider. The healthcare provider acts as the intermediary by issuing a service token and creating an anonymous credential. This process ensures patient privacy and the legitimacy of the claim throughout the entire procedure. The claim of the patient is shown in Figure 2 and consists of the following steps:

1. Share Patient ID: The patient shares their Patient ID with the healthcare provider to receive healthcare services.
2. Service Token Issued: The healthcare provider generates a Service Token and provides it to the patient.
3. Anonymous Credential Creation: The healthcare provider creates an Anonymous Credential that includes the Patient ID, Hospital ID, Service Token, and a Timestamp. This credential is securely stored on the Blockchain Network using IPFS to ensure data privacy.
4. Store Data on Blockchain: The anonymous patient data are stored on the blockchain via IPFS, ensuring that patient identity is preserved while still providing access to required claim information.
5. Submit Claim: The patient submits a claim to the Health Insurance Provider using the Service Token provided earlier.
6. Claim Verification: The Health Insurance Provider verifies the claim by using smart contracts on the blockchain. The smart contract cross-checks the Service Token with the stored Anonymous Credential to validate the claim.

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

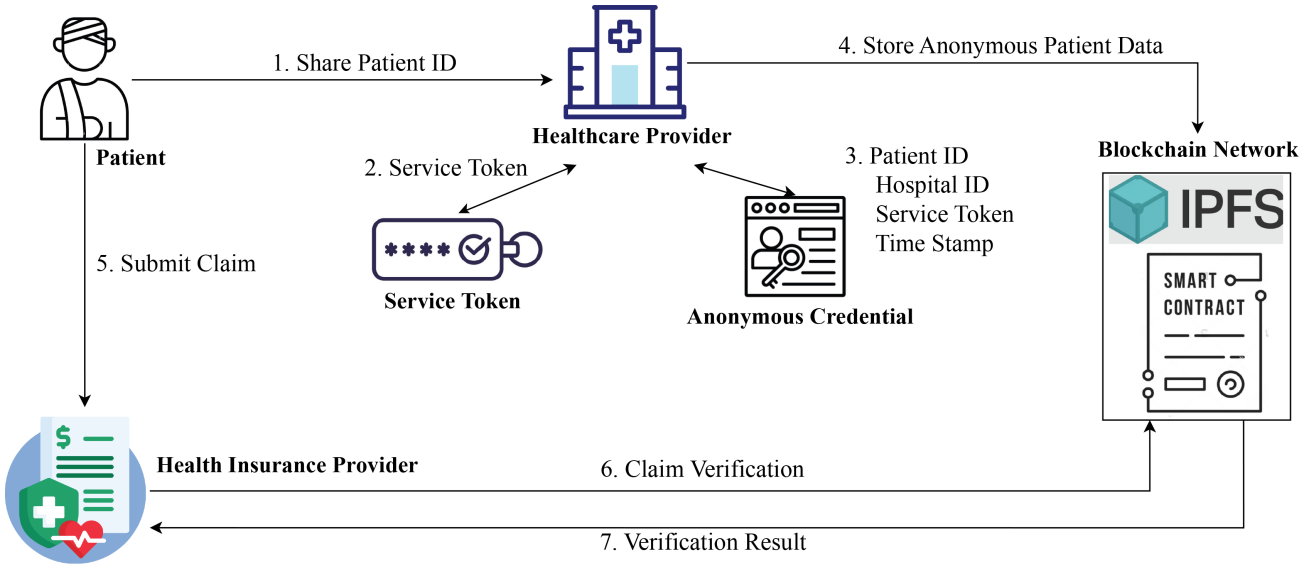

FIGURE 2 | Insurance claim submission by a patient to the insurance provider, where the healthcare provider issues a service token to the patient and creates and stores anonymous patient data to IPFS.

7. Verification Result: The verification result is sent back to the Health Insurance Provider, confirming whether the claim is legitimate.

4.3.2 | Scenario 2: Claim Submission by the Healthcare Provider

In this scenario, the healthcare provider submits the insurance claim on behalf of the patient. Although the overall process is similar to Scenario 1, the key difference lies in who initiates the claim submission. In this case, the healthcare provider assumes the responsibility of submitting the claim directly to the insurance provider, ensuring that the patient's data remain anonymous and the claim is processed efficiently. The process is depicted in Figure 3 and consists of the following steps:

1. Share Patient ID: As in Scenario 1, the patient shares their Patient ID with the healthcare provider to receive healthcare services.
2. Service Token Issued: The healthcare provider generates a Service Token for the patient.
3. Anonymous Credential Creation: The healthcare provider creates an Anonymous Credential containing the Patient ID, Hospital ID, Service Token, and Timestamp, which is stored on the Blockchain Network via IPFS.
4. Store Data on Blockchain: The anonymous data are recorded on the blockchain, ensuring that patient data remains private and immutable.
5. Submit Claim by Healthcare Provider: Instead of the patient submitting the claim, the healthcare provider submits the claim directly to the Health Insurance Provider using the stored anonymous credentials.
6. Claim Verification: The Health Insurance Provider verifies the claim by checking the Anonymous Credential stored on the blockchain through smart contracts.
7. Verification Result: Once the claim is verified, the result is sent back to the Health Insurance Provider, allowing them to proceed with payment if the claim is valid.

4.4 | Algorithms for the Smart Contracts

The proposed system incorporates two distinct models to address fraud detection and privacy preservation in health insurance claims: Scenario 1, which handles claims submitted directly by patients, and Scenario 2, which focuses on claims initiated by healthcare providers. At the core of both scenarios is the generation of an Anonymous Credential (AC), which ensures patient privacy by anonymizing sensitive data. The AC is created by hashing individual components such as the patient's unique identifier, the healthcare provider's identifier, the service token, and a timestamp, and then concatenating these hashes to produce a secure and irreversible credential. Each model employs a detailed algorithm integrated with blockchain and smart contracts, leveraging the AC to verify claims while protecting patient identity. Together, these scenarios create a comprehensive framework to detect fraudulent activities across different entities while preserving data privacy.

4.4.1 | Generation of Anonymous Credentials for Privacy Preservation

The anonymous credential plays a central role in the proposed system, ensuring privacy preservation and secure data handling during health insurance claims. By anonymizing sensitive information such as the patient's identifier, healthcare provider details, and service records, the anonymous credential safeguards personal data from unauthorized access or misuse. The credential is designed as a unique, irreversible identifier that links essential data components while maintaining anonymity. This approach is integrated seamlessly into the fraud detection and validation processes, enhancing both the security and privacy of the system.

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

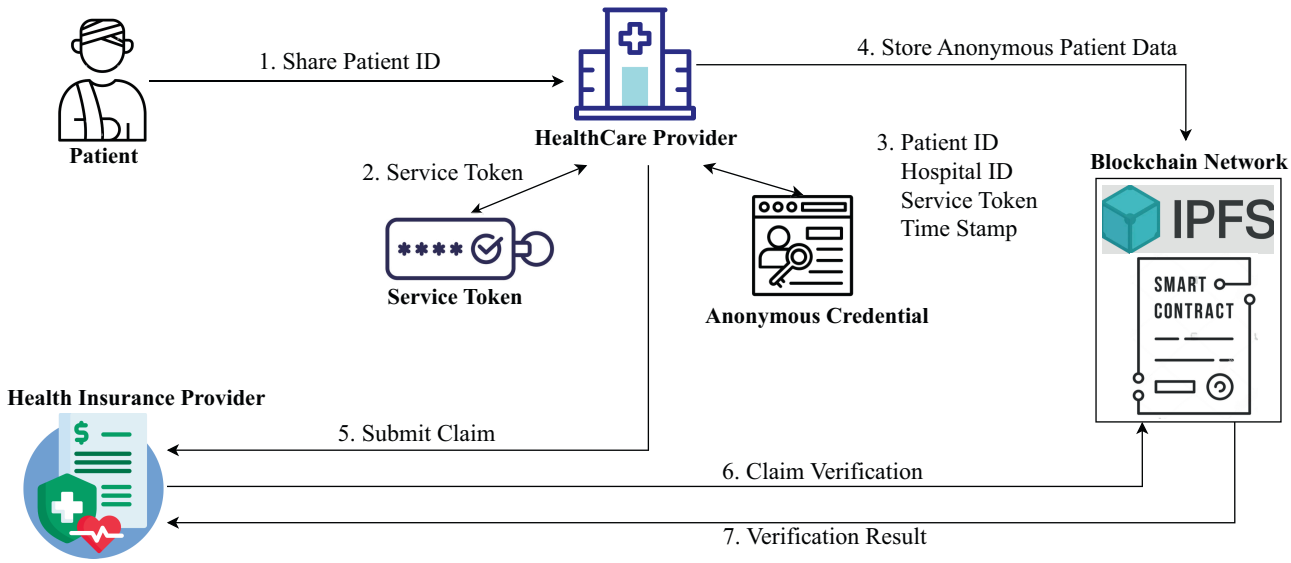

FIGURE 3 | Insurance claim submission by the healthcare provider to the insurance provider, where the healthcare provider creates a service token that is included in the insurance claim and anonymous patient data that is stored in IPFS.

ALGORITHM 1 | Anonymous credential generation.

