Forti-Ins: A Blockchain Based Framework to Automate Healthcare Insurance Processing in Smart Cities

Musharraf N. Alruwaill*, Saraju P. Mohanty*, Elias Kougianos†
* Department of Computer Science and Engineering, University of North Texas, USA
† Department of Electrical Engineering, University of North Texas, USA
Email: MusharrafAlruwaill@my.unt.edu, saraju.mohanty@unt.edu, elias.kougianos@unt.edu

***Abstract*—Individuals with health insurance are protected from financial risk and have access to critical medical treatments. However, traditional healthcare insurance has issues such as complexity, availability, claim processing time, fraudulent claims, and double claims. These problems can lead to issues such as patient funds being held, lengthy claim processing, and fraudulent claims. The claim process is handled manually in order to verify each medical treatment, validate the claim, and ensure that it complies with the coverage policy. Significant advantages of an automated system for healthcare insurance procedures include a reduction in time, increased accuracy, and improved insurance service quality. However, the centralized nature of such systems may present vulnerabilities, such as a single point of failure, loss of transparency, and integrity. The proposed Forti-Ins system integrates blockchain technology, smart contracts, and a distributed file system to facilitate automated claim processing, prevent double claims, increase transparency, reduce administrative costs, and strengthen system robustness, all within a secure framework. Smart contracts facilitate the automated handling of healthcare insurance procedures in a secure manner, while distributed file systems provide cost-effective management of large volumes of files.**

***Index terms*—** Smart Healthcare, Blockchain, Smart Contract, Healthcare Cyber-Physical Systems.

I. Introduction

A healthcare insurance policy covers an individual's medical expenses in the case of illness, injury, or the need for medical treatment. In the instance of a serious illness or an emergency, it is essential to protect the individual from incurring excessive costs. Prior to a visit, the healthcare provider verifies the patient's insurance coverage when he or she requires medical treatment. After delivering medical care to a patient, the healthcare provider submits an insurance claim. The claim will be authorized or denied after manual validation by the claims adjuster. Therefore, the claim procedure is lengthy, as it involves the insured paying out of pocket until the insurance company pays for the visit. In addition to lengthy claim processing times and claim fraud, traditional healthcare insurance has high premiums. Furthermore, a centralized system can result in problems such as a single point of failure and a lack of transparency, which can lead to data manipulation. A significant improvement in conventional medical practice is required to accommodate evolving technologies. Smart healthcare is thus a solution for maximizing the services and advantages supplied by healthcare providers to smart city citizens. Figure 1 presents the system overview of smart insurance in a centralized manner. To automate healthcare insurance procedures in a secure manner, emerging technologies such as blockchain, smart contracts, and distributed storage systems can be utilized and eliminate third parties [1]. A number of fundamental qualities of blockchain technology are required for its deployment in smart healthcare insurance.

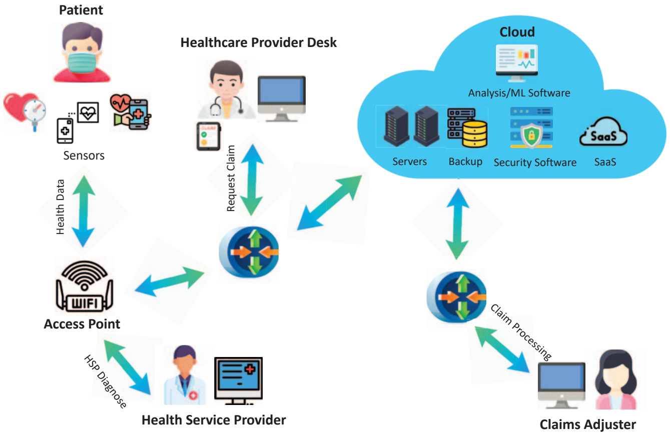

Fig. 1: Overview of a Smart Insurance System and Healthcare Cyber-Physical Systems (H-CPS).

Once an insured patient has entered a foreign country, they are able to access their insurance benefits without waiting a long period of time for their claim to be confirmed, verified, and approved. Regarding an individual's health, time is money. Therefore, insurance companies must improve their processes so that they can be automated to accelerate the approval procedure. Individuals and insurers may engage in a contract using a smart contract to automate the claims procedure. The integration of blockchain technology and smart contracts allows the secure administration and use of individual insurance plans on a global domain and can be beneficial to designing a policy for each client.

The proposed framework is called Forti-Ins. It utilizes blockchain technology and smart contracts alongside distributed storage systems to improve overall security and provide a secure decentralized system with a secured intermediate automated secure system.

II. Related Work

Different approaches are proposed by researchers in various insurance domains. [2] proposed blockchain-based power out insurance to address these issues in the current or traditional method of data security, process efficiency, and high claim costs with the help of blockchain technology. In [3], the author discussed different challenges to having insurance for smallholder farmers, such as high administrative costs, moral hazards, and fake information provided by farmers. Therefore, the author suggests using blockchain technology for index-based crop insurance for smallholder farmers and presents examples of existing blockchain-based insurance, such as ACRE Africa and Aon. In [4], the author discusses different types of insurance and its capabilities of using blockchain technology, such as health insurance, home insurance, and disability insurance, with an exploration of claim submission using blockchain. In [5], blockchain-based insurance from different perspectives is discussed, such as the benefits of using technology, the regulation, and the law's role, and present the differences between traditional and blockchain-based insurance. The author in [6] presents the areas in which blockchain can be used, such as fraud detection, quick processing, and payment, as well as the use cases and solutions to the presented challenges.

[7] proposed a system for health insurance with automated payment through smart contract. However, the system uses a relational database with indexing to the records on on-chain storage. In [8], the author proposed InsurModel Blockchain to overcome the bitcoin-like blockchain in the insurance industry. These issues include inefficiency in data auditing, difficulty in verifying encrypted data, and traceability at the file level. In addition, ZKP (zero-knowledge-proof) is proposed to solve the problem of ensuring the price is within the range without knowing the actual price. However, the proposed system is designed for LTCI (Long-Term-Care-Insurance) and has not yet been generalized to other healthcare insurance types. It also adds additional unnecessary data pointers between transactions to be used in different types of health insurance, as well as transaction dependency, where the proposed system provides independence. In addition, the proposed system, CioSy [9], solves traditional collaborative insurance issues. However, a claim request and other processes need a system that is applicable to a huge file and cost-effective. In [10], the author's proposed solution uses, in particular, some automated processes. However, it relies on third-party trusted data sources, and these data sources might be centralized.

The proposed system in [11] uses smart contact and machine learning algorithms to classify the EHR (Electronic Health Record) of the patient to decide whether the patient is approved for the claim or not. As proposed in [12], it aims to secure the claim process using smart contracts and private blockchain through the Hyperledger fabric. In [13], the proposed system uses BigchainDB and several technologies, such as Neo4j, for fraud detection, as the system mainly aims to detect fraud. The proposed system in [14] uses blockchain and smart contracts to build a secure system for claim validation. In [15], the proposed system uses private blockchain and smart contract to automate the claim and payment to reduce the time of traditional insurance consumption.

However, the proposed system, Forti-Ins, aims to automate the insurance claim process, resulting in time reductions and reduced administrative and operational costs, which leads to cheaper premium insurance. In addition, Forti-Ins uses different designs and technologies, such as the integration of IPFS and blockchain, to maintain security and have cost efficiency. In addition to claim process automation, location-based authentication and double claim detection are proposed to ensure the claim procedures are securely processed. Moreover, access control management and document sharing are proposed through smart contracts and IPFS for data sharing. A comparative view of related research works is shown in Table I.

III. Novel Contributions

A. Problem

The existing healthcare and insurance systems are centralized. Centralized systems raise issues regarding security, such as a single point of failure, data security breaches, privacy breaches, and a lack of transparency and secure automation. Due to the globalization of healthcare insurance, data availability is crucial for authenticating policyholders worldwide. This raises concerns about human mistakes and decision-making. The presence of double claims and false claims is considered an additional challenge that contributes to the economic strain experienced by insurance companies. Furthermore, the process of claiming requires a significant amount of time for validation and approval.

B. The Novelty of the Proposed Solution

The proposed system is called Forti-Ins (Figure 2), and provides decentralized, secure data management using blockchain technology. Blockchain technology's characteristics enhance system security and reliability. It provides data privacy, transparency, and decentralization. Thus, it makes data available globally at any time, under any conditions, and without constraints. It uses distributed file storage to make data accessible across different nodes, minimize blockchain transaction size, and reduce transaction expenses. However, the content identifier (CID) will be maintained on the blockchain to ensure data integrity and prevent tampering. Smart contracts have been proposed to simplify end-user engagement. Claim verification will take seconds and track records accurately. Forti-Ins automates the claim submission procedure [16]. A single person may have multiple insurance policies. Fort-ins prevent multiple claims and use one insurance policy per patient encounter.

