iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.68225

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

A Blockchain-Based System for Secure and Transparent Healthcare Insurance Claim Authentication

Shruthi.P[1], Divya Mallikarjuna[2], Uthpala V S[3], Harini Yalipi[4]
Information Science & Engineering, RV Institute of Technology & Management

Abstract: ***The healthcare and insurance industries face significant challenges in data authenticity, fraud prevention, and secure processing. This paper presents a blockchain-based insurance claim authentication system that ensures transparency, security, and efficiency. The system facilitates seamless interactions among hospitals, insurance companies, and patients using Ganache, Truffle, MetaMask, and Django. It leverages cryptographic methods, digital signatures, and smart contracts to validate transactions, thereby enhancing trust and minimizing manual errors.***
Keywords: Blockchain, Digital Signature, Smart Contracts, Insurance Claims, Fraud Prevention, Data Security, Decentralized Applications

I. INTRODUCTION

Advancements in blockchain technology have transformed data security, transparency, and automation across various industries, particularly in healthcare and insurance, where traditional claim processing systems often suffer from inefficiencies, fraud, and lack of transparency due to centralized control and manual verification. This paper presents a blockchain-based insurance claim authentication system that ensures data authenticity, fraud prevention, and efficient processing of insurance claims by leveraging smart contracts and cryptographic techniques to automate key operations such as bill verification and policy validation. Implemented using Ganache, Truffle, MetaMask, and Django, the system provides seamless interactions among three primary portals: the Hospital, the Insurance Company Portal, and the Patient Portal, with digital signatures and cryptographic hashing mechanisms ensuring the integrity and security of each transaction while mitigating risks associated with data manipulation and unauthorized modifications. Beyond enhancing security, the blockchain-based approach streamlines claim processing by reducing dependency on intermediaries, minimizing human errors, and accelerating verification times, with the decentralized nature of the system fostering trust between stakeholders and ensuring that insurance claims are authenticated transparently and efficiently, ultimately underscoring blockchain's potential to revolutionize insurance claim authentication by driving greater efficiency, security, and reliability in the industry as adoption continues to expand.

II. LITERATURE REVEIW

Blockchain has numerous benefits such as decentralisation, persistency, anonymity and auditability. There is a wide spectrum of blockchain applications ranging from cryptocurrency, financial services, risk management, Internet of Things (IoT) to public and social services. Although a number of studies focus on using the blockchain technology in various application aspects, there is no comprehensive survey on the blockchain technology in both technological and application perspectives. To fill this gap, conducting a comprehensive survey on the blockchain technology is necessary. The author presents a blockchain taxonomy, explores typical consensus algorithms, reviews various applications, and discusses technical challenges along with recent advancements in addressing them[1].

Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company, or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published. This document provides a high level technical overview of blockchain technology. The purpose is to help readers understand how blockchain technology works[2].

On top of distributed computing, Bitcoin was implemented as cryptocurrency. Bitcoin originally came with blockchain technology to protect coins from misuse. Blockchain provided a distributed ledger of cryptocurrency transactions in an immutable form to protect data from malicious attacks. Thus blockchain complemented the security aspect of Bitcoin. In the later stages, blockchain evolved as a distributed ledger technology that is used in different domains like healthcare. There are different issues associated with different domains. For instance, in the insurance domain, there are issues related to false claims and the claims that are manipulated by competent authority illegally. This problem addressed in this paper by implementing an insurance application with blockchain technology. The consensus is used to ensure that the claim process of the insurance company will be carried out with integrity, accountability, and non-repudiation. Especially, every transaction is cryptographically signed and stored as a collection of blocks in the blockchain. This approach safeguards claim transactions and prevent any fraudulent attempts. A prototype application is built using the IBM blockchain platform and its underlying components. Experimental results showed that the proposed implementation prevents fraud claims in the insurance industry.The advent of blockchain technology has introduced promising solutions to many of the challenges faced by the healthcare and insurance sectors, particularly in managing insurance claims. These systems often suffer from issues such as fraud, delays in claim processing, lack of data transparency, and security concerns regarding patient information. By leveraging the immutability and decentralization of blockchain, several recent studies have demonstrated how these problems can be effectively addressed. This review draws upon key advancements in blockchain-based healthcare and insurance claim systems, focusing on several recent works that have influenced the development of this proposed system[3].