Input: Patient_ID, Hospital_ID, Service_Token, Timestamp
Output: Anonymous Credential (AC)
Steps:
1: Compute individual hashes:
2: Patient_ID_Hash ← sha256Hash(Patient_ID)
3: Hospital_ID_Hash ← sha256Hash(Hospital_ID)
4: Service_Token_Hash ← sha256Hash(Service_Token)
5: Timestamp_Hash ← sha256Hash(Timestamp)
6: Concatenate the individual hashes:
7: AC ← Patient_ID_Hash + Hospital_ID_Hash + Service_Token_Hash + Timestamp_Hash
8: **return** Anonymous Credential (AC)

The generation algorithm for the anonymous credential is straightforward yet robust. It begins by hashing four critical data components: the patient identifier, healthcare provider identifier, service token, and timestamp, using the SHA-256 hashing algorithm. Each hash is unique and irreversible, ensuring the confidentiality of the original data. These hashes are then concatenated in a predefined order to create the final anonymous credential, which serves as a secure and anonymized link between patient data and claims. This process ensures data integrity and privacy while enabling efficient integration with blockchain storage and smart contract algorithms, which is shown in Algorithm 1.

The notation table defines the variables, arrays, and identifiers used in Scenario 1 and Scenario 2 algorithms, ensuring clarity and consistency. It outlines key components like patient and provider identifiers, billing codes, claim records, and insurance policy details. These notations link the algorithms to their data structures, enabling accurate claim validation and fraud detection. Table 4 serves as a reference, aligning the algorithmic processes with their described roles.

4.4.2 | Algorithm for Fraud Detection and Validation in Patient-Submitted Insurance Claims

Algorithm 2 outlines the step-by-step process for detecting and validating potential fraud in insurance claims submitted by patients. It leverages anonymous credentialing, smart contract-based verification, and blockchain-stored records to ensure claim legitimacy while preserving patient privacy. The algorithm performs a series of checks including identity verification, service validation, billing accuracy, policy compliance, and payment validation. Below is a detailed explanation of each phase of the algorithm:

The algorithm begins by initializing the claim process in lines 1–4. The patient's unique identifier (`Patient_ID`) is read and sent to the healthcare service provider (Line 1). The healthcare provider generates an *Anonymous Credential (AC)* using the `Patient_ID` and a `Service_Token` (Line 2). This credential acts as a pseudonym, ensuring the patient's identity is anonymized to protect privacy. These credentials, along with patient data, are securely stored on a blockchain network using IPFS and smart contracts (Line 3). Once the health insurance provider submits a claim referencing the AC (Line 4), the algorithm transitions to the fraud detection and validation phase.

The next step focuses on validating the patient's identity in lines 5–8. The algorithm retrieves the AC and reads the `Patient_Records (PRs[])` and `Service_Records (SRs[])` from the blockchain (Line 5). It checks whether the AC exists in the `Patient_Records` array (Line 6). If the AC is missing, the fraud is flagged as *False Identity or Misrepresentation of Identity* (Line 7). This ensures that the claim originates from a legitimate patient and prevents the use of stolen or fabricated credentials. If the AC passes this check, the algorithm moves on to validating the associated services.

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 4 | Notations used in scenario 1 and scenario 2 algorithms.

Notation	Description
`Patient_ID`	Unique identifier of the patient applying for insurance claims.
`Provider_ID`	Unique identifier of the healthcare provider.
`Service_Token`	Token provided by the healthcare service to validate services rendered.
`Timestamp`	Time at which the service or claim event occurred.
`Anonymous_Credential (AC)`	Credential generated by hashing identifiers for privacy preservation.
`Billing_Codes`	Codes representing the services or treatments provided.
`Claim_Record`	Record of the claim submitted by the patient or provider.
`Patient_Records (PRs[])`	Array of all patient-related records stored on the blockchain.
`Service_Records (SRs[])`	Array of all service-related records stored on the blockchain.
`Insurance_Policy (IP)`	Policy details including coverage and claim limits.
`Claimed_Amount`	Total monetary amount claimed by the patient or provider.
`Max_Coverage`	Maximum allowable coverage specified by the insurance policy.
`Paid_Amount`	Amount already paid by the insurance provider for the claim.
`Recalculated_Amount`	Amount recalculated based on valid billing codes and costs.
`IRs[]`	Array of valid insurance records for registered providers.

In lines 9–10, the algorithm verifies whether the AC exists in the `Service_Records (SRs[])` array. If the AC is not found (Line 9), the fraud is flagged as *Invalid Service Record (Billing for Unprovided Services)* (Line 10). This indicates that the patient is attempting to claim insurance benefits for services that were never rendered. These initial checks for identity and service validation are critical for filtering out fraudulent claims early in the process.

The algorithm evaluates the claim for duplication in lines 11–12. It checks the `Claim_Record` to verify whether the `Insurance_ID` is null (Line 11). If the `Insurance_ID` is not null, the fraud is flagged as *Multiple Claims Detected* (Line 12). This ensures that patients cannot submit duplicate claims for the same treatment across different insurance providers, safeguarding the system from repetitive misuse.

The algorithm performs detailed billing validation in lines 13–22. First, it verifies if the `Billing_Codes` in the claim exist in the `Patient_Records` (Line 13). If the codes are missing or invalid, the fraud is flagged as *Fake Billing Code* (Line 14). Next, the algorithm recalculates the total billing amount by extracting the `billingCode`, splitting it into service codes (`temp[]`), and summing up the costs (Lines 16–18). If the recalculated billing amount does not match the claimed amount, the fraud is flagged as *Inflated Claims Detected* (Line 19). These steps ensure that the claim reflects the actual services provided and prevents exaggerated or falsified billing.

In lines 23–33, the algorithm validates the insurance policy and payment details. It compares the `Claimed_Amount` with the `Max_Coverage` specified in the insurance policy (Line 23). If the claimed amount exceeds the allowed coverage, the fraud is flagged as *Misrepresentation of Coverage* (Line 24). It then verifies the `Paid_Amount` in the claim record (Line 28). If no payment has been made, the claim is approved as valid (Line 29). However, if the payment is less than the allowable coverage, the fraud is flagged as *Underpayment Detected* (Line 31). These final checks ensure that all claims adhere to policy terms and maintain fairness for all entities.

4.4.3 | Algorithm for Fraud Detection and Validation in Healthcare Provider Submitted Insurance Claims

Algorithm 3 outlines the process for identifying fraudulent behavior in insurance claims submitted by healthcare providers. It utilizes anonymous credentialing, blockchain-based service verification, and structured billing validation to ensure the integrity of claims while protecting provider confidentiality. This algorithm is designed to detect a wide range of fraudulent patterns, including unauthorized service submissions, fake billing codes, and overcharging. The step-by-step breakdown below explains how each component contributes to fraud prevention and claim validation:

The algorithm begins by initializing the claim process in Lines 1–4. The healthcare provider's unique identifier (`Provider_ID`) and a `Service_Token` are received from the provider (Line 1). Using these inputs, the provider generates an *Anonymous Credential (AC)*, ensuring that their identity is anonymized while maintaining a link to the service data (Line 2). These credentials, along with relevant service records, are securely stored on the blockchain (Line 3). A claim referencing the `AC` is then submitted by the health insurance provider (Line 4), transitioning the algorithm into the fraud detection and validation phase.

In Lines 5–6, the algorithm validates the provided service data. It retrieves the `Service_Records (SRs[])` from the blockchain and checks if the `Service_Token` exists in the records (Line 5). If the token is invalid or missing, the fraud is

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

ALGORITHM 2 | Fraud detection while submitting claim by patient.

Input: Patient_ID, Service_Token, Claim_Record, Patient_Records PRs[], Service_Records SRs[], Billing_Codes blling_codes[], Insurance_Policy IP

Output: Fraud detection results and insurance claim validation

Initialization:

1: Read Patient_ID and send to HealthCare Service Provider
2: Generate Anonymous Credential (AC) using Patient_ID and Service_Token
3: Store AC and associated data on Smart Contract
4: Read claim requests with AC from the Health Insurance Provider

Fraud Detection and Validation:

5: Read AC, PRs[], SRs[]
6: **if** AC not in PRs[] **then**
7: **return Fraud: "False Identity or Misrepresentation of Identity"**
8: **end if**
9: **if** AC not in SRs[] **then**
10: **return Fraud: "Invalid Service Record (Billing for Unprovided Services)"**
11: **end if**
12: **if** Insurance_ID in Claim_Record is not null **then**
13: **return Fraud: "Multiple Claims Detected"**
14: **end if**
15: Validate Billing_Codes:
16: **if** billing_codes[] not in Patient_Record **then**
17: **return Fraud: "Fake Billing Code"**
18: **else**
19: Extract billingCode, Split into service codes temp[], Calculate billByServiceCode
20: **if** billingAmount ≠ billByServiceCode **then**
21: **return Fraud: "Inflated Claims Detected"**
22: **end if**
23: **end if**
24: Validate Insurance Policy:
25: **if** Claimed_Amount > Max_Coverage in IP **then**
26: **return Fraud: "Misrepresentation of Coverage"**
27: **end if**
28: Validate Paid_Amount in Claim_Record:
29: **if** Paid_Amount == null **then**
30: **return Fraud: "Insurance Claim is Valid"**
31: **else**
32: **return Fraud: "Underpayment Detected"**
33: **end if**

flagged as *Billing for Unprovided Services* (Line 6). This ensures that only genuine services rendered by the provider are eligible for claims.

