Online at: https://researchtrendsjournal.com
Indexed Journal

ISSN No: 2584-282X
Peer Reviewed Journal

INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Volume 3; Issue 1; 2025; Page No. 216-223

Received: 11-10-2024
Accepted: 19-11-2024

A Model and Algorithm for a Car Insurance System Using Machine Learning and Distributed Ledger Technology

[1]Pramod Kumar Yadav and [2]Dr. Prince Jain

[1]Research Scholar, Mahakaushal University, Jabalpur, Madhya Pradesh, India
[2]Professor, Mahakaushal University, Jabalpur, Madhya Pradesh, India

DOI: https://doi.org/10.5281/zenodo.18383964

Corresponding Author: Pramod Kumar Yadav

Abstract

Blockchain technology has significant applications in medicine, particularly in ensuring the confidentiality of medical records and enhancing the transparency of healthcare data management. Rapid digitalization in healthcare presents challenges related to interoperability and privacy, which traditional centralized systems struggle to address. Blockchain, as immutable and distributed ledger technology initially designed for cryptocurrencies, offers a solution by securing and decentralizing healthcare data management. The NAIBHSC framework exemplifies this integration, utilizing blockchain alongside IoT, cloud computing, and AI to enhance the supply chain management of healthcare products and electronic health records. Additionally, its implementation in car insurance systems showcases automated damage identification and secure premium transactions. The study concludes that by combining blockchain with modern technologies, solutions can be developed that enhance security, transparency, and efficiency across various domains, ultimately fostering trust and innovation within critical industries.

Keywords: Blockchain, data, personalized car insurance, privacy preservation

Introduction

The Telecare Medicine Information System (TMIS) is a product of the revolutionary growth of information and communication technologies that allows medical treatment to be delivered directly to patients. By facilitating communication between patients and other medical professionals, the TMIS enables clinicians to offer remote medical support, including the ability to discuss patients' illnesses. The TMIS can significantly lower treatment costs in this manner. Through the utilization of current medical records, this method enables precise disease diagnostic decisions. On the other hand, there are restrictions to this method in terms of making decisions for new patients whose health records do not contain their medical history or other relevant data. Electronic health records (EHRs) provide a solution to this problem by storing all relevant data in one place. This includes data pertaining to patients, scan reports, clinical notes, sensors, billing information, prescriptions, medical history, insurance, and more. There would be problems with data security and privacy when sharing this kind of record. The healthcare industry has been at the forefront of recent developments in wearable device technology and the IoT. The cloud saved information from all the wearable gadgets., which can offer useful insights and large amounts of health data. The health monitoring, disease diagnosis, and treatment processes are all enhanced by the integration of this data with the EHR.

A standardized digital record that contains healthcare information for groups and individuals is known as a health record stored digitally. Medical records stored digitally were originally intended to improve hospital data management and supplant paper-based medical records. Following that, with more and more people worrying about their own health, it became necessary for the general public to have permission to see their own health data. Thus, EHRs offer a novel approach to healthcare data organization that is both innovative and tailored to each individual.

Electronic health records and medical records provide

several benefits to healthcare, including enhanced security and a better user experience. However, it was thought that Blockchain technology would solve certain security issues. When applied to healthcare, blockchain technology creates an immutable ledger of patient records. Paper medical records have a number of drawbacks that this technology can help eliminate, including inefficiency, security risks, impurity, disorganization, duplication, and redundancy. Those who are fighting for the privacy of blockchain transactions argue that the relevant patient populations should not be able to easily trace their status.

Tokenization, a technique for making merely a representation of the release of delicate data while safeguarding the confidentiality of the first, sensitive data packet, is suggested as a means to do this. In addition, it specifies that medical records must be kept off the blockchain in a safe environment. One common use case for this blockchain is storing references to entries in an Access database., so it's important that the database is safeguarded separately. By encapsulating data in the database, our architecture ensures data security on blockchain as well.

Literature Review

Aivar *et al*. (2025) [7] One possible solution to the three most important issues in healthcare today Concerns about data breaches, patient autonomy, and interoperability may be addressed using blockchain technology. Three areas where blockchain technology is being used include electronic health records, clinical trials, and pharmaceutical supply chain traceability. technology that are examined in this research. In their discussion of smart contract shortcomings, regulatory compliance, and security concerns, the authors provide solutions like as enhanced encryption and more effective consensus procedures. Two practical instances demonstrating the potential for enhanced security and transparency are medical chain and Medi Ledger, both created by Chronicled.