One significant challenge in traditional healthcare claim systems is the rampant issue of fraudulent claims. Insurance providers, healthcare institutions, and patients all bear the burden of high costs due to fraudulent activities, whether through false submissions, overbilling, or duplication of claims. Traditional systems struggle with identifying and preventing fraud, often relying on manual checks that are both time-consuming and prone to human error. A notable contribution to solving this issue is highlighted in a study that proposed a blockchain-based solution for processing health insurance claims, particularly for prescription drugs. This system utilizes the Inter Planetary File System (IPFS) for securely storing prescriptions, alongside a robust hashing mechanism that ensures the integrity of the data being processed. By integrating smart contracts, the process of validating claims becomes automated, removing the need for manual intervention. Claims are processed only if they match pre-defined rules encoded in the smart contract, ensuring both efficiency and accuracy. This approach not only minimizes fraud but also guarantees that the data remains secure and transparent throughout the process, fostering trust among all parties involved [4].

The healthcare ecosystem is the management and sharing of sensitive patient data. Traditional systems often struggle with interoperability, where patient records are scattered across multiple platforms or hospitals, leading to inefficiencies and redundancies. Additionally, concerns regarding the privacy and security of patient data are exacerbated by centralized systems that can become targets for data breaches. A study focused on managing patient records using blockchain offers a promising solution. This system enables decentralized control over patient data, empowering patients to manage who can access their information through the use of cryptographic techniques such as public and private key encryption. By storing sensitive data off-chain, scalability issues typically associated with blockchain technology are addressed, and only metadata is recorded on the blockchain, ensuring that large volumes of data can be securely managed without overloading the network. This approach not only ensures the privacy of patient data but also provides a transparent and immutable audit trail, which enhances trust and accountability across all healthcare providers accessing the data. Additionally, the system enhances interoperability by enabling seamless data sharing between healthcare institutions, thereby reducing redundant tests and improving patient care [5].

Fraudulent claims and the inefficiencies in claim validation also extend to the broader insurance industry. A study on a blockchain-based fraud detection system for healthcare insurance claims presents a unique solution by incorporating real-time monitoring and advanced analytics to identify fraudulent activities. The proposed blockchain system uses predefined smart contract rules to verify the legitimacy of claims, immediately flagging those that do not meet the required criteria. By employing real-time analytics, the system is capable of identifying suspicious patterns over time, which can then be flagged for further review. This fraud detection mechanism significantly reduces manual intervention, ensuring that only legitimate claims are processed and approved. Moreover, blockchain's decentralized nature ensures that no single entity controls the data, thus preventing any tampering or manipulation of claims, further enhancing the transparency and security of the process [6].

In addition to fraud prevention and data management, the integration of blockchain into healthcare insurance claims also promises to improve the efficiency of the claims process. A primary benefit is the automation of claim processing. With traditional systems, claims are often delayed due to manual verifications and paper-based documentation.

By using blockchain's smart contracts, claims can be validated and processed in real-time based on pre-configured rules. This not only speeds up the claims processing time but also reduces operational costs for both hospitals and insurance companies. For example, in systems where hospitals submit claims for patients under insured policies, the details of the patient, the medical procedures performed, and the charges associated with them can all be recorded on the blockchain. A smart contract can then automatically verify whether the claim is eligible for reimbursement based on the conditions set by the insurance provider, streamlining the entire process [6].

III. PROPOSED APPROACH

The core functionality of the system is embedded in Ethereum smart contracts, which include Insurance Policy Management that enables companies to add and manage policies linked to users, Bill Processing that allows hospitals to generate bills, sign them using private keys, and submit them to the blockchain for verification, and an authentication mechanism that uses cryptographic hashing and digital signatures to validate transactions.

