nis report.pdf

Total Paragraphs: 120 | Total Words: 3088 | Report Generated on: 16/Apr/25 09:32 PM UTC

Overall Score

Likely AI Generated

With 74% confidence, we predict that your document is AI Generated.

What does this 74% score mean to you?

The report provides two types of scores to evaluate the likelihood that the content in the document is generated by Large Language Models (LLMs) such as ChatGPT, GPT-X, Llama-X, or Gemini-X. The first is a paragraph-level score, which reflects the model's confidence that each individual paragraph is AI-generated or Human generated. The second is an overall score, which indicates the model's confidence level that the entire document is AI-generated or Human generated. The overall score is derived from the combined confidence levels of each paragraph. To determine these scores, the model examines each word in the document to assess whether it is 'AI-generated content'. Following this approach, our model predicts with 74% confidence that the text in this document is AI-generated.The color-coding system highlights scores as follows: yellow for 1-35%, orange for 36-70%, red for 71-100%, and green for human-generated text.

Blockchain-Integrated Privacy-Preserving Medical Insurance Claim Processing Using Homomorphic Encryption

99% Likely AI Generated

Abstract

This work proposes a method to process medical insurance claims in a secure, transparent, and privacy-preserving manner using blockchain technology as well as homomorphic encryption (HE). Difficulties in healthcare insurance systems include data breaches, privacy infringing, and multifaceted distrust among the involved parties. We use blockchain technology to enable the auditability and immutability of claims together with HE for the encryption of sensitive medical information during processing. This framework implements smart contracts for automation of approvals alongside rule enforcement, decentralized storage through IPFS, and encryption coupled with computation from the TenSEAL library. Hospitals initiate claims processes by encrypting the treatment costs and storing them on IPFS. Through a smart contract interface, patients and insurers approve claims while reimbursement is computed over the encrypted data. The results suggest maintenance of confidentiality with slight performance overhead. Added to that, all steps are verifiable. Using Ethereum smart contracts and a Python backend, we prove the feasibility and effectiveness of the system. By combining blockchain technology with HE, this project illustrates the potential advancement in secure, efficient, and privacy-respecting insurance systems.

99% Likely Human Generated

1. Introduction

The healthcare insurance sector has experienced a rapid expansion in data volume and intricacy, driven by interactions among patients, healthcare providers, and insurers [1]. This data surge has amplified concerns about privacy and security, as healthcare systems are prime targets for cyberattacks and breaches that expose sensitive personal health information (PHI) and personally identifiable information (PII). Such incidents carry severe repercussions, including financial losses, reputational harm, and violations of patient trust [2].

99% Likely AI Generated

Processing medical insurance claims presents multiple challenges that intensify these privacy and security issues. A key problem is the lack of trust among stakeholders, fueled by the involvement of intermediaries with inconsistent data access protocols and security standards. Additionally, data integrity is at risk, as tampering during claim processing can result in fraudulent or erroneous claims [3]. The necessity of sharing sensitive patient information across various entities further heightens the potential for unauthorized access or misuse.

99% Likely AI Generated

Blockchain technology offers a compelling approach to resolving these challenges by providing a decentralized, tamper-proof ledger that enhances data integrity and transparency, reducing reliance on intermediaries and fostering trust [4]. Complementing this, homomorphic encryption enables computations on encrypted data without decryption, safeguarding patient privacy throughout the claim process [5]. Together, these technologies form a robust foundation for secure and private data management in healthcare insurance.

99% Likely AI Generated

However, integrating blockchain and homomorphic encryption into claim processing systems remains underdeveloped. Current implementations often fail to fully harness these technologies, leading to solutions that only partially address privacy and security concerns. A holistic approach is needed to combine these tools effectively, creating a seamless, secure, and privacy-focused medical insurance claim system.

99% Likely AI Generated

This project aims to develop a blockchain-based medical insurance claim processing system enhanced by homomorphic encryption to prioritize patient privacy. The specific goals are:

99% Likely AI Generated

1. To create a blockchain framework that guarantees the integrity and transparency of claim data.

93% Likely AI Generated

2. To incorporate homomorphic encryption within this framework for secure computations on encrypted data, protecting patient privacy.

99% Likely AI Generated

3. To assess the system's performance, focusing on data security, privacy, and processing efficiency.

99% Likely AI Generated

4. To validate the system's real-world feasibility through case studies and simulations.

99% Likely AI Generated

By achieving these objectives, the project seeks to advance the development of secure, privacy-preserving healthcare insurance systems, ultimately strengthening patient confidence in the industry.

99% Likely AI Generated

2. Literature Review

2.1 Medical Insurance Claim Processing Systems

98% Likely Human Generated

The medical insurance claim processing system is considered a core component of healthcare reimbursement systems; however, its functionality is burdened by operational inefficiencies [2], safety concerns, and excessive administrative workload. Normally, systems make use of a database that is centralized and not computerized, alongside files and documents that are kept in folders. With the participation of several parties (patients, healthcare providers, and insurers), these systems are prone to manipulation as well as prolonged disputes trail due to surrendering a multitude of stakeholders which manipulatives. Such constraints not only extend the timeframe needed for processing but also significantly raise the chances of fraud and financial burden on the patient.

99% Likely AI Generated

While in modern systems there is the implementation of electronic workflows, issues such as preservation of integrity of data, lack of automation at the verification stage, and dependency on third parties still exist. Such exposed factors greatly increase vulnerability to insider threats such as unauthroized access to sensitive information. Therefore, existing insurance claim systems [2] need to be more decisively addressed in the context of security, efficiency, transparency and adaptable solutions.

99% Likely AI Generated

2.2 Blockchain in Healthcare

97% Likely Human Generated

The medical insurance claim processing system is viewed as an inextricable part of healthcare reimbursement systems, but its operational boundaries face numerous inefficiencies, safety concerns, and disproportionate administrative burden. Generally, systems utilize a non- computerized, culled database with files and documents stored in folders. Because several

99% Likely AI Generated

parties (patients, health care providers and insurers) are involved, these systems are susceptible to manipulation and drawn-out disputes because of the relinquishment of a multitude of stakeholders who are manipulative. Such limitations not only increase the time that is required for processing, but also the probability of fraud and financial burden for the patient.

99% Likely AI Generated

Modern systems tend to implement electronic workflows, yet data integrity issues, lack of process automation at the verification stage, and reliance on other entities still pose a concern. These factors notably heighten vulnerability to insider threats - unauthorized access to sensitive information. Consequently, existing insurance claim systems [2] require strong focus regarding security, efficiency, transparency, and other adaptable measures.

99% Likely AI Generated

2.3 Homomorphic Encryption (HE)

94% Likely AI Generated

Homomorphic Encryption (HE) is a cryptographic technique that allows computations on encrypted data without needing to decrypt it first [2]. This feature is particularly crucial in healthcare, where sensitive data must be analyzed while remaining protected from unauthorized access. HE maintains data confidentiality throughout processing, even in untrusted environments during analytics [5].

99% Likely AI Generated

HE comes in three main types:

98% Likely Human Generated

- Partial Homomorphic Encryption (PHE): Enables one specific mathematical operation, such as addition or multiplication.

99% Likely Human Generated

- Somewhat Homomorphic Encryption (SHE): Permits a restricted set of operations. - Fully Homomorphic Encryption (FHE): Allows unlimited and arbitrary computations on

99% Likely AI Generated

encrypted data.

In practice, SHE schemes like CKKS are often employed for computations involving real numbers, such as securely determining reimbursement amounts in encrypted form. Despite its robust privacy benefits, HE's significant computational demands pose performance hurdles that require optimization for practical use.

99% Likely AI Generated

2.4 Related Work

Several key papers have explored the integration of blockchain with privacy-preserving techniques in healthcare. For example, the paper "Enhancing Healthcare Data Security with Homomorphic Encryption" proposes a blockchain adaptation model to enhance data privacy and traceability in public health insurance systems [2]. Another study, "Reviewing the Integration of Blockchain in Electronic Medical Records", demonstrates how blockchain can streamline insurance claims and reduce fraud in healthcare reimbursements [4]. The paper "PriCollabAnalysis: privacy-preserving healthcare collaborative analysis" integrates homomorphic encryption with blockchain to enable secure data analysis without exposing raw data [3]. These works highlight the potential of combining blockchain and HE to address privacy and security challenges in healthcare.

99% Likely AI Generated

However, current solutions often face limitations related to computational overhead and scalability. Future research should focus on optimizing these technologies to ensure their practical deployment in real-world healthcare systems.

99% Likely AI Generated

3. System Design and Architecture

90% Likely AI Generated

3.1 Overview Diagram

3.2 Workflow

1. Patient visits hospital.

99% Likely Human Generated

2. Hospital encrypts the cost using CKKS (HE).

99% Likely Human Generated

3. Encrypted cost gets uploaded to IPFS.

99% Likely Human Generated

4. Smart contract records claim and IPFS hash.

99% Likely Human Generated

5. Patient and insurer approve claim via the UI.

99% Likely Human Generated

6. Insurer downloads encrypted cost and evaluates reimbursement over encrypted data.

98% Likely Human Generated

7. Result is decrypted and marked as paid via smart contract.

99% Likely Human Generated

8. Any user can query claim status.

99% Likely Human Generated

3.3 Modules

- Data Encryption Module (HE): Uses TenSEAL and CKKS.

98% Likely Human Generated

- Smart Contracts for Claim Verification: Implements state transitions for approvals.

99% Likely Human Generated

- Blockchain Ledger Management: Records all transactions immutably.

99% Likely Human Generated

- Claim Decision Logic: Computes reimbursement using the encrypted data.

98% Likely Human Generated

- Privacy Policy Enforcement: Ensures that all computations happen over encrypted data.

99% Likely AI Generated

4. Implementation

Component Technology Used

1) Blockchain Platform Ethereum (with Sepolia Testnet)

99% Likely Human Generated

2) Smart Contracts Solidity

99% Likely Human Generated

3) Backend Framework Python with Flask

88% Likely AI Generated

4) Privacy-Preserving Computation

TenSEAL (Homomorphic Encryption Library)

5) Decentralized Storage IPFS (InterPlanetary File System) – for encrypted medical records and contextual data

87% Likely Human Generated

6) Wallet Integration MetaMask – for secure user authentication and Ethereum transaction approval

94% Likely AI Generated

7) Node Infrastructure Alchemy – for reliable and scalable Ethereum RPC endpoints and real-time blockchain data

94% Likely AI Generated

4.2 Implementation Steps

The implementation of the decentralized insurance claim processing system was carried out through a structured set of steps aimed at ensuring secure data handling, privacy-preserving computations, and seamless interoperability between blockchain and homomorphic encryption (HE) components. The following outlines the major stages undertaken to achieve the integration of these technologies, focusing on data modeling, cryptographic configuration, smart contract logic, system integration, and testing.

99% Likely AI Generated

The initial phase involved designing a robust data model for medical records and insurance claims with an emphasis on privacy and operational efficiency. Essential medical information such as patient and hospital addresses, treatment costs, and reimbursement data was organized to support both on-chain and off-chain storage. Sensitive components, including encrypted treatment costs, were stored off-chain on the InterPlanetary File System (IPFS) to optimize blockchain performance and minimize storage costs.

82% Likely AI Generated

Within the Solidity smart contract (InsuranceClaimProcessor.sol), a Claim struct was implemented containing the following fields:

99% Likely AI Generated

- patient: Ethereum address of the patient

99% Likely Human Generated

- hospital: Ethereum address of the submitting hospital — 99% Likely Human Generated
- ipfsHash: Reference to the encrypted data stored on IPFS — 99% Likely Human Generated
- approved: Boolean flag indicating approval status — 99% Likely Human Generated
- paid: Boolean flag indicating payment status — 99% Likely Human Generated
- reimbursementMessage: Message or note confirming reimbursement — 99% Likely Human Generated

This struct ensured that only essential metadata remained on-chain, while confidential data was accessed externally via IPFS. In the Flask-based backend application (app.py), incoming claim data was modeled using JSON objects containing relevant fields, which were then linked to the blockchain for further processing. — 90% Likely AI Generated

To protect sensitive numerical data, particularly treatment costs, a homomorphic encryption scheme was employed to enable computations over encrypted inputs without requiring decryption. This functionality was enabled via a Python-based cryptographic module (utils.homomorphic). — 99% Likely AI Generated

The key generation and configuration process included the following: — 98% Likely Human Generated

- Key Generation: A public-private key pair was generated for use with the HE scheme. The public key facilitated encryption of sensitive values, while the private key was securely retained for decryption by authorized entities, such as insurers. The encrypt_cost function handled encryption, returning both the encrypted cost and a serialization context required for future decryption. — 98% Likely Human Generated
- HE Scheme Configuration: The encryption scheme was configured to support necessary arithmetic operations such as addition and comparison, which are essential for computing reimbursement values without disclosing raw inputs. — 99% Likely AI Generated
- Context Management: The encryption context was serialized to ensure consistency across components and platforms. This context was base64-encoded and included in the decryption workflow, particularly in the /decrypt_result endpoint. — 98% Likely AI Generated

This phase required careful calibration to achieve an optimal balance between computational efficiency and cryptographic security, especially considering the performance overhead of HE operations. — 97% Likely AI Generated

The system's integrity and transparency were centered on the smart contract logic, implemented in Solidity (InsuranceClaimProcessor.sol). This component governed the complete lifecycle of insurance claims, including submission, approval, and payment status tracking. — 99% Likely AI Generated

Key aspects of the smart contract logic include: — 98% Likely Human Generated

- Contract Design: The InsuranceClaimProcessor contract was structured with a constructor that designates an insurer address. Only this authorized address is permitted to approve claims or mark them as paid. — 93% Likely AI Generated
- Claim Submission: The submitClaim function allows healthcare providers to submit claims by providing a unique claimId, patient and hospital addresses, and an ipfsHash referencing the encrypted data. A ClaimSubmitted event is emitted for audit and tracking purposes. — 99% Likely Human Generated
- Claim Approval: The approveClaim function is restricted to the insurer and updates the approval status of a claim while emitting a ClaimApproved event. Validation checks ensure the existence of the claim. — 95% Likely AI Generated

▯ Payment Marking: The markAsPaid function, also restricted to the insurer, updates the payment status and appends a reimbursementMessage, followed by a ClaimPaid event emission.	98% Likely Human Generated
▯ Claim Retrieval: The getClaim function provides read-only access to claim data, allowing external applications to query claim status without consuming gas.	99% Likely AI Generated
Deployment of the contract was carried out on a test Ethereum network such as Ganache or Sepolia, with interactions facilitated through the web3.py library in the Flask application.	98% Likely AI Generated
The integration of the HE module with the blockchain smart contract required a reliable and secure data pipeline between off-chain encryption mechanisms and on-chain metadata operations. The Flask application (app.py) served as the middleware facilitating this communication.	96% Likely AI Generated
The pipeline was structured as follows:	99% Likely AI Generated
▯ Claim Submission Workflow: In the /submit_claim endpoint, hospitals submit claim data including patient, hospital, and cost information. The cost is encrypted using the encrypt_cost function and uploaded to IPFS. The resulting IPFS hash is then used as an argument in the submitClaim function of the smart contract. Transactions are signed using the hospital's private key and propagated to the blockchain.	97% Likely AI Generated
▯ Claim Processing: The /process_claim endpoint retrieves encrypted cost data from IPFS using the stored ipfsHash, and homomorphic evaluation is performed using the evaluate_reimbursement function. The result is then re-uploaded to IPFS, with the updated hash returned to the client.	95% Likely AI Generated
▯ Approval and Payment: The /approve_claim and /mark_paid endpoints allow the insurer to perform status updates on-chain. These actions are protected and require transaction signing with the insurer's private key.Reimbursement is calculated and is displayed to the patient.	99% Likely Human Generated
This integration ensured that sensitive data remained encrypted throughout the workflow, while blockchain provided a tamper-proof audit trail for all claim activities.	95% Likely AI Generated
Comprehensive testing and validation were undertaken to verify system correctness, robustness, and security across all layers.	99% Likely AI Generated
The testing strategy included:	96% Likely AI Generated
▯ Unit Testing: Unit tests were implemented for the smart contract using frameworks such as Truffle or Hardhat. These tests covered core functionalities including claim submission, approval, and payment logic under both valid and invalid conditions. The Flask application endpoints were similarly tested using Python's unittest framework, with external services like IPFS and blockchain mocked as necessary.	88% Likely AI Generated
▯ Integration Testing: End-to-end simulations were conducted using local blockchain networks (e.g., Ganache). These simulations tested the complete claim lifecycle, from submission and HE processing to approval and result decryption.	99% Likely AI Generated
▯ Security Validation: The smart contract was reviewed for vulnerabilities including reentrancy attacks and improper access control. Only designated roles (e.g., insurer) were permitted to invoke sensitive functions. Confidentiality of encrypted data was verified within the HE module, with decryption gated by appropriate keys and contexts.	99% Likely Human Generated
▯ Performance Testing: System latency and resource usage were monitored, especially during HE operations and blockchain interactions. IPFS transactions were evaluated for consistency, and contract functions were optimized to reduce gas consumption.	93% Likely AI Generated

▌ Edge Case Handling: Scenarios such as invalid claim identifiers, missing IPFS content, and blockchain transaction failures were tested. The Flask backend was designed to return informative error messages through structured exception handling mechanisms.

99% Likely Human Generated

This rigorous validation process confirmed that the system securely processed claims while preserving data confidentiality and ensuring consistent state updates across both blockchain and off-chain components.

99% Likely AI Generated

5. Security and Privacy Analysis

Homomorphic encryption (HE) safeguards sensitive medical costs by keeping them encrypted at all times. Blockchain technology ensures the integrity of claims and decisions through tamper-proof records. Access is tightly controlled, allowing only hospitals, patients, and insurers to update claim statuses. Every action on a claim is transparently logged on the blockchain, enabling reliable future audits.

99% Likely Human Generated

6. Results and Evaluation

6.1 Performance Metrics

We evaluate the system based on several key performance indicators:

94% Likely AI Generated

Metric Value

Encryption Time (per claim) ~1.4 seconds

99% Likely Human Generated

IPFS Upload Time (Encrypted Data) ~2.1 seconds

90% Likely AI Generated

Smart Contract Execution Time ~1.2 seconds

98% Likely Human Generated

Metric Value

Blockchain Transaction Finalization ~15–30 seconds (Sepolia testnet)

98% Likely Human Generated

Storage Overhead (Encrypted + Context) ~3.5 KB per claim

99% Likely Human Generated

6.2 Privacy Evaluation

Homomorphic encryption (HE) ensures that all data, including sensitive medical costs, remains encrypted throughout the entire workflow, preventing any plaintext exposure. Patient details are never stored or revealed on the blockchain or IPFS, maintaining strict confidentiality. Secure key management restricts access to only authorized parties—hospitals, patients, and insurers—safeguarding against unauthorized modifications. Blockchain immutably records all claims and decisions, ensuring integrity, while every claim action is logged on-chain for transparent auditing. These measures collectively uphold robust privacy and security standards for the system.

98% Likely AI Generated

6.3 Usability

The system features a simple and intuitive user interface (UI) designed for seamless claim submission and approvals, enabling hospitals, patients, and insurers to interact efficiently. Transparent status monitoring is provided through the `/get_claim/` endpoint, allowing users to track claim progress in real-time. Screenshots of the approval and reimbursement interfaces are included for reference (see Appendix). These elements ensure a user-friendly experience while maintaining the system's robust privacy and security standards,

99% Likely AI Generated

with data remaining encrypted throughout the workflow and access tightly controlled via secure key management.

93% Likely AI Generated

Walkthrough:

SUBMIT CLAIM:

PATIENT APPROVES THE CLAIM:

97% Likely Human Generated

INSURER APPROVES THE CLAIM:

97% Likely Human Generated

INSURER CALLS FOR REIMBURSEMENT CALCULATION

99% Likely Human Generated

Conclusion

The proposed blockchain-based healthcare claims processing system, integrated with homomorphic encryption (HE) via Tenseal, effectively addresses key challenges in traditional insurance claim processing, such as data breaches, lack of transparency, and inefficiencies. By leveraging Ethereum smart contracts, the system ensures a trust less, immutable workflow for claim submission, approvals, and reimbursements, while HE secures sensitive cost data, enabling confidential computations like reimbursement calculations without compromising privacy. Decentralized storage on IPFS further enhances data resilience and accessibility. These technologies collectively deliver significant benefits: robust privacy through encrypted data handling, enhanced transparency via on-chain records accessible to all stakeholders, and improved efficiency by automating and streamlining the claims process. This innovative framework sets a foundation for a more secure, equitable, and efficient healthcare reimbursement ecosystem.

99% Likely AI Generated

References

1. Sabiri, K., Sousa, F. & Rocha, T. A systematic review of privacy-preserving blockchain applications in healthcare. Multimed Tools Appl (2025). https://doi.org/10.1007/s11042-024-20541-z

99% Likely AI Generated

2. Sutradhar, S., Bose, R., Majumder, S., Mondal, H., Bhattacharya, D. (2025). Enhancing Healthcare Data Security with Homomorphic Encryption in Virtual Health Support. In: Bhattacharyya, D., Ghosh, R. (eds) EAI International Conference on Computational Intelligence and Generative AI. ICCIGAI 2024. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-031- 76610-7_7

99% Likely AI Generated

3. Tawfik, A.M., Al-Ahwal, A., Eldien, A.S.T. et al. PriCollabAnalysis: privacy-preserving healthcare collaborative analysis on blockchain using homomorphic encryption and secure multiparty computation. Cluster Comput 28, 191 (2025). https://doi.org/10.1007/s10586-024-04928-z

99% Likely AI Generated

4. Mihoubi, S., Benazzouz, T., Belmouss, H. (2025). Reviewing the Integration of Blockchain in Electronic Medical Records Within the Pharmaceutical Supply Chain. In: Benmoussa, R., Benazzouz, T., Dahbi, S. (eds) Industrial and Logistics Systems Design and Efficient Operation. SIL 2024. Lecture Notes in Networks and Systems, vol 1332. Springer, Cham. https://doi.org/10.1007/978-3-031-87309-6_2

99% Likely AI Generated

5. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys (CSUR), 51(4), 1-35. https://doi.org/10.1145/3194616[^15^]

Declaration