Swaraj *et al*. (2021) [8] The usage of medical applications, both by professionals and by patients themselves, is on the rise. Existing solutions for exchanging data from health records and the IoT are riddled with privacy and security issues. A method that addresses all of these concerns is one that use blockchain technology in conjunction with There is a safe and privacy-conscious file sharing system called IPFS (Inter Planetary File System). electronic health record.

Vipin *et al*. (2025) [9] Data storage and security in the cloud has been revolutionized by blockchain technology. Its original use was as a basis for digital currencies like Bitcoin-a decentralized, immutable record of financial transactions-but its reach has now expanded to include protecting patients' personal health information. Blockchain technology depends on mining to ensure data validity and immutability. Building a system that securely stores and manages patient The primary objective is to digitalize medical records using blockchain technology. initiative. Keeping patients' medical records safe and securely and mining blocks on a blockchain.

Qingtao *et al*. (2024) [10] Public interest in the area of medical data informatization has expanded in step with the need such that electronic health records pertaining to individual patients are secure, easily manageable, and kept private. The distributed ledger technology known as blockchain has enormous potential as a novel method for the safe transmission of electronic health records. Protecting electronic medical records has prompted some researchers to suggest blockchain-based alternatives to fix the problems with traditional online medical data sharing in terms of security. This paper evaluates and summarizes the current schemes blockchain technology for the protection of electronic health records sharing in an effort to promote their further growth.

Fahad *et al*. (2021) [1] Connected Interconnected What is often referred to as the "Internet of Medical Things" (IoMT) consists of electronic health records, mobile applications, and other related technology. These medical devices and applications are linked to healthcare systems over the Internet. Some of the things that are involved with the IoMT, or Internet of Medical Things, include biggest problems include issues with scalability, data accessibility, and patient data security. Potentially changing the character of patient data, the blockchain in many ways, including its accessibility, interchangeability, accumulation, control, and contribution. Accordingly, this research proposes an IoMT-based health information blockchain-based secure data management system (BSDMF) to improve scalability, data accessibility, and secure patient data transfers.

Research Methodology

Proposed Novel Approach for Integrated Iot with Blockchain in Health Supply Chain (NAIBHSC) Approach

Supply chain network design

Each link associated with the supply chain contributes to the overall network, which includes suppliers, producers, merchants, damaged points, and consumers. The major goal of this network architecture in terms of product transit from manufacturer to consumer is to reduce the number of items that stay intact and the cost of the destination. A mathematical model with two goals allowed us to lessen not just the distance travelled and the expense of transportation. Both the list of parameters and the list of variables are included below.

Variables

1. Where the damage is located (d € D)
2. Placement of the end user (e € E)
3. Location of manufacturing (m € M)
4. Product or thing (p € P)
5. s suppliers (s € S)
6. The duration (t € T)

Novel Approach for Securing an Cloud-Based Electronic Health Record System Using Blockchain Technology

Proposed System Model

When working Safely transferring EHR data across authorized individuals using a shared cloud service is a major challenge. Existing EHR systems encountered issues with data privacy and security, including as data availability, decentralization of permission, data access, authentication of users, data integrity, and data availability confidentiality. The safe transfer of information among authorized users in a cloud setting was impeded by these obstacles.

System Architecture

The Private and health-related information about a patient information is included in each individual electronic health record (EHR) that makes up an EHR system. Medical records include both the Area ID and the Patient ID for each patient. Pictured in Figure 1 is an EHR platform that utilizes blockchain technology and operates in the cloud. The many parts that make it up are detailed in the following manner:

First Stage Data Upload

During the beginning of When data is uploaded, the owner of the data requests the establishment of a Blockchain from the Cloud Server (CS). After the request has been received, the EHR Manager verifies it CS. A signal is sent to the smart contract by the EHR administration to begin the verification process. This signal contains the upload request. Verification of the policy list is performed by the smart contract once it has visited the policy store

A Distributed Leger and Machine Learning System for Auto Insurance

In its most fundamental form, CIAS, as well as the Automobile Insurance Automation System, main components:

1. UCR stands for "user and vehicle registration..."
2. PP, or Premium Pay
3. Insurance Reimbursement (IS)
4. Payment Return (RT).