As shown in Fig. 1, which illustrates the step-by-step process of the proposed blockchain-based insurance claim authentication system. The workflow begins with the hospital collaborating with insurance companies to establish policies. Once policies are added, the hospital registers patients and processes their medical bills. The hospital then generates a cryptographic hash of the bill and signs it before submitting it to the blockchain. A smart contract verifies the authenticity of the bill by validating the digital signature and checking the policy coverage. Upon successful verification, the blockchain is updated with the transaction, ensuring immutability and transparency. Finally, patients can view their processed bills and verify claim status, while the insurance portal enables companies to manage their policies efficiently

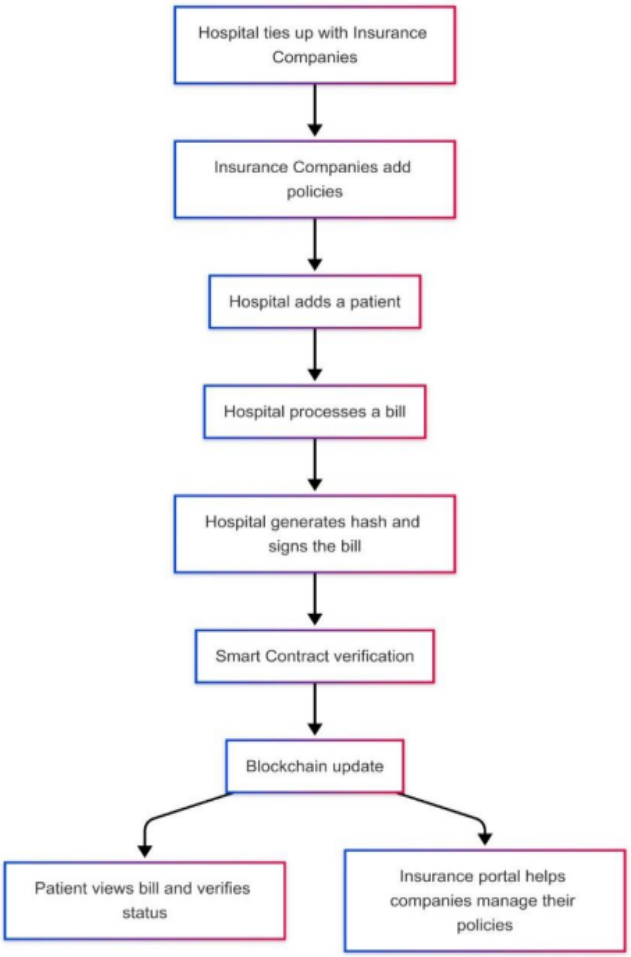


Fig. 1. Blockchain-Based Insurance Claim Authentication Workflow

Fig. 2 illustrates the initial steps in processing an insurance claim. The hospital submits a bill with patient and policy details, ensuring all entities exist and the user is part of the policy. A new bill structure is created and stored, after which a cryptographic hash is generated to maintain data integrity. This hash serves as the first layer of security verification before signature validation.

```
function addAndProcessBill(
    string memory patientID,
    string memory companyID,
    string memory policyID,
    uint256 totalBill,
    string memory billID,
    bytes32 dataHash,
    bytes memory signature,
    string memory userID
) public onlyHospital {
    // Ensure patient, company, and policy exist
    require(bytes(patients[patientID].patientID).length != 0, "Patient not found");
    require(bytes(companies[companyID].companyID).length != 0, "Company not found");
    require(bytes(policies[companyID][policyID].policyID).length != 0, "Policy not found");
    bool userExists = false;
        for (uint i = 0; i < policies[companyID][policyID].userIDs.length; i++) {
            if (keccak256(abi.encodePacked(policies[companyID][policyID].userIDs[i])) == keccak256(abi.encodePacked(userID))) {
                userExists = true;
                break;
            }
        } require(userExists, "User is not part of the specified policy");

    // Create the new bill
    Bill memory newBill = Bill({
        billID: billID,
        totalBill: totalBill,
        remainingCoverage: policies[companyID][policyID].coverage,
        additionalAmount: totalBill > policies[companyID][policyID].coverage ? totalBill - policies[companyID][policyID].coverage : 0,
        verifiedBy: hospitalAddress,
        processedDate: 0,
        isProcessed: false
    });

    // Store the new bill
    billIDs.push(billID);
    // Emit the BillAdded event (after the bill is added)
    emit BillAdded(billID);
// Now process the bill immediately
    bytes32 expectedHash = keccak256(abi.encodePacked(patientID, billID));
    require(expectedHash == dataHash, "Data mismatch");
```