TABLE I: Comparision Table

Framework	Data Storage	Platform	Authentication-Based-Location	Smart Contract	Double Claim Detection
Jha et al, 2021 [10]	Blockchain	Ethereum	No	Few Client procedure Functionalities	No
Loukil et al, 2021 [9]	Blockchain	Ethereum	No	More Client procedure Functionalities	No
Zhang et al, 2021 [8]	Blockchain	Hyperledger	No	Merkle tree Construction	No
Chondrogiannis et al, 2022 [7]	Blockchain and off-chain	Ethereum	No	High Client procedure Functionalities	No
Alnavar and Babu, 2021 [11]	Blockchain	Ethereum	No	Claim verification through EHR	No
Gera et al, 2020 [12]	Blockchain	Hyperledger	No	Claim Process	No
Saldamli et al, 2020 [13]	Blockchain and off-chain	BigChainDB	No	Uses Neo4j for fraud detection	No
Varalakshmi et al, 2022 [14]	Blockchain	Ethereum	No	Claim approval through multiple Signatures	No
Aleksieva et al, 2020 [15]	Blockchain	Hyperledger	No	Few Client procedure Functionalities	No
Forti-Ins	**Blockchain - IPFS**	**Ethereum**	**Yes**	**High Client procedure Functionalities**	**Yes**

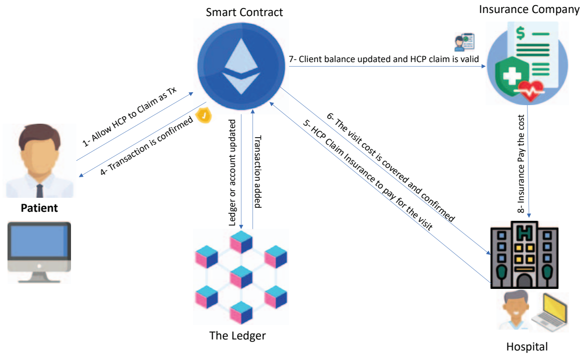
Smart Contract
Insurance Company
7- Client balance updated and HCP claim is valid
1- Allow HCP to Claim as Tx
4- Transaction is confirmed
Ledger or account updated
Transaction added
6- The visit cost is covered and confirmed
5- HCP Claim Insurance to pay for the visit
8- Insurance Pay the cost
Patient
The Ledger
Hospital

Fig. 2: Forti-Ins Cliam Overview.

IV. A Novel Forti-Ins

A. Framework Components

1) Blockchain Technology: The blockchain is used to manage insured and insurer memberships in a trustworthy environment. It provides a secure decentralized system with transparency and availability, which helps globalize the system and prevent single point of failure. In contrast with the existing centralized systems, blockchain ensures non-repudiation, integrity, and data validity through consensus algorithms and blockchain mechanisms, which are essential in the insurance industry.

2) Smart Contract: Smart contracts provide a secure intermediate business logic. Within the framework of Forti-Ins, these smart contracts are employed to mechanize insurance processes and enrollment procedures. Each membership has different roles and privileges. These privileges are verified by smart contracts, and each transaction is stored on the blockchain after being confirmed.

3) Distributed Storage: Distributed storage is characterized by the ability to store a file through a decentralized protocol, which is performed using a peer-to-peer mechanism to form a network. The InterPlanetary File System, known as IPFS, is a system that enables users to store files in several places and index them with hashes. It is used to upload huge files and documents to reduce costs and include the content identifier of the file in the blockchain network.

4) Location-Based Authentication: Each medical center has a primary blockchain member that serves as the center's representative and has an internal, independent system. Therefore, the independent system can be partially integrated through smart contracts. The internal system can verify each patient encounter within the healthcare provider's location and validate the patient encounter through a smart contract to ensure double verification, prevent false claims, and give healthcare providers a single node with full privileges. The internal database uses SQLite3 for portability and a lightweight database.

V. Fort-ins Architecture

The core components of a Forti-Ins architecture can be broken down into three distinct layers. The patient who makes use of the insurance benefits makes up the patient layer, which is the first layer of the pyramid. The network layer is the second layer, and it is comprised of the blockchain network and a peer-to-peer network that both stores the data and keeps the ledger updated. In addition, the smart contract that will allow the network layer to interact with the end-users whether patient or other stakeholders, such as the customer, the claim adjuster, and the healthcare providers activities, are contained within the network layer. In Forti-Ins architecture, the insurance companies and healthcare providers and other stakeholders make up the third layer of the architecture. This layer communicates and interacts with the smart contract and allows users to submit their policies by means of the smart contract in order to automate the process by which clients receive the benefits of their policies. Forti-Ins architecture is depicted in Figure 3.

A. The Proposed Algorithms For Forti-Ins

Each client needs to enroll for coverage with the insurance company. After that, the insurance provider adds the customer

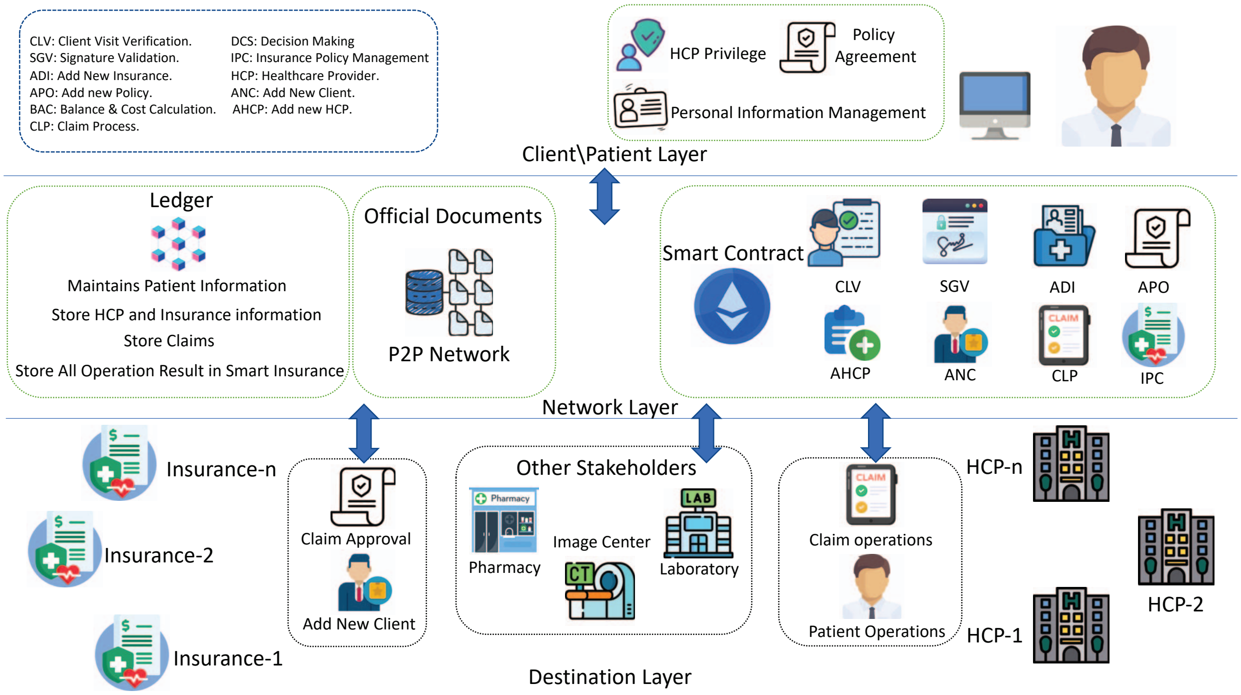

Fig. 3: Forti-Ins Architecture.

to their list of policyholders. Once the customer has successfully enrolled, the healthcare provider can submit a claim for the insured person with a valid customer address. The address represents the insured person's identity. As shown in algorithm 1, the customer chooses the insurance provider and plans to enroll. Smart contracts work as secured intermediate business logic to interact with different entities and members and then store the valid data into a hashmap to navigate once it is needed. At the end, the enrollment request is pending until the decision is made by the insurance provider. Once the subscription is approved, the insured person can use the insurance benefits provided by the healthcare provider within the insurance plan.

Algorithm 1 Client Enrollment

```
Require: Client address $C_{addr}$ , and personal information $PI$,
    Insurance Plan $InsP$.
Ensure: Client enrollment through smart contract $SC$.
Client Writes $PI$ and $C_{addr}$
Client determines which insurance company and $InsP$ to subscribe.
Client makes an enrollment request.
$SC$ receives the enrollment request.
$SC$ verifies whether the client is registered or not.
if Client is not regisetered: then
    $SC$ associates the account with unique identifier.
    $SC$ associates the account with client privilege.
    $SC$ processes Tx and makes the enrollment request pending until insurer approved the client subscription.
    Client receives unique identifier.
end if
Insurer whether accept or rejects the enrollment request.
```

After the client successfully enrolls, the healthcare provider and client are able to make a claim request. Algorithm 2 describes the claim process and input requirements. HCP requests a claim through the smart contract with a valid address. The transaction includes the CID of the documents, patient information, and visit ID. Forti-Ins smart contract verifies the claim to prevent double claims through visit ID validity and insurance plan coverage. After that, the healthcare provider's internal system marks the claim with a valid value after verification processes via location-based authentication and HCP credentials. At the end, the claim is approved or rejected based on the coverage plan. Moreover, the system updates the claim requester with notifications about the