Results and Analysis

Novel Approach for Securing an Cloud-Based Electronic Health Record System Using Blockchain Technology Security and Privacy Performance Criteria

Table 1: Evaluation of our system's performance indicators in comparison to those of other works

Feature	Zhang [54]	BaDs' [55]	HealthTap [56]	Rifi [18]	Our system
Data confidentiality	No	No	No	Yes	Yes
Availability	No	No	Yes	Yes	Yes
Decentralized access	Yes		Yes	Yes	Yes
Data Authorization	Yes	No	Yes	No	Yes
User authentication	Yes	Yes	Yes	No	Yes
Data Integrity	Yes	Yes	Yes	Yes	Yes
Data privacy	Yes	Yes	Yes	Yes	Yes

The proposed method is assessed using a number of different security and privacy performance criteria, which are shown in Table 1. These metrics include data security, availability, authorization, decentralization of access, authentication of users, data integrity, and privacy. The results of this comparative investigation demonstrate that our method offers increased protection and privacy against a wide range of assaults and dangers.

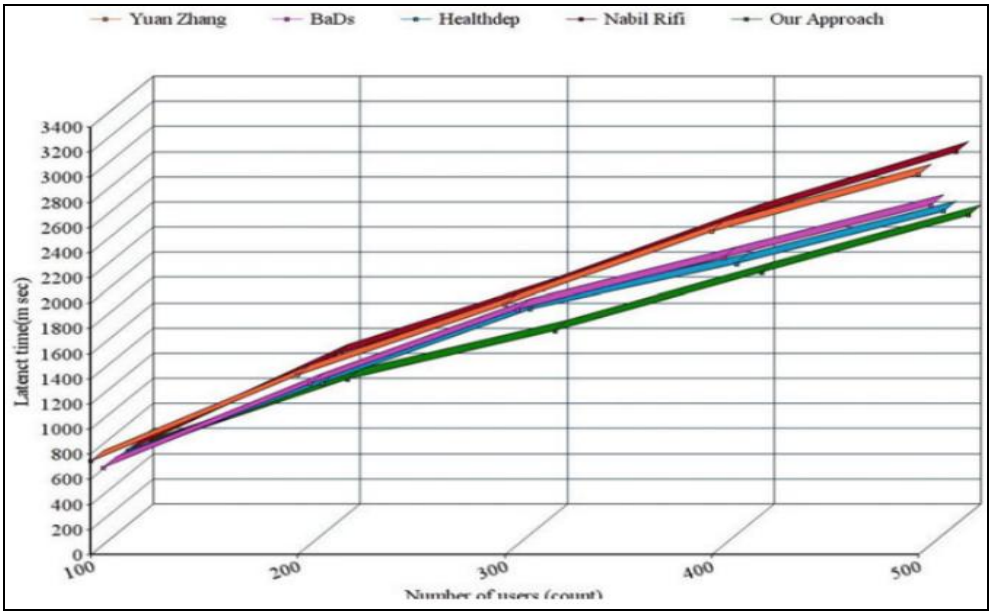

Fig 1: Latency time

The term "network latency" refers to the entire amount of time that elapses between the both the sender and the recipient as a means to transmit and process the request. In a cloud setting, the typical time needed to deal with a distinct number of requests is shown in Figure1. In terms of the performance of network latency, our technique demonstrates superior results when compared to other approaches that are currently in use.

Information Selection and Uploading: In order to upload and manage the data set, healthcare providers employ the personal health record (PHR) as part of this cloud function (Fig.2).

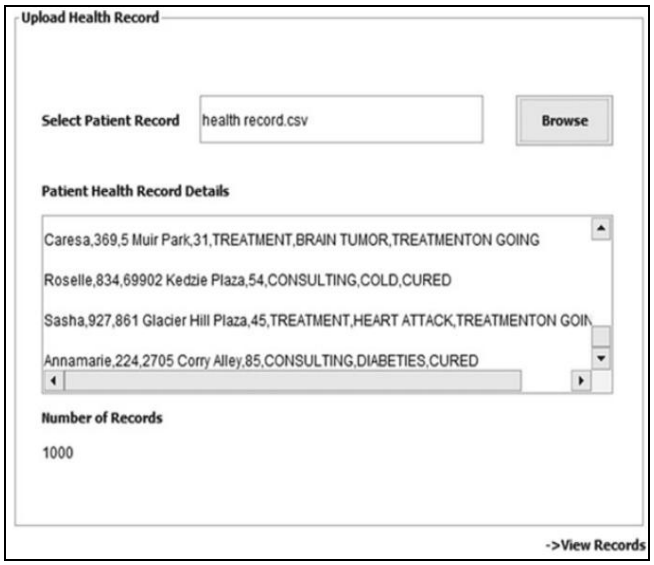

Fig 2: The process of selecting and submitting information

Key Generation and Encrypted Patient Records: An encryption operation is carried out on patients' data by the healthcare provider, using a key that the cloud provider establishes before the data is transferred to the cloud (Fig.3).