Fig. 2. Bill Submission and Initial Verification

Fig. 3 depicts the cryptographic authentication mechanism used in claim verification. The smart contract validates the hospital's digital signature to ensure authenticity. Once verified, the bill is processed by deducting the coverage and computing the remaining amount. Finally, the transaction is permanently stored on the blockchain, ensuring tamper-proof claim records.

```
    // Recover the signer and verify the signature
    address signer = recoverSigner(dataHash, signature);
    require(signer == hospitalAddress, string(abi.encodePacked("Invalid signature from hospital. Recovered signer: ",addressToString(signer))));

    // Calculate remaining coverage after processing
    uint256 remainingCoverage = totalBill > newBill.remainingCoverage ? 0 : newBill.remainingCoverage - totalBill;
    newBill.isProcessed = true;
    newBill.processedDate = block.timestamp;
  // Store the processed bill details in the processedBills mapping
    processedBills[billID] = ProcessedBillDetails({
      billID: billID,
      totalBill: totalBill,
      coverageAmount: policies[companyID][policyID].coverage,
      remainingCoverage: remainingCoverage, // Updated remaining coverage after processing
      additionalAmount: totalBill > policies[companyID][policyID].coverage ? totalBill - policies[companyID][policyID].coverage : 0,
      verifiedBy: hospitalAddress,
      processedDate: newBill.processedDate, // Store the processed date
      isProcessed: true // Mark the bill as processed
    });

    // Add the processed bill to the patient's bill list (patientBills mapping)
    patientBills[patientID].push(Bill({
      billID: billID,
      totalBill: totalBill,
      remainingCoverage: remainingCoverage,
      additionalAmount: totalBill - (totalBill - remainingCoverage), // Amount to be paid by patient
      verifiedBy: hospitalAddress,
      processedDate: block.timestamp,
      isProcessed: true
    }));

    // Emit the BillProcessedEvent (after processing the bill)
    emit BillProcessedEvent(billID);
  }
```

Fig. 3. Digital Signature Verification and Blockchain Update

IV. RESULTS AND DISCUSSION

Results of the blockchain-based insurance claim authentication system based on smart contract execution and user evaluation mutable blockchain framework.

TABLE I. Evaluation of System Features

Feature	Hospital Portal	Insurance Company Portal	Patient Portal
User Authentication	Blockchain-Based	Blockchain-Based	Blockchain-Based
Claim Submission	Yes	No	No
Policy Management	No	Yes	No
Claim Verification	Yes	Yes	No
Bill Viewing	Yes	Yes	Yes
Tamper-Proof Records	Yes	Yes	Yes

Table I represents a feature-based evaluation of the system. The hospital portal enables bill submission and cryptographic signing, ensuring data integrity. The insurance company portal manages policies and verifies claims, while the patient portal provides transparency by allowing users to view processed bills. Since all records are stored on the blockchain, the system ensures tamper-proof claim authentication.

TABLE II. Claim Processing and Verification Results

Test Case	Expected Outcome	Observed Outcome
Valid Bill Submission	Claim Approved	Approved
Tampered Bill Attempt	Claim Rejected	Rejected
Incorrect Digital Signature	Claim Rejected	Rejected
Policy Not Found	Claim Rejected	Rejected

Table II presents the evaluation of claim processing. The system correctly processes valid claims and prevents fraudulent activities by rejecting tampered bills and invalid digital signatures. This demonstrates the effectiveness of blockchain in maintaining claim authenticity.

The blockchain-based claim authentication system was evaluated across multiple test cases involving different scenarios of claim submission and verification. The system successfully authenticated valid claims while preventing fraudulent attempts. Hospitals were able to generate and sign bills efficiently, while insurance companies seamlessly validated claims based on policy data. Patients could transparently access their processed bills. The use of smart contracts eliminated manual errors and delays, ensuring faster and more reliable claim approvals. Additionally, by leveraging cryptographic hashing and digital signatures, the system maintained data integrity and security throughout the process.

V. CONCLUSIONS AND FUTURE WORK

The blockchain-based insurance claims system transforms traditional claim processing by eliminating manual checks, reducing fraud, and ensuring transparency through an immutable blockchain framework. By leveraging hashing and hospital signature authentication, it enhances data integrity while automating claim verification via smart contracts. This reduces human intervention, accelerates approvals, and improves efficiency for hospitals, insurance companies, and patients.

Future enhancements include integrating layer 2 protocols for scalability, machine learning for fraud detection, and interoperability with healthcare systems for seamless data exchange. Real-time claim tracking and insurer communication will further streamline the process, making insurance claims more secure, transparent, and efficient.