The next step focuses on validating the provider's identity in Lines 7–8. The algorithm verifies whether the `Provider_ID` exists in the `Insurance_Records (IRs[])` (Line 7). If the provider is not found in the records, the fraud is flagged as *Fake Provider* (Line 8). This validation ensures that only authorized providers can submit claims, preventing unauthorized entities from exploiting the system.

In Lines 9–16, the algorithm validates the billing details submitted by the provider. It checks whether the `Billing_Codes` in the claim exist in the `Service_Records (SRs[])` (Line 9). If the codes are invalid or missing, the fraud is flagged as *Fake Billing Code* (Line 10). The algorithm then extracts the `billingCode` and recalculates the total billing amount using the valid codes (Lines 11–16). If the recalculated amount does not match the claimed amount, the fraud is flagged as *Inflated Billing* (Line 16). These checks ensure the accuracy and legitimacy of the billing information provided by the healthcare provider.

The algorithm proceeds to validate the insurance policy and patient association in Lines 17–20. It checks whether the `Patient_ID` in the claim is associated with an active `Insurance_Policy (IP)` (Line 17). If no valid or active policy is linked, the fraud is flagged as *Policy Misuse* (Line 18). This step ensures that claims are only processed for patients with legitimate, active insurance policies.

Finally, in Lines 21–26, the algorithm checks for duplicate claims. It ensures that the claim has not already been submitted by the provider (Line 21). If a duplicate claim is detected, the fraud is flagged as *Duplicate Billing* (Line 22). If all validations are successfully passed, the claim is approved as valid (Line 26), ensuring transparency and fairness in the process.

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

ALGORITHM 3 | Fraud detection while submitting claim by healthcare provider.

Input: Provider_ID, Service_Token, Claim_Record, Patient_Records PRs[], Service_Records SRs[], Insurance_Records IRs[], Billing_Codes blling_codes[], Insurance_Policy IP
Output: Fraud detection results and insurance claim validation
Initialization:
Read Provider_ID and Service_Token
Generate Anonymous Credential (AC) using Provider_ID and Service_Token
Store service data and AC on the Smart Contract
Read claim requests referencing AC
Fraud Detection and Validation:
if Service_Token not in Service_Records SRs[] **then**
    return Fraud: "Billing for Unprovided Services"
end if
if Provider_ID not in Insurance_Records IRs[] **then**
    return Fraud: "Fake Provider"
end if
if Billing_Codes not in Service_Records SRs[] **then**
    return Fraud: "Fake Billing Code"
else
    Extract billingCode and billingAmount
    Recalculate billingAmount
    if Recalculated billingAmount ≠ Claimed billingAmount **then**
        return Fraud: "Inflated Billing"
    end if
end if
if Patient_ID not associated with active Insurance_Policy **then**
    return Fraud: "Policy Misuse"
end if
if Claim already submitted **then**
    return Fraud: "Duplicate Billing"
end if
Final Decision:
    return "Insurance Claim is Valid and Approved"

4.5 | Fraud Detection Model

The Fraud Detection Model integrates blockchain-based smart contracts and the proposed algorithms to identify fraudulent activities in health insurance claims. By leveraging the Anonymous Credential (AC) and validating claim data against stored records, the system efficiently detects and flags various types of fraud. Table 5 outlines the list of potential frauds and their detection mechanisms.

5 | Implementation of the Proposed System

This section describes the implementation process of the proposed system, focusing on the technologies used and the working procedure. The system is designed to ensure privacy preservation and fraud detection while providing a seamless experience for patients, healthcare providers, and insurance service providers.

5.1 | Technology Used

To implement this system as per the proposed model, we utilized several recent technologies to facilitate efficient, secure, and privacy-preserving operations. Table 6 below lists the technologies used, their versions, and their respective roles in the system.

5.2 | Working Procedure

This section explains the working procedure of the insurance claim system, detailing each step in the workflow. It outlines the key steps, including the generation of a patient's anonymous credential, secure storage of anonymized patient data on the blockchain, claim submission by patients and healthcare service providers, claim verification by the health insurance provider, and the detection of fraudulent activities. Additionally, it highlights how privacy preservation and fraud detection mechanisms are seamlessly integrated into the system to ensure secure handling of sensitive information, data security, transparency, and the identification of fraudulent activities during the insurance claim process.

5.2.1 | Anonymous Credential Generation

In the first step, the patient shares their personal information, including Patient ID, Hospital ID, and Service Token, with the healthcare service provider. The healthcare service provider then

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 5 | Fraud types and detection procedures by algorithms.

Fraud name	Fraud detection procedure
False Identity or Misrepresentation of Identity	The system generates an Anonymous Credential (AC) using the Patient ID and Service Token and stores it on a Smart Contract. If a claim request is submitted, the system checks whether the AC exists in the Patient Records (PRs[]). If the AC is not found, it flags the claim as fraud due to false identity or misrepresentation.
Billing for Unprovided Services	The system retrieves the Anonymous Credential (AC) and Service Token from the claim and verifies their existence in the Service Records (SRs[]). If the Service Token or AC is missing, the claim is flagged as fraud due to billing for unprovided services.
Fake Billing Code	The system extracts the Billing Codes from the submitted claim and cross-checks them against Patient Records (PRs[]) and Service Records (SRs[]). If the codes are not found in these verified records, the claim is flagged as fraud due to fake billing codes.
Inflated Claims	The system extracts billing codes from the claim, recalculates the total billing amount, and compares it with the claimed amount. If the recalculated billing amount does not match the submitted claimed amount, the claim is flagged as fraud due to inflated claims.
Multiple Claims	The system checks the Insurance ID in the claim record against previously submitted claims. If a duplicate Insurance ID is detected for the same treatment, the claim is flagged as fraud due to multiple claims.
Duplicate Billing	The system compares the current claim record with previously submitted claims. If identical billing codes, Patient ID, or Service Token are found in past claims, the system flags the claim as fraud due to duplicate billing.
Falsifying Medical Conditions	The system compares the submitted diagnosis and treatment details in the Claim Record with the Patient Records (PRs[]). If the claim details are inconsistent with the patient's verified medical history, the system flags the claim as fraud due to falsifying medical conditions.
Misrepresentation of Coverage	The system retrieves the Max Coverage and covered services from the patient's Insurance Policy (IP). If the claimed amount exceeds the Max Coverage or includes treatments not covered by the policy, the claim is flagged as fraud due to misrepresentation of coverage.
Fake Provider	The system retrieves the Provider ID from the claim and validates it against the Insurance Records (IRs[]). If the Provider ID is not found in the verified records, the claim is flagged as fraud due to a fake provider.
Policy Misuse	The system retrieves the Patient ID and associated Insurance Policy (IP) details. If no valid or active policy is found for the patient at the time of the claim, the system flags the claim as fraud due to policy misuse.
Underpayment Detected	The system retrieves the Paid Amount from the claim record and compares it with the recalculated valid claim amount. If the Paid Amount is less than the valid claim amount without valid justification, the case is flagged as fraud due to underpayment detected.

generates an anonymous credential using the SHA-256 algorithm to ensure the privacy preservation of the patient. This process secures the patient's sensitive information by creating a unique credential that can be used without revealing personal details. As shown in Figure 4, the patient input form allows the healthcare service provider to generate the anonymous credential, ensuring privacy while maintaining a secure link to the patient's identity.

5.2.2 | Secure Storage of Patient Data Using Blockchain

After generating the anonymous credential for the patient, the healthcare service provider proceeds to store the patient's information securely on the blockchain. This includes the anonymous credential and the associated service token, ensuring that the data remain immutable and cannot be tampered with. The data are also stored in IPFS to provide decentralized and reliable storage, enhancing security and availability. By integrating IPFS with the blockchain, the system ensures that sensitive patient data is stored off-chain while its hash is recorded on-chain, creating a verifiable and tamper-proof link to the data. Smart contracts are utilized to automate this process, enforcing predefined rules for data storage and retrieval, thereby maintaining transparency and ensuring that only authorized entities can access the information.

As shown in Figure 5, the healthcare service provider first creates the patient record using the anonymous credential and service

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 6 | Technologies used in the development of the system.

Technology name	Version	Usage
Node Package Managers	9.8.1	Package management for Node.js modules and dependencies.
NodeJS	18.17.1	Backend development and integration with the blockchain network.
ReactJS	18.1.0	Frontend development for creating a responsive and user-friendly interface.
Material UI	5.0.6	UI components and styling for the web application.
Hyperledger Fabric	2.5.10	Blockchain platform for implementing secure, immutable ledgers.
Hyperledger Fabric SDK	2.2	Node.js SDK for interaction with the Hyperledger Fabric network.
IPFS	0.32.1	Decentralized storage for storing patient data securely.
MySQL	8.0.36	Relational database for storing application metadata.
Docker Engine	3.7	Containerization for deploying system components.
Docker Compose	2.27.0	Multicontainer application orchestration.
CouchDB	3.4.2	Document-based database for blockchain states.

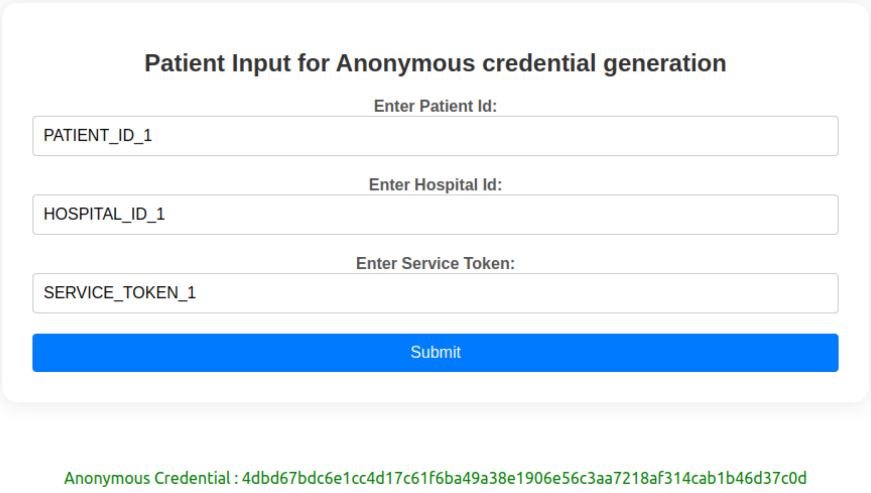

FIGURE 4 | Input form for generating a patient's anonymous credential.

token through the "Create Patient" functionality, which securely stores the data. The successful creation of the patient record is confirmed with a message displaying the anonymous credential and service token. Later, the "Read Patient" functionality allows authorized health insurance provider to retrieve the patient data securely. This workflow guarantees the preservation of sensitive information, leveraging blockchain, IPFS, and smart contracts to ensure privacy, integrity, and security in the healthcare system.

5.2.3 | Insurance Claim Verification

In this section, the process of insurance claim verification by the health insurance provider is discussed. Both patients and healthcare service providers can initiate claims by sharing the anonymous credential with the health insurance provider. This credential is then used to search the patient's data stored on the blockchain through the smart contract for claim verification. The smart contract ensures that the claim is validated based on predefined rules and securely stored data, allowing the detection of potential frauds.

In the case of a valid claim, the smart contract verifies several parameters, including the claim's association with a valid patient record, the identity of the patient through their anonymous credential, and the accuracy of the service token linked to the claim. Once all checks are passed, the claim is marked as "VALID," confirming that it adheres to the system's rules and policies. As shown in Figure 6, the successful verification process displays the validity of the claim, ensuring transparency and trustworthiness.

In contrast, for an invalid or false claim, the smart contract identifies discrepancies such as mismatched anonymous credentials, invalid service tokens, or attempts to submit fraudulent claims. When such issues are detected, the claim verification fails, and the status is displayed as "Failed to verify claim." As shown in Figure 7, this ensures that fraudulent activities, such as falsifying medical conditions or billing for unprovided services, are effectively detected and rejected.

By leveraging the anonymous credential and the smart contract's fraud detection capabilities, the system guarantees data security and integrity while maintaining a transparent and robust insurance claim process.

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

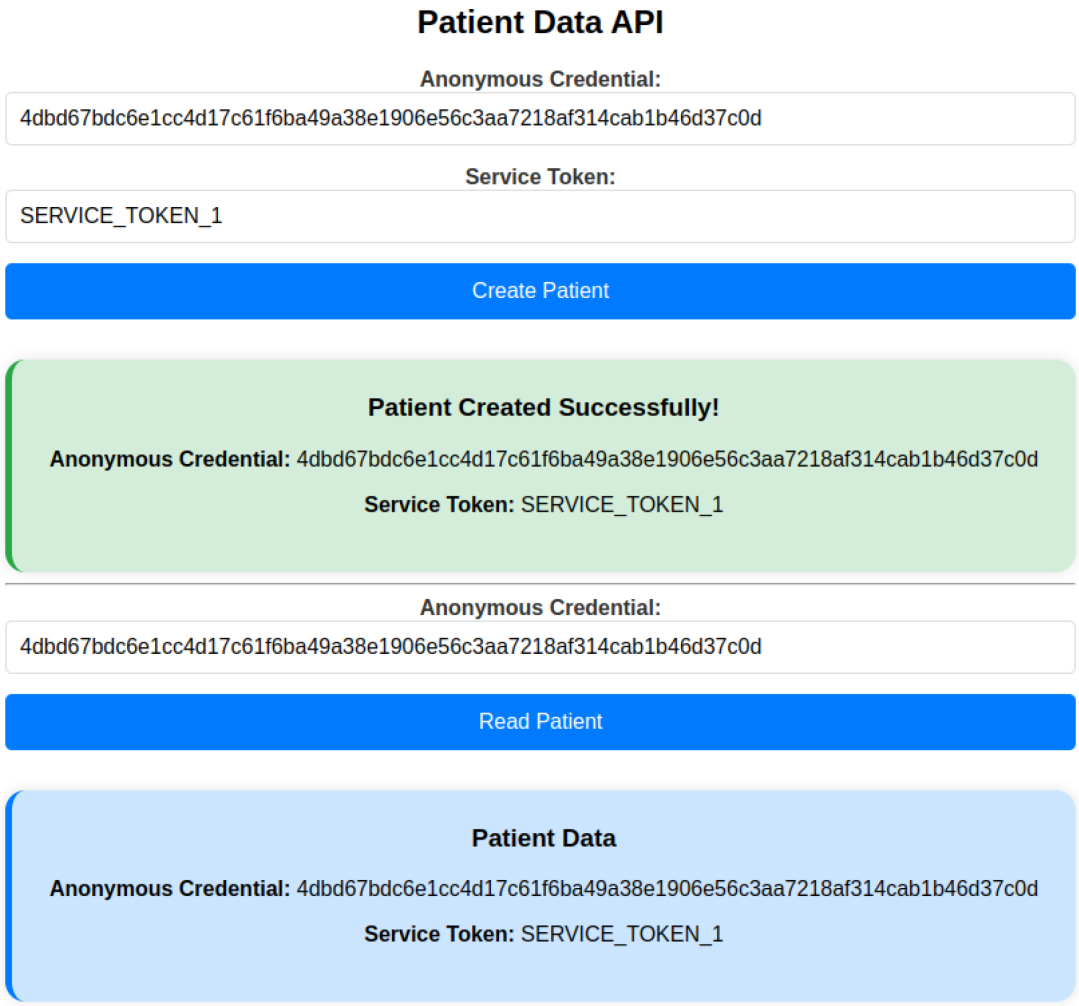

FIGURE 5 | Creating and storing patient data securely using an anonymous credential and service token.

6 | Performance Analysis

The performance of the proposed system is assessed by evaluating key operations and their associated resource utilization. This analysis provides insights into the efficiency, reliability, and scalability of the system in handling privacy-preserving health insurance claims. The system was tested on a machine with the following specifications: AMD Ryzen 7 5700U processor, 16 GB RAM, and 512 GB SSD storage. Performance metrics were measured in varying user loads, ranging from 1 to 200 concurrent users, focusing on two critical aspects: latency and throughput analysis. It is important to note that for operations related to writing and storing patient information, the users are the healthcare provider and the patient, while for validating legitimate claims and identifying fraudulent claims, the user is the health insurance provider. This distinction helps to analyze system performance based on different interacting entities.

6.1 | Latency Analysis

Latency refers to the time taken to complete a transaction, measured in milliseconds (ms), and serves as a key metric for evaluating the responsiveness of the system. In the context of this work, latency reflects how quickly the system performs critical operations such as writing patient data, validating legitimate insurance claims, and identifying fraudulent activities. Lower latency results in faster claim processing, reduced wait times, and an improved user experience, which are essential in real-time healthcare environments.

As illustrated in Figure 8, the latency remains low when the system operates under lighter user loads, specifically between 1 to 20 concurrent users, with all operations completing in under 1000 milliseconds. This highlights the efficiency of the system in low-demand environments. However, as the number of users increases beyond 50, latency rises steadily across all operations. This growth in latency can be attributed to processing overhead introduced by smart contract execution, metadata hashing, and cryptographic credential generation, especially as the blockchain network handles concurrent transactions.

Writing patient information exhibits the highest latency overall, with an initial drop at 10 users followed by a consistent increase as user load rises. At the highest concurrency level (200 users), this operation reaches a peak latency of nearly 7900 ms. This is largely due to the computational demands of generating anonymous credentials, encrypting data, and storing patient references

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

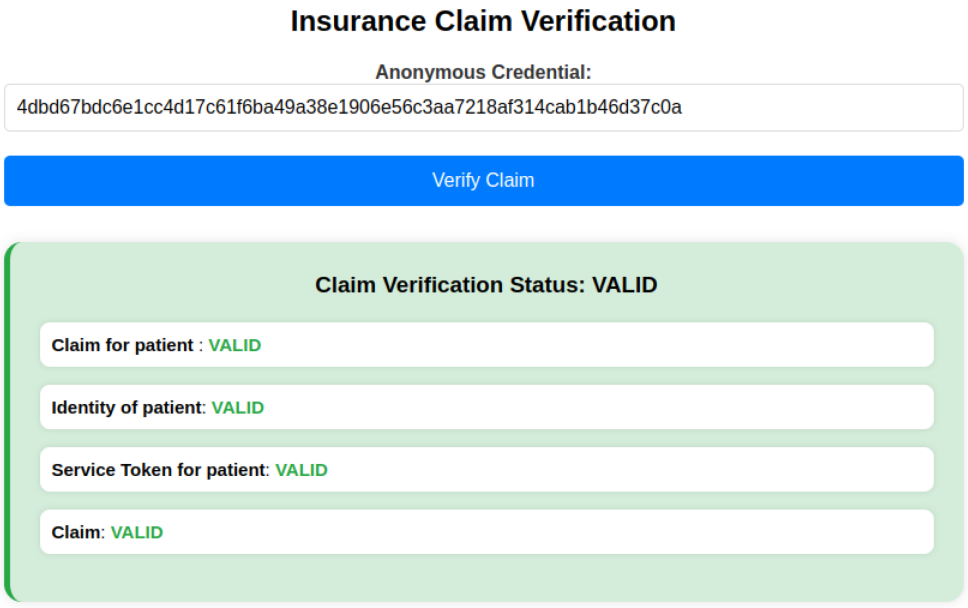

FIGURE 6 | Valid claim verification—successful verification confirming all parameters as valid.

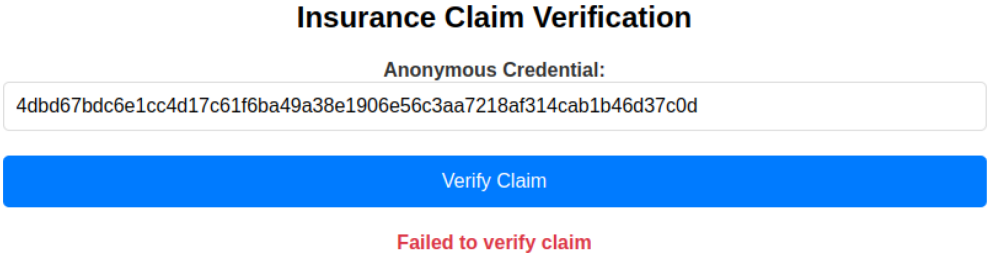

FIGURE 7 | Invalid claim verification—failed claim verification due to invalid data or discrepancies.

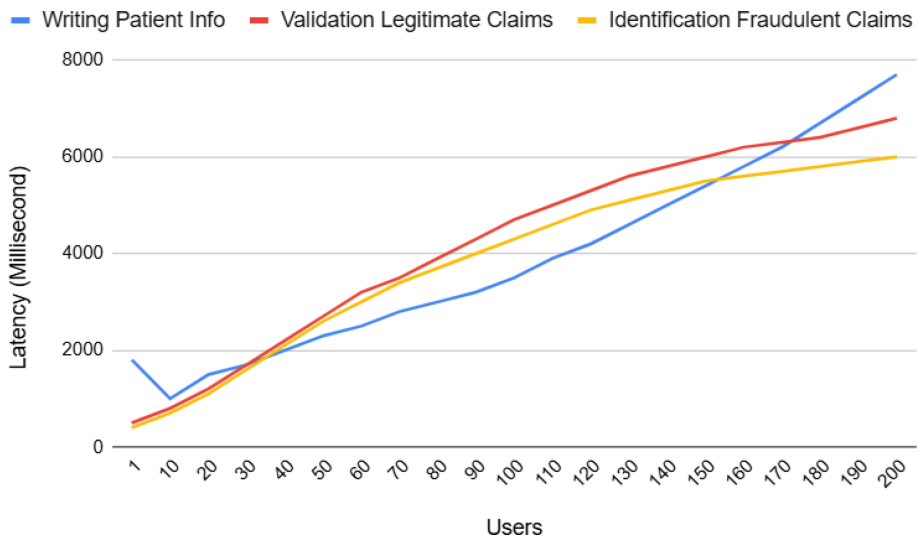

FIGURE 8 | Latency analysis of patient data writing, claim validation, and fraud detection.

securely in IPFS. The validation of legitimate claims also shows a sharp increase in latency, peaking at around 7000 ms. This can be attributed to the additional steps involved in verifying policy coverage, checking billing codes, and ensuring claim authenticity via smart contract logic. Meanwhile, the identification of fraudulent claims demonstrates relatively stable latency growth and levels off after 160 users, peaking at approximately 6000 ms. This suggests that the fraud detection process is more optimized, relying on streamlined verification rules and pattern matching with historical data.

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Overall, these latency trends confirm that while the system performs well at low to moderate user loads, the growing delay at higher concurrency highlights areas for optimization. Future enhancements may include refining smart contract logic, implementing off-chain validation for certain operations, or adopting parallel processing techniques to improve scalability without compromising processing speed.

6.2 | Throughput Analysis

Throughput measures the system's ability to process multiple transactions per second (TPS) and is a critical metric for evaluating its efficiency under concurrent user loads. A higher throughput indicates that the system can support larger volumes of claim processing without delays, which is essential for real-time health insurance operations.

As shown in Figure 9, the system exhibits an initial increase in throughput with growing user loads. The store patient information operation reaches its peak around 30 users, with a maximum throughput of approximately 6.5 TPS. Beyond this point, throughput declines gradually due to increasing overhead from encryption, credential generation, and IPFS-related operations. The validation of legitimate claims operation maintains a more stable profile, with throughput increasing up to 100 users and peaking near 3 TPS. The gradual decline afterward is attributed to complex verification steps, including billing code validation and policy rule enforcement via smart contracts.

In the case of identification of fraudulent claims, the throughput curve demonstrates notable fluctuations with two significant peaks-around 50 users and again between 110 and 130 users, reaching above 6 TPS. These spikes reflect the behavior of the fraud detection module, which was tested using multiple fraud scenarios defined in the proposed model. Each fraud type, such as identity misrepresentation, inflated billing, duplicate claims, and policy misuse, introduces unique logic paths and execution times. The observed throughput spikes suggest that under certain combinations of fraud patterns and input data, the system optimizes resource use effectively, leading to higher performance during those intervals. After the peak, throughput gradually stabilizes, indicating that computational saturation is reached as user concurrency increases.

Overall, the throughput behavior confirms that while the system is well-optimized for moderate loads, its performance varies depending on the complexity and nature of the operation. Fraud detection, benefiting from a flexible and modular rule-based design, demonstrates the highest scalability among the three.

6.3 | Analysis of Resource Utilization

A further resource utilization analysis was performed by integrating the Hyperledger Caliper with the blockchain-based patient healthcare insurance system. The resource utilization results are measured in terms of the maximum and average usage of CPU, memory, incoming traffic, and outgoing traffic. As shown in Table 7, memory usage is reported in megabytes (MB), and memory limits are expressed in gigabytes (GB). These units are widely used to measure and evaluate resource allocation in computing environments, providing clear insights into the performance of the Hyperledger Fabric network components. Here, two peer nodes (`peer0.org1.example.com` and `peer0.org2.example.com`) represent the roles of the patient and the healthcare provider, respectively. The patient peer node initiates insurance claims, while the healthcare provider peer node validates and processes these claims, including verifying the authenticity of the claims.

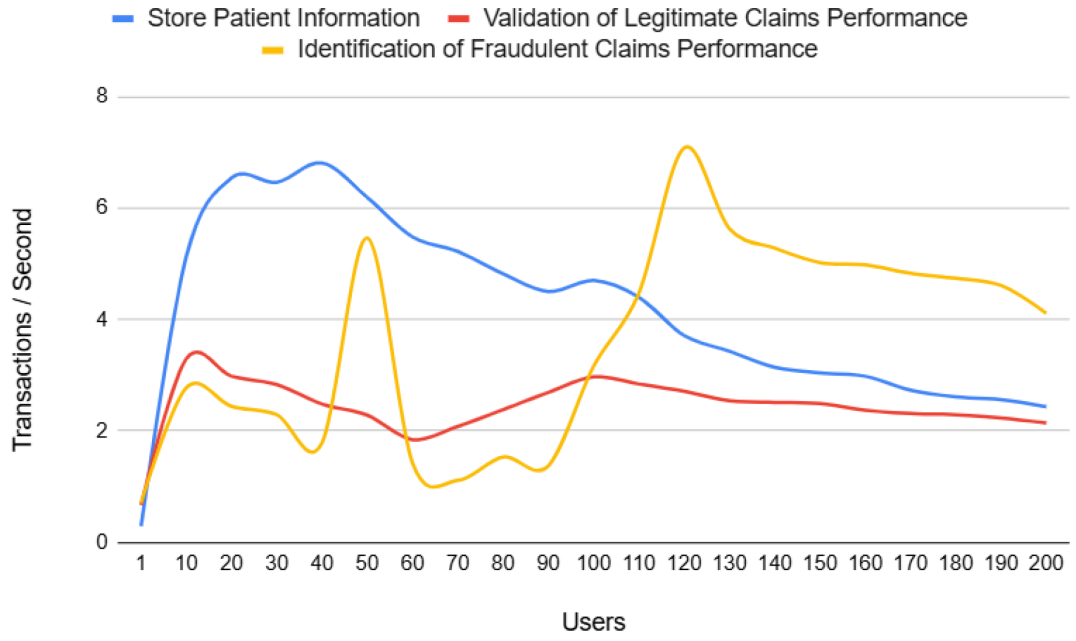

FIGURE 9 | Throughput analysis of writing patient information, validating legitimate claims, and identifying fraudulent claims under varying user loads.

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 7 | Resource allocation metrics for Hyperledger Fabric network components.

Name	CPU %	Memory usage (MB)/Limit (GB)	Memory %	Net I/O (KB)	Block I/O (KB)
peer0.org1.example.com (Peer node of org1)	2.47	39.32/14.99	0.26	2.11/2.16	8.19/778
peer0.org2.example.com (Peer node of org2)	2.06	38.53/14.99	0.25	1.95/1.73	0/778
orderer.com (Ordered Node)	0.37	15.98/14.99	0.10	2.09/4.07	81.9/426
ca_org1 (CA for org1)	0.00	9.258/14.99	0.06	59.7/48.8	36.9/868
ca_org2 (CA for org2)	0.00	9.273/14.99	0.06	59.6/48.6	0/868
ca_orderer (CA for orderer)	0.00	9.078/14.99	0.06	49.6/27.3	0/659

One orderer node (`orderer.example.com`) controls the transaction flow and ensures that all transactions are written to the blockchain in the correct order. Three Certificate Authorities (CAs) (`ca_org1`, `ca_org2`, and `ca_orderer`) provide membership services for their respective organizations. These CAs issue certificates that authenticate and authorize the peer nodes, enabling secure interactions between the patient, healthcare provider, and insurance provider within the blockchain network.

It is observed that the peer nodes, particularly the healthcare provider node, consume the majority of the resources due to the computationally intensive process of verifying claims and detecting potential fraud. The orderer node also shows notable resource consumption as it maintains the integrity and order of transactions within the network. The CAs consume minimal resources since their primary function is limited to certificate management. Overall, the analysis demonstrates that the blockchain-based healthcare insurance system achieves efficient resource utilization while ensuring the security and integrity of patient insurance claims.

6.4 | Analysis and Observations

The analysis of the proposed system evaluates its scalability, efficiency, and resource utilization under varying user loads. Below are the key observations:

- Scalability: The system showed consistent performance for up to 10 users, with a slight increase in latency for 20 users.
- Efficiency: Valid claim verification was faster compared to invalid claim verification due to optimized smart contracts.
- Resource Utilization: CPU and memory usage increased linearly with the number of users, while disk usage remained relatively constant.

The performance analysis reveals that the system efficiently handles moderate user loads, maintaining acceptable levels of latency and resource utilization. Future enhancements could target optimizing smart contracts and refining database interactions to further improve scalability.

7 | Discussion

In this section, we provide a comprehensive discussion about how our system ensures the security and privacy services outlined in Section 4.2. The goal is to assess how effectively the system safeguards healthcare insurance claim data while maintaining patient anonymity and enabling fraud detection. In addition to rule-based logic and smart contract-driven validation, this discussion also explores how Machine Learning (ML) can be integrated into the model to enhance fraud detection capabilities. By analyzing patterns and behaviors across historical data, ML contributes to more accurate, adaptive, and intelligent identification of fraudulent activities, thereby strengthening the overall reliability and scalability of the system. Finally, we highlight on the integration of our system with the existing health insurance systems.

7.1 | Security Analysis

The proposed blockchain-based model ensures critical attributes of a secure and privacy-preserving system, including pseudonymity, privacy, integrity, accountability, and overall security.

Pseudonymity: Our system uses SHA-256 hashing to generate anonymous credentials that obscure a patient's actual identity. These credentials are dynamically created using a combination of identifiers, as implemented in the credential generation mechanism. The algorithm concatenates the Patient_ID, Hospital_ID, Service_Token, and Timestamp individually, then hashes them to form a unique anonymous credential (AC):

$$AC = SHA256(Patient\_ID\_Hash + Hospital\_ID\_Hash + Service\_Token\_Hash + Timestamp\_Hash) \quad (1)$$

This method guarantees patient identity concealment throughout all stages of data handling and transmission.

Privacy: The proposed system ensures privacy by decoupling identifiable patient information from the claim processing workflow. Instead of encrypting data, all sensitive patient data are hashed using SHA-256 and transformed into anonymous credentials, which are then stored off-chain using IPFS. This method ensures that readable personal data is never stored in the blockchain. Only references or hashes are recorded on-chain, making it impossible to link transactions back to a specific patient without external context or authorization. Thus, the following privacy-preserving structures are achieved:

- Personal health information is never exposed on the blockchain.

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

- The risk of data leakage or correlation attacks is significantly reduced.
- Patient anonymity is preserved throughout the claim submission and validation process.

This approach aligns with privacy-by-design principles and ensures compliance with data protection requirements, making it suitable for secure healthcare data management in insurance claim systems.

Integrity: The integrity of data is ensured through the blockchain's immutable ledger and smart contract validation rules. Each transaction is verified against blockchain-stored values. The system implements conditional checks to detect data tampering, misrepresentation, or altered billing. The core logic is defined as:

$$Integrity\_Check = \begin{cases} Valid, & \text{if data matches} \\ & \text{blockchain records} \\ Fraudulent, & \text{otherwise} \end{cases} \quad (2)$$

This approach ensures that once submitted, claim data cannot be altered without detection.

Accountability: Smart contracts log every interaction transparently, allowing for full traceability. In both patient-submitted and provider-submitted scenarios, the system verifies claim legitimacy through rule-based decision-making. The accountability validation mechanism is described as:

$$Accountability = \begin{cases} Valid\_Claim, & \text{if criteria is satisfied} \\ Fraudulent\_Claim, & \text{otherwise} \end{cases} \quad (3)$$

This ensures that every stakeholder is held responsible for the correctness of their input and actions.

Security: The security of the proposed system is established through a layered combination of blockchain immutability, decentralized storage, anonymous credentialing, and smart contract enforcement. Rather than relying on direct encryption, the model secures patient interactions and claim data through structural and procedural safeguards. Security validation and fraud detection are handled programmatically through smart contracts, which autonomously enforce predefined rules to detect anomalies or misuse. This includes checks for identity spoofing, billing inconsistencies, fake providers, and multiple claims. The overall security model can be represented as:

$$\begin{aligned} SecurityModel = {} & AnonymousCredential \\ & + DecentralizedStorage(IPFS) \\ & + SmartContractValidation \end{aligned} \quad (4)$$

This layered architecture ensures that patient data and claim processing are secured against tampering, unauthorized access, and internal fraud, all while maintaining system transparency and auditability.

7.2 | Enhancing Fraud Detection Using Machine Learning

While the system effectively uses smart contracts and predefined rule-based logic for fraud detection, integrating Machine Learning (ML) techniques can significantly improve its adaptability and accuracy [56]. ML models can learn from historical claim data, uncover hidden patterns, and detect fraudulent behavior that might evade traditional rule-based methods.

Patient-Submitted Insurance Claims (**Algorithm 2**): In case of claims submitted by patients, ML can support several critical validation steps. During identity verification (Step 5), ML models can analyze claim histories and behavioral patterns to generate a fraud score. If the score exceeds a defined threshold (e.g., 80%), the system can automatically flag the claim for further review [57]. In billing validation (Step 15), ML can identify anomalies in billing codes, such as duplicate charges or services inconsistent with the patient's medical history, indicating potential fraud. Additionally, at the billing amount estimation stage (Step 19), ML can predict expected costs based on past trends [58]. Claims that significantly deviate from learned norms can be flagged as inflated or suspicious.

Healthcare Provider-Submitted Claims (**Algorithm 3**): ML also enhances fraud detection for healthcare provider-submitted claims. At Step 9, ML can assess a provider's historical behavior to assign a risk score, highlighting those with patterns of suspicious activity [59]. In Step 10, ML checks whether submitted billing codes align with the patient's typical medical profile, flagging mismatched entries as potential fraud. Finally, in Step 15, ML models evaluate the billing amount in context with previous claims. Unusual spikes or inconsistencies can trigger alerts for potential overbilling [60].

ML models enable early identification of suspicious behavior, such as unusual billing codes, inflated charges, or inconsistent claim histories, and can assign fraud scores or flag claims for further review. This not only accelerates fraud detection but also improves accuracy and reduces the need for manual checks. When combined with blockchain's inherent auditability and transparency, ML integration positions the system as a scalable and robust solution for modern health insurance fraud prevention.

7.3 | Interoperability of the Proposed System

The proposed system is designed for scalability and interoperability, enabling seamless integration into health insurance infrastructures across various countries. By aligning with industry standards such as Health Level Seven Fast Healthcare Interoperability Resources (HL7 FHIR), RESTful APIs, and privacy-focused data handling, the system ensures compatibility with existing digital health ecosystems operated by both public and private insurers.

In the United States, major claim processing and health IT companies such as Change Healthcare [61] and Optum (Unit-

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

edHealth Group) [62] provide extensive claim management, fraud analytics, and payer-provider integration. These platforms increasingly support open standards and API-based workflows, making them ideal candidates for integration with our proposed system, and thus, can introduce anonymous credential mechanisms for privacy preservation.

In Canada, digital health claims are handled through platforms like TELUS Health eClaims [63], and provincial systems such as the Ontario Health Insurance Plan (OHIP) [64]. These systems operate under strict privacy legislation like the Personal Information Protection and Electronic Documents Act (PIPEDA) and benefit from solutions that enhance trust and reduce fraud in both private and public insurance contexts. In India, health claim management is rapidly evolving with digital initiatives like National Health Claims Exchange (NHCX) [65]. The proposed model's modular design and compliance-ready architecture allow for smooth integration with these systems.

These platforms are adopting FHIR standards and API gateways to handle high-volume claims and integrate third-party services. The proposed system, with its blockchain-based audit trail, rule-based fraud detection, and support for future machine learning enhancements, is well-suited for scalable deployment within such frameworks.

Looking ahead, integrating machine learning into the proposed model will enhance real-time anomaly detection and adaptive fraud scoring, allowing the system to respond effectively to evolving fraud tactics. Combined with its scalable infrastructure and open integration capabilities, the proposed solution stands as a globally adaptable platform for improving the speed, security, and integrity of health insurance claim processing.

8 | Conclusion

The aim of this research was to develop a system that preserves patient privacy and detects fraud in health insurance claims by addressing key challenges in multiprovider environments. We designed a framework that ensures the confidentiality of sensitive patient data and implements mechanisms to detect fraudulent activities. However, the system has certain limitations, including its inability to cover all types of fraud and the assumption that healthcare providers are trustworthy, which narrows its scope. Implementation results demonstrated that the system effectively preserves privacy and manages claims securely, with performance evaluations indicating its efficiency in handling moderate-scale operations. While these results are promising, scalability remains a challenge, particularly for larger networks with higher transaction volumes. Future work will focus on optimizing the system for larger-scale implementations, incorporating broader fraud detection scenarios, and integrating advanced technologies such as AI and ML to enhance fraud detection accuracy and adaptability. Additionally, techniques like zero-knowledge proofs will be explored to further strengthen security and ensure a more comprehensive, scalable, and intelligent solution for privacy-preserving and fraud-resistant health insurance systems.

Author Contributions

Md. Mazharul Islam: investigation, methodology, software, writing – original draft. **Mubasshir Ahmed:** software, validation, methodology. **Rajesh Palit:** conceptualization, funding acquisition, writing – review and editing. **Mohammad Shahriar Rahman:** writing – review and editing, visualization, conceptualization. **Salekul Islam:** conceptualization, writing – review and editing, supervision, project administration.

Acknowledgments

The research was funded by the Institute for Advanced Research (IAR), United International University, and the Office of Research (OR), North South University (Grant No. UIU-IAR-02-2023-SE-41).

Data Availability Statement

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

References

1. B. D. Deebak and S. O. Hwang, "Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework," *IEEE Transactions on Mobile Computing* 23, no. 5 (2023): 5897–5916.

2. V. R. Saddi, S. Boddu, B. Gnanapa, N. Jiwani, and T. Kiruthiga, "Leveraging Big Data and AI for Predictive Analysis in Insurance Fraud Detection," in *Proceedings of the 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)* (IEEE, 2024), 1–6.

3. S. M. Williamson and V. Prybutok, "Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare," *Applied Sciences* 14, no. 2 (2024): 675.

4. M. F. Ahammed and M. R. Labu, "Privacy-Preserving Data Sharing in Healthcare: Advances in Secure Multiparty Computation," *Journal of Medical and Health Studies* 5, no. 2 (2024): 37–47.

5. C. Dhasarathan, M. Shanmugam, M. Kumar, D. Tripathi, S. Khapre, and A. Shankar, "A Nomadic Multi-Agent Based Privacy Metrics for e-Health Care: A Deep Learning Approach," *Multimedia Tools and Applications* 83, no. 3 (2024): 7249–7272.

6. B. P. Kasaraneni, "Machine Learning Models for Fraud Detection in Health Insurance Claims: Techniques, Applications, and Real-World Case Studies," *Journal of Machine Learning in Pharmaceutical Research* 4, no. 1 (2024): 110–147.

7. Countries with Universal Healthcare 2025, (2025), https://worldpopulationreview.com/country-rankings/countries-with-universal-healthcare.

8. The Challenge of Health Care Fraud (2024), https://www.nhcaa.org/tools-insights/about-health-care-fraud/the-challenge-of-health-care-fraud/.

9. K. Kiania, S. M. Jameii, and A. M. Rahmani, "Blockchain-Based Privacy and Security Preserving in Electronic Health: A Systematic Review," *Multimedia Tools and Applications* 82, no. 18 (2023): 28493–28519.

10. I. P. S. Setiawan and A. Alamsyah, "Enhancing Security, Privacy, and Traceability in Indonesia's National Health Insurance Claims Process Using Blockchain Technology," in *Proceedings of the 2023 International Conference on Artificial Intelligence, Blockchain, Cloud Computing, and Data Analytics (ICoABCD)* (IEEE, 2023), 77–82.

11. Staff, V, *Insurance Claim Denials: Worst Companies and How to Appeal* (valuepenguin, 2024), https://www.valuepenguin.com/health-insurance-claim-denials-and-appeals.

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

12. E. Trish, P. Ginsburg, L. Gascue, and G. Joyce, "Physician Reimbursement in Medicare Advantage Compared With Traditional Medicare and Commercial Health Insurance," *JAMA Internal Medicine* 177, no. 9 (2017): 1287–1295.

13. M. S. A. Mazumder, M. A. Rahman, and D. Chakraborty, "Patient Care and Financial Integrity in Healthcare Billing Through Advanced Fraud Detection Systems," *Academic Journal on Business Administration, Innovation & Sustainability* 4, no. 2 (2024): 82–93.

14. T. Ekin, L. Frigau, and C. Conversano, "Health Care Fraud Classifiers in Practice," *Applied Stochastic Models in Business and Industry* 37, no. 6 (2021): 1182–1199.

15. R. Nowrozy, K. Ahmed, A. Kayes, H. Wang, and T. R. McIntosh, "Privacy Preservation of Electronic Health Records in the Modern Era: A Systematic Survey," *ACM Computing Surveys* 56, no. 8 (2024): 1–37.

16. D. Naik, D. Patil, and D. Lakshmi, "Sentinels of Privacy: Mastering Data Breach Detection and Response in Healthcare Ecosystems," in *Cybersecurity and Data Management Innovations for Revolutionizing Healthcare* (IGI Global, 2024), 98–131.

17. S. Sawalka, A. Lahiri, and D. Saveetha, "EthInsurance: A Blockchain Based Alternative Approach for Health Insurance Claim," in *Proceedings of the 2022 International Conference on Computer Communication and Informatics (ICCCI)* (IEEE, 2022), 1–9.

18. A. El Koshiry, E. Eliwa, T. Abd El-Hafeez, and M. Y. Shams, "Unlocking the Power of Blockchain in Education: An Overview of Innovations and Outcomes," *Blockchain: Research and Applications* 4, no. 4 (2023): 100165.

19. A. A. Khan, J. Yang, A. A. Laghari, et al., "BAIoT-EMS: Consortium Network for Small-Medium Enterprises Management System With Blockchain and Augmented Intelligence of Things," *Engineering Applications of Artificial Intelligence* 141 (2025): 109838.

20. A. Karmakar, P. Ghosh, P. S. Banerjee, and D. De, "ChainSure: Agent Free Insurance System Using Blockchain for Healthcare 4.0," *Intelligent Systems with Applications* 17 (2023): 200177.

21. A. A. Khan, S. Dhabi, J. Yang, W. Alhakami, S. Bourouis, and L. Yee, "B-LPoET: A Middleware Lightweight Proof-Of-Elapsed Time (PoET) for Efficient Distributed Transaction Execution and Security on Blockchain Using Multithreading Technology," *Computers and Electrical Engineering* 118 (2024): 109343.

22. M. Younis, W. Lalouani, N. Lasla, L. Emokpae, and M. Abdallah, "Blockchain-Enabled and Data-Driven Smart Healthcare Solution for Secure and Privacy-Preserving Data Access," *IEEE Systems Journal* 16, no. 3 (2021): 3746–3757.

23. C. Huang, W. Wang, D. Liu, R. Lu, and X. Shen, "Blockchain-Assisted Personalized Car Insurance With Privacy Preservation and Fraud Resistance," *IEEE Transactions on Vehicular Technology* 72, no. 3 (2022): 3777–3792.

24. A. El Azzaoui, H. Chen, S. H. Kim, Y. Pan, and J. H. Park, "Blockchain-Based Distributed Information Hiding Framework for Data Privacy Preserving in Medical Supply Chain Systems," *Sensors* 22, no. 4 (2022): 1371.

25. A. A. Khan, J. Yang, S. A. Awan, A. M. Baqasah, R. Alroobaea, and Y. L. Chen, "Artificial Intelligence, Internet of Things, and Blockchain Empowering Future Vehicular Developments: A Comprehensive Multi-Hierarchical Lifecycle Review," *Human-centric Computing and Information Sciences* 15 (2025): 1–20.

26. J. Yin, Y. Xiao, Q. Pei, et al., "SmartDID: A Novel Privacy-Preserving Identity Based on Blockchain for IoT," *IEEE Internet of Things Journal* 10, no. 8 (2022): 6718–6732.

27. D. Rachmawati, J. Tarigan, and A. Ginting, "A Comparative Study of Message Digest 5 (MD5) and SHA256 Algorithm," *Journal of Physics: Conference Series* 978 (2018): 12116.

28. M. C. Shekar, H. L. Gururaj, and F. Flammini, "Securing Personal Identity Using Blockchain," *International Journal of Critical Computer-Based Systems* 10, no. 3 (2022): 248–267.

29. S. Agarwal, "An Intelligent Machine Learning Approach for Fraud Detection in Medical Claim Insurance: A Comprehensive Study," *Scholars Journal of Engineering and Technology* 11, no. 9 (2023): 191–200.

30. M. Chase and K. Lauter, *An Anonymous Health Care System*. (19th USENIX Security Symposium, 2010).

31. A. Zhang, A. Bacchus, and X. Lin, "A Fairness-Aware and Privacy-Preserving Online Insurance Application System," in *Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM)* (IEEE, 2016), 1–6.

32. X. He, S. Alqahtani, and R. Gamble, "Toward Privacy-Assured Health Insurance Claims," in *Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (IEEE, 2018), 1634–1641.

33. L. Hirtan, P. Krawiec, C. Dobre, and J. M. Batalla, "Blockchain-Based Approach for e-Health Data Access Management With Privacy Protection," in *Proceedings of the 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)* (IEEE, 2019), 1–7.

34. F. Li, K. Liu, L. Zhang, S. Huang, and Q. Wu, "EHRChain: A Blockchain-Based EHR System Using Attribute-Based and Homomorphic Cryptosystem," *IEEE Transactions on Services Computing* 15, no. 5 (2021): 2755–2765.

35. A. Al Omar, A. K. Jamil, A. Khandakar, et al., "A Transparent and Privacy-Preserving Healthcare Platform With Novel Smart Contract for Smart Cities," *IEEE Access* 9 (2021): 90738–90749.

36. A. Alnuaimi, A. Alshehhi, K. Salah, R. Jayaraman, I. A. Omar, and A. Battah, "Blockchain-Based Processing of Health Insurance Claims for Prescription Drugs," *IEEE Access* 10 (2022): 118093–118107.

37. M. Al Amin, R. Shah, H. Tummala, and I. Ray, "Utilizing Blockchain and Smart Contracts for Enhanced Fraud Prevention and Minimization in Health Insurance Through Multi-Signature Claim Processing," in *Proceedings of the 2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)* (IEEE, 2024), 1–9.

38. H. Shi, M. A. Tayebi, J. Pei, and J. Cao, "Cost-Sensitive Learning for Medical Insurance Fraud Detection With Temporal Information," *IEEE Transactions on Knowledge and Data Engineering* 35, no. 10 (2023): 10451–10463.

39. A. J. Mary and S. A. Claret, "Design and Development of Big Data-Based Model for Detecting Fraud in Healthcare Insurance Industry," *Soft Computing* 27, no. 12 (2023): 8357–8369.

40. Z. Hamid, F. Khalique, S. Mahmood, A. Daud, A. Bukhari, and B. Alshemaimri, "Healthcare Insurance Fraud Detection Using Data Mining," *BMC Medical Informatics and Decision Making* 24, no. 1 (2024): 112.

41. J. M. Johnson and T. M. Khoshgoftaar, "Data-Centric Ai for Healthcare Fraud Detection," *SN Computer Science* 4, no. 4 (2023): 389.

42. S. Seshagiri and K. Prema, "Efficient Handling of Data Imbalance in Health Insurance Fraud Detection Using Meta-Reinforcement Learning," *IEEE Access* 13 (2025): 23482–23497.

43. C. Dhasaratha, M. K. Hasan, S. Islam, et al., "Data Privacy Model Using Blockchain Reinforcement Federated Learning Approach for Scalable Internet of Medical Things," *CAAI Transactions on Intelligence Technology* (2024): 1–16.

44. M. Shinde and S. V. Gumaste, "Privacy Preserving in Healthcare Sector Using Blockchain Technology," *International Journal of Innovative Science and Applied Engineering (IJISAE)* 24 (2023): 1651–1658.

45. R. Gupta, P. Kanungo, N. Dagdee, et al., "Secured and Privacy-Preserving Multi-Authority Access Control System for

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Cloud-Based Healthcare Data Sharing," *Sensors (Basel)* 23, no. 5 (2023): 2617.

46. R. Dey, A. Roy, J. Akter, A. Mishra, and M. Sarkar, "AI-Driven Machine Learning for Fraud Detection and Risk Management in US Healthcare Billing and Insurance," *Journal of Computer Science and Technology Studies* 7, no. 1 (2025): 188–198.

47. G. Fernández-Blanco, P. García-Cereijo, D. Lema-Núñez, D. Ramil-López, P. Fraga-Lamas, and L. Egia-Mendikute, "HELENE: An Open-Source High-Security Privacy-Preserving Blockchain Based System for Automating and Managing Laboratory Health Tests," (2025)arXiv preprint arXiv:250220477.

48. K. L. Tan, C. H. Chi, and K. Y. Lam, "Secure and Privacy-Preserving Sharing of Personal Health Records With Multi-Party Pre-Authorization Verification," *Wireless Networks* 30, no. 6 (2024): 4773–4795.

49. T. Mohan and K. Praveen, "Fraud Detection in Medical Insurance Claim With Privacy Preserving Data Publishing in TLS-N Using Blockchain," in *Advances in Computing and Data Sciences: Third International Conference, ICACDS 2019, Ghaziabad, India, April 12–13, 2019, Revised Selected Papers, Part I 3* (Springer, 2019), 211–220.

50. K. Kapadiya, U. Patel, R. Gupta, et al., "Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: An Analysis, Architecture, and Future Prospects," *IEEE Access* 10 (2022): 79606–79627.

51. A. Lakhan, M. A. Mohammed, J. Nedoma, et al., "Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare," *IEEE Journal of Biomedical and Health Informatics* 27, no. 2 (2022): 664–672.

52. R. Kaafarani, L. Ismail, and O. Zahwe, "Automatic Recommender System of Development Platforms for Smart Contract–Based Health Care Insurance Fraud Detection Solutions: Taxonomy and Performance Evaluation," *Journal of Medical Internet Research* 26 (2024): e50730.

53. L. Settipalli and G. Gangadharan, "Provider Profiling and Labeling of Fraudulent Health Insurance Claims Using Weighted MultiTree," *Journal of Ambient Intelligence and Humanized Computing* 14 (2023): 3422–3487.

54. G. Saldamli, V. Reddy, K. S. Bojja, M. K. Gururaja, Y. Doddaveerappa, and L. Tawalbeh, "Health Care Insurance Fraud Detection Using Blockchain," in *Proceedings of the 2020 Seventh International Conference on Software Defined Systems (SDS)* (IEEE, 2020), 145–152.

55. R. Egan, S. Cartagena, R. Mohamed, et al., "Cyber Operational Risk Scenarios for Insurance Companies," *British Actuarial Journal* 24 (2019): e6.

56. E. Nabrawi and A. Alanazi, "Fraud Detection in Healthcare Insurance Claims Using Machine Learning," *Risks (Basel)* 11, no. 9 (2023): 160.

57. J. Lu, K. Lin, R. Chen, M. Lin, X. Chen, and P. Lu, "Health Insurance Fraud Detection by Using an Attributed Heterogeneous Information Network With a Hierarchical Attention Mechanism," *BMC Medical Informatics and Decision Making* 23, no. 1 (2023): 62.

58. K. Kapadiya, F. Ramoliya, K. Gohil, et al., "Blockchain-Assisted Healthcare Insurance Fraud Detection Framework Using Ensemble Learning," *Computers and Electrical Engineering* 122 (2025): 109898.

59. J. T. Hancock, R. A. Bauder, H. Wang, and T. M. Khoshgoftaar, "Explainable Machine Learning Models for Medicare Fraud Detection," *Journal of Big Data* 10, no. 1 (2023): 154.

60. J. Zhu, J. Jang-Jaccard, A. Singh, I. Welch, H. Al-Sahaf, and S. Camtepe, "A Few-Shot Meta-Learning Based Siamese Neural Network Using Entropy Features for Ransomware Classification," *Computers & Security* 117 (2022): 102691.

61. "Unknown, Change Healthcare, a Healthcare Technology and Business Solutions Company," — changehealthcare.com (2025), https://www.changehealthcare.com/.

62. "Welcome to UnitedHealth Group," — unitedhealthgroup.com (2025), https://www.unitedhealthgroup.com/.

63. "eClaims — TELUS Health," — telus.com (2025), https://www.telus.com/en/health/health-professionals/allied-healthcare-professionals/eclaims.

64. K. L. Schwartz, N. Jembere, M. A. Campitelli, S. A. Buchan, H. Chung, and J. C. Kwong, "Using Physician Billing Claims From the Ontario Health Insurance Plan to Determine Individual Influenza Vaccination Status: An Updated Validation Study," *CMAJ Open* 4, no. 3 (2016): E463–E470.

65. S. Prinja, Y. Chugh, B. Garg, and L. Guinness, "National Hospital Costing Systems Matter for Universal Healthcare: The India PM-JAY Experience," *BMJ Global Health* 8, no. 11 (2023): e012987.

25778196, 2025, 8, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/eng2.70315 by Mazharul Islam - Bangladesh Hinari NPL , Wiley Online Library on [18/02/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License