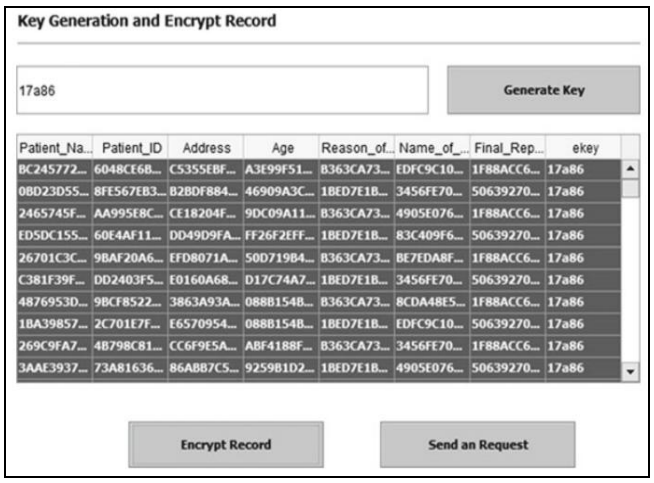

Fig 3: Secure patient data storage and key creation

View patient records: Once the data has been uploaded into the cloud, the healthcare professional will be able to examine the records of the patient. By making use of the patient-id, the data owner is able to readily get the records that are necessary (Fig.4).

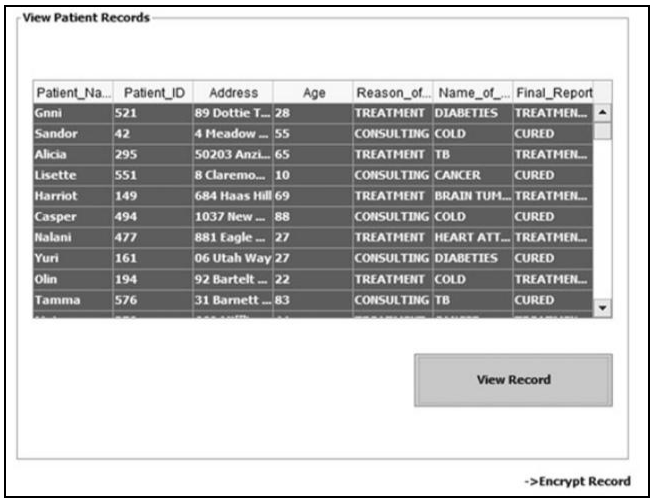

Fig 4: Examine the medical records of the patient

"Make a request to a server in the cloud." After finishing off with the encryption process, the healthcare provider will next submit a request to the cloud service provider (CSP) to create blocks and then store them in the cloud. When the request has been successfully sent to the CSP, By checking the patient's vitals, the doctor can determine the request using the verification key. This allows the provider to determine if the CSP has accepted, rejected, or is awaiting the current state (Fig.5).

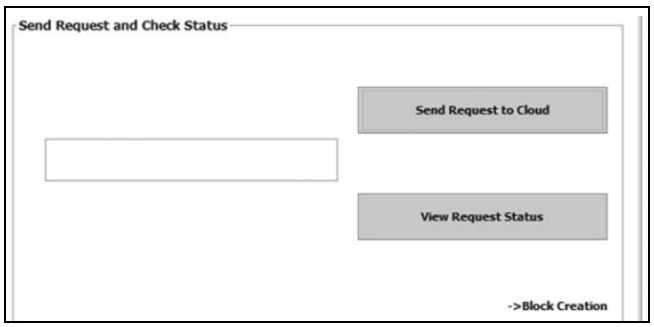

Fig 5: Submit a query to a server in the ether

Block Creation: Once the cloud service provider (CSP) gives the go-ahead, the healthcare provider may proceed with developing and building blocks, seeing block metadata, and uploading them as seen in Figure 6.

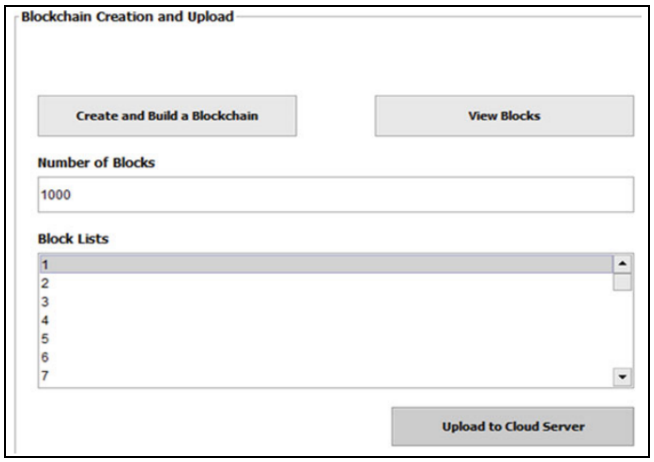

Fig 6: Building blocks

View Blocks: The number of blocks and the date that are formed are both shown in Figure 7, and we are also able to inspect those blocks. The information is recorded in each block, while the A timestamp is a brief piece of information that is uniquely serialized and stored in every block. To pinpoint exactly when the blockchain network validated and mined the block is the main function of the timestamp.

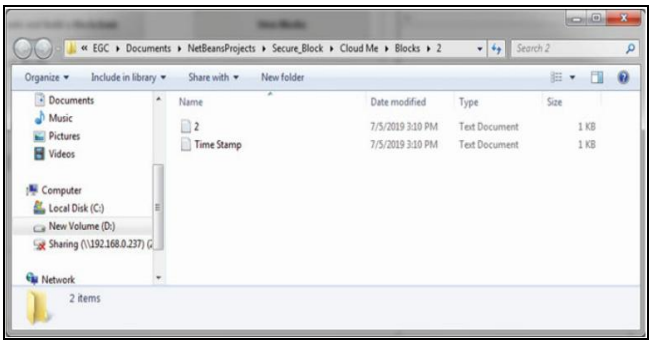

Fig 7: View blocks

Upload Acknowledgement: According to Figure 8 shows that after the information has been saved to the server in the cloud, the cloud service provider (CSP) will notify the healthcare provider.

Fig 8: Upload acknowledgements

A Distributed Leger and Machine Learning System for Auto Insurance

Auto insurance is a contract where drivers pay premiums to an insurance provider for coverage in case of accidents. The global expansion of vehicle insurance has paralleled the increase in registered vehicles, with India seeing over 295 million registrations as of the 2019 fiscal year. Legally, all vehicles must have insurance, leading to a rise in both claims and insured individuals. While user registration for vehicle insurance is quick, filing a claim is cumbersome, involving multiple intermediaries and processes: (1) the policyholder files a claim, (2) a damage assessment is conducted, and (3) the necessary documentation is submitted for reimbursement. This paper proposes an automated car insurance system that utilizes bitcoin for claims payments, starting with user registration and employing a PyTorch-based machine learning model to assess damages, eliminating the need for middlemen. Additionally, the reimbursement claim settlement involves verifying damages and processing payments via bitcoin on the Ethereum blockchain.

Data analysis

According to what was said before, the system is primarily made up of four components: the RC, the IS, the PP, and the UCR. The Insurance claim (IS) module utilizes computer vision and model-based machine learning for damage detection using the input picture from the user. Thanks to CIAS's integration with blockchain technology, users and insurance provider to make safe and verifiable payments back and forth. In the future lessons, we'll get further into this subject.

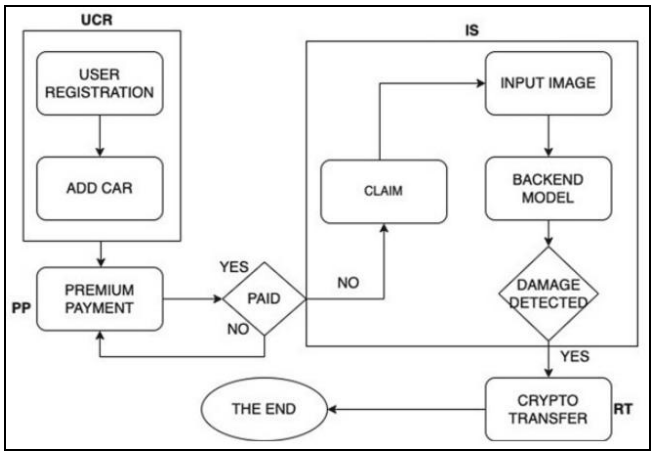

Fig 9: Complete description of the system architecture, including the components and operation of the RT, IS, UCR, and PP are the four modules.

The first and most important step in the CIAS is registering users and cars, as shown in Fig. 9. The insurance company hosts a website built on the REACT framework that uses Website markup languages as well as JavaScript, Cascading Style Sheets, and HTML. Users may register as clients when they provide the insurance business with the required information. At a later time, they will need to provide the registration of the vehicle they want to cover. The customer's Firebase is a safe place to save data. Looking at the premium payment (PP) process now that registration is complete.

Fig 10: Enhanced payment page with a QR code and an essential area for the verification of the transaction hash

As part of the premium payment process using bitcoin (ETH), blockchain technology is leveraged. A backend API retrieves the premium amount for a vehicle type and generates a QR code for payment. Upon scanning the QR code with the MetaMask wallet app, users are redirected to the payment page. After payment completion, a sixteen-digit transaction hash is generated. This hash undergoes verification through three checks: the shipping address must match the provider's information, the payment amount must be adequate, and fresh transaction IDs should be used to prevent fraud. Once verified, the transaction hash is stored in Firebase's database, confirming the user's insurance coverage.

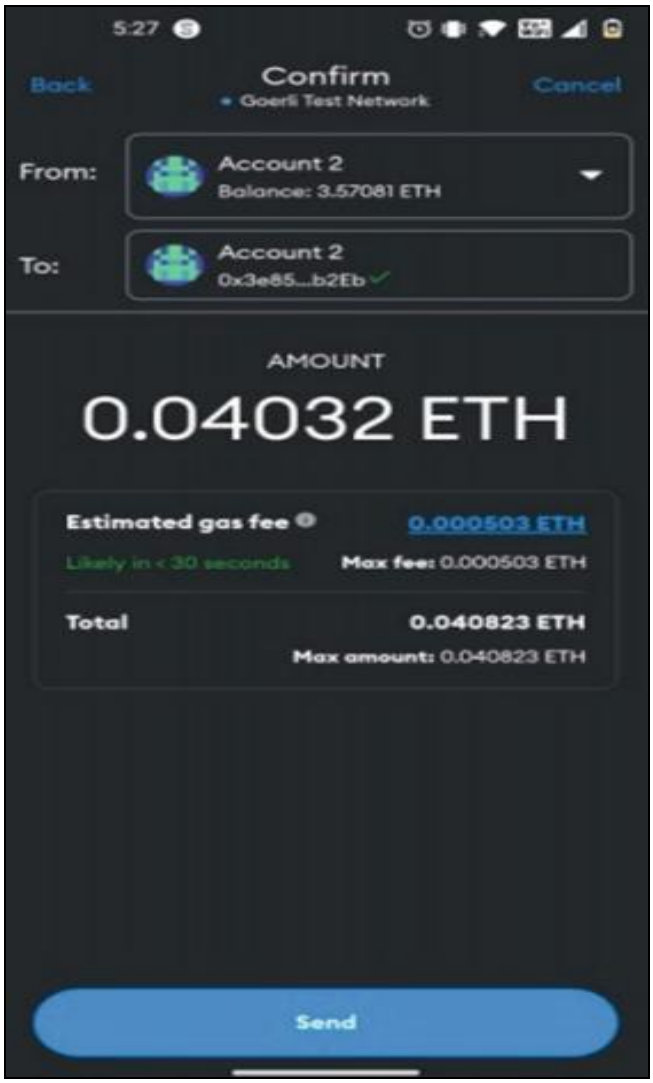

Fig 11: After the QR code has been scanned for payment, the payment page will appear in the MetaMask wallet app.

This brings us on to the Insurance Claim (IS) module, the third module. Figure 12 shows the user interface of the website that an active insurance user will view when submitting a claim for car damage. The client is then sent to a page where they may upload images of the damaged vehicle. In section 3.2, we'll go into more depth about how the machine learning instance segmentation model works after receiving the input image. running on the backend will identify the area of the damage and then provide it back to the user.

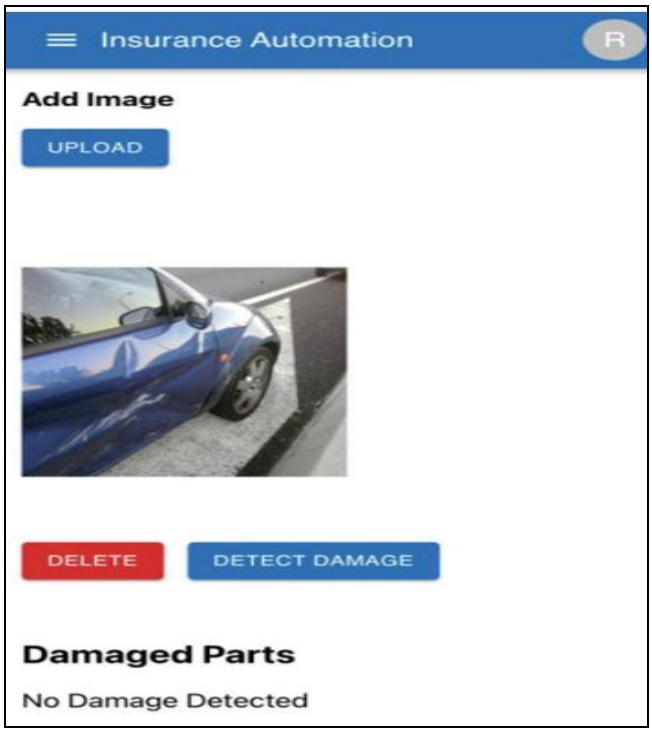

Fig 12: For the purpose of filing an insurance claim, a portal for uploading images

In the Reimbursement module, after notifying the user about the damage, the backend API retrieves the ETH amount to be sent for the damage to the specific automobile model from a firebase database with pricing data. A button appears for the user to claim the ETH, and upon pressing it, the funds are immediately transferred to their Metamask wallet through activated smart contracts, facilitated by blockchain technology.

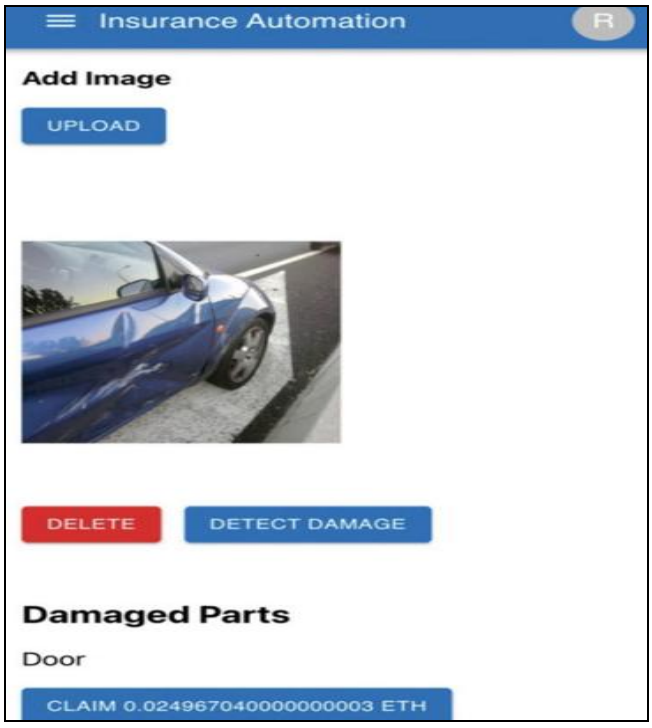

Fig 13: Once the damage has been determined and the amount of Ethereum required to be given for compensation, the output will be shown.

An AI-Powered Damage Detection System

Using computer vision methods and the cutting-edge object recognition "Detectron2" package created with the help of PyTorch by Facebook's AI Research (FAIR) team, the machine learning models presented in this work are constructed according to the principles of machine learning.

Fig 14: Only a small subset of the COCO Dataset's photos has been annotated with the word "damage."

Bounding outlines and segmentation markers are present in these images.

Fig 15: A selection of photos from the COCO Dataset have been annotated in five different ways: Doors, Hood, Front and Rear Bumpers, and Headlights.

The dataset used for model training and testing was formatted in COCO and consists of 80 photographs: 61 for training, 13 for validation, and 6 for testing. Annotations stored in JSON format include segmentation masks and bounding boxes, identifying damaged automotive components such as "Headlight," "Front Bumper," "Rear Bumper," "Hood," and "Door." Additionally, there is a single type of annotation indicating presence or absence of damage. Visualizations of segmentation and bounding boxes are provided in Figures 14 and 15, respectively.

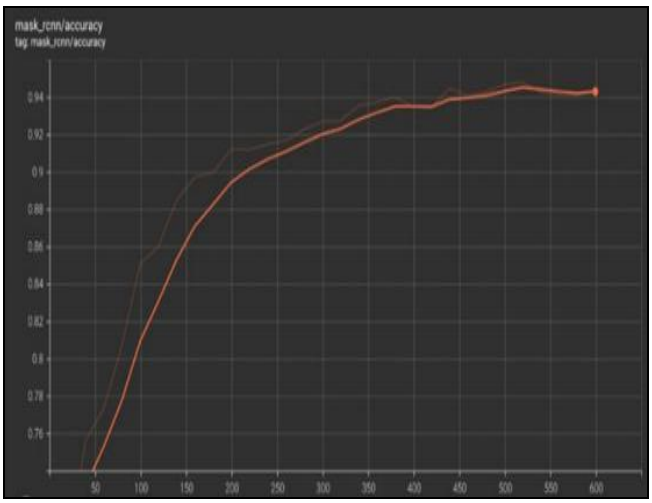

Fig 16: Shows the accuracy curve obtained from the mask_rcnn model after 600 iterations

cfg has been updated to include COCO Trainer for the purpose of training as can be seen in Figure 16, After 600 mask_rcnn achieved an accuracy of 94.4% after many successful repetitions.

Conclusion

This study demonstrates that the NAIBHSC framework effectively addresses key issues in healthcare supply chain management, such as counterfeit drugs, transparency, and stakeholder inefficiencies, which pose risks to patient safety and healthcare professionals. By leveraging blockchain technology and IoT devices like RFID tags and sensors, the system ensures product traceability and secures data on a tamper-proof ledger, fostering trust among all parties involved. Smart contracts further enhance the NAIBHSC ecosystem by automating verification and payment processes, minimizing errors and delays while providing accountability through documented actions. Performance analysis through benchmarking tools indicates that NAIBHSC offers superior throughput and reduced latency compared to traditional and existing blockchain models, confirming its technological scalability and effectiveness in real-world healthcare supply chain challenges.

References

1. Abbas A, Alroobaea R, Krichen M, Rubaiee S, Shanmuganathan V, Almansour F. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Personal and Ubiquitous Computing. 2021;28. doi:10.1007/s00779-021-01583-8.
2. Ad S, Damancharla H, Metta A. Enhancing data privacy in healthcare systems using blockchain technology. 2023.
3. Adapa CSR, Pub R. Blockchain-based master data management: a revolutionary approach to data security and integrity. International Journal of Information Technology and Management Information Systems. 2025;16:1061–1076. doi:10.34218/IJITMIS_16_02_067.
4. Agarwal C, Jha A, Anand V, Kumar A, Kasar M. A study to implement blockchain in health care. 2022.
5. Ahmad R, Salah K, Jayaraman R, Yaqoob I, Ellahham S, Omar M. The role of blockchain technology in telehealth and telemedicine. International Journal of Medical Informatics. 2021;148:104399. doi:10.1016/j.ijmedinf.2021.104399.
6. Alebaba DB, Hamzah M, Ghazali MF, Asli M. Bringing blockchain technology in innovating industries: a systematic review. In: Blockchain Technology and Applications. Cham: Springer; 2022. p. 1–? doi:10.1007/978-3-030-85990-9_33.
7. Shynar Y, Seitenov A, Kenzhegarina A, Kenzhetayev A, Kemel A, Ualiyev N, *et al*. Comprehensive analysis of blockchain technology in the healthcare sector and its security implications. International Journal of E-Health and Medical Communications. 2025;15:1–45. doi:10.4018/IJEHMC.372423.
8. Sabu S, Ramalingam HM, Vishaka M, Swapna HR, Hegde S. Implementation of a secure and privacy-aware e-health record and IoT data sharing using blockchain. Global Transitions Proceedings. 2021;2.

doi:10.1016/j.gltp.2021.08.033.
9. Kaushal P, Saxena V. Secure management of patient medical records using blockchain technology. Journal of Advances in Computer Science Engineering and Computer Science. 2025;40:77–87. doi:10.9734/jamcs/2025/v40i82033.
10. Qin M, Wu Q. A review of blockchain-based research on e-health data sharing. International Journal of Computer Science and Information Technology. 2024;3:37–43. doi:10.62051/ijcsit.v3n1.06.