VI. ACKNOWLEDGMENT

We would like to express our sincere gratitude to RV Institute of Technology and Management for their invaluable support and resources throughout this project. Special thanks to the Information Science Department for their guidance and assistance.

REFERENCES

[1] Aysha Alnuaimi, Amna Alshehhi, Khaled Salah, Raja Jayaraman, Ilhaam A. Omari and Ammar Battah, "Blockchain-Based Processing of Health Insurance Claims for Prescription Drugs", IEEE Access, vol. 10, pp. 118093 – 118107, Nov 2022.

[2] Bharath H, Rahul N, Shylash S and Vinny Pious, "Patient Data Management Using Blockchain",International Journal of Scientific and Research Publications, vol. 10, pp. 310-316, July 2020.

[3] Roshan Lal Neupane, Ernest Bonnah, Bishnu Bhusal, Kiran Neupane, Khaza Anuarul Hoque and Prasad Calyam, "Formal Verification for Blockchain-based Insurance Claims Processing", arXiv:2402.13169v1, Feb 2024.

[4] Dylan Yaga, Peter Mell, Nik Roby and Karen Scarfone, "Blockchain Technology Overview", arXiv:1906.11078, Jun 2019.

[5] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen and Huaimin Wang, " Blockchain challenges and opportunities: a survey", International Journal of Web and Grid Services, vol. 14,pp. 352-375, Oct 2018.

[6] Jaideep Gera, Anitha Rani Palakayala, Venkata Kishore Kumar Rejeti and Tenali Anusha, "Blockchain Technology for Fraudulent Practices in Insurance Claim Process", IEEE Access, July 2020.

[7] Chin-Ling Chen, ORCID,Yong-Yuan Deng, Woei-Jiunn Tsaur, ORCID, Chun-Ta Li, ORCID, Cheng-Chi Lee and Chih-Ming Wu , "A Traceable Online Insurance Claims System Based on Blockchain and Smart Contract Technology", Journals, Sustainability ,vol. 13, August 2021.

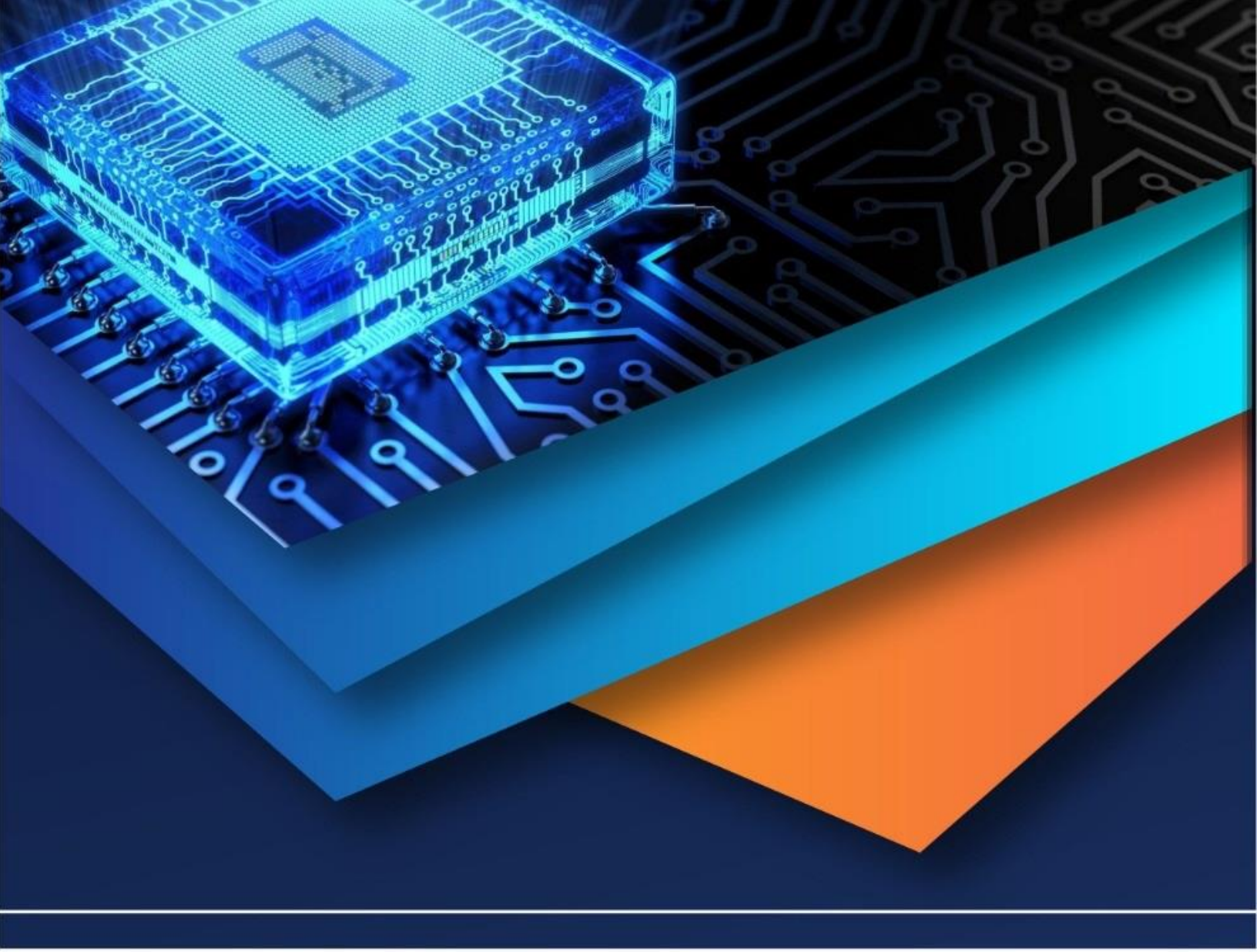
[8] Shafaq Naheed Khan, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa and Anoud Bani-Hani,"Blockchain smart contracts: Applications, challenges, and future trends", Springer,April 2021.

[9] G. Saldamli, V. Reddy, K. S. Bojja, M. K. Gururaja, Y. Doddaveerappa, and L. Tawalbeh, "Health care insurance fraud detection using blockchain," International Conference on Computer Science, Engineering and Applications (ICCSEA), pp. 1-4,July 2022.

[10] Leila Ismail and Sherali Zeadally," Healthcare Insurance Frauds: Taxonomy and BlockchainBased Detection Framework (Block-HI)", IEEE Access, vol. 23, pp. 36-43, August 2021.

[11] Houyu Zheng, Lin You and Gengran Hu, " A novel insurance claim blockchain scheme based on zero-knowledge proof technology", Sciencedirect, September 2022.

[12] Khatun, Mahafujaa Islam, Ridwan Arefinb Islam and Salekula, " B-SAHIC: A blockchain based secured and automated health insurance claim processing system", Journal of Intelligent & Fuzzy Systems, vol. 44, no. 3, pp. 4869-4890, March 2023.
[13] Arpan Kumar Kar and L. Navin," Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature", Sciencedirect, November 2022.
[14] Sumit Oberoi and Pooja Kansra, " Blockchain Technology in the Insurance Industry", In IGI GLOBAL, 2022.
[15] Simon Grima, Jonathan Spiteri and Inna Romānova,"A STEEP framework analysis of the key factors impacting the use of blockchain technology in the insurance industry", Springer, March 2020.
[16] V. P. Kalsgonda and R. V. Kulkarni, "APPLICATIONS OF BLOCKCHAIN IN INSURANCE INDUSTRY: A REVIEW ", PIMT Journal of Research, vol. 12, no. 4, September 2020.
[17] Lanqing Zhao, "The Analysis of Application, Key Issues and the Future Development Trend of Blockchain Technology in the Insurance Industry", American Journal of Industrial and Business Management, vol. 10, no.2, February 2020.
[18] Tarr and Julie-Anne, "Distributed ledger technology, blockchain and insurance: Opportunities, risks and challenges", Insurance Law Journal, 29(3), pp. 254-268, March 2024.
[19] Shakil Ahmad and Charu Saxena, "Artificial Intelligence and Blockchain Technology in Insurance Business", International Conference on Recent Innovations in Computing, vol. 10,May 2023.
[20] Marijn Janssen , Vishanth Weerakkody , Elvira Ismagilova , Uthayasankar Sivarajah and Zahir Irani ,“A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors", Sciencedirect, February 2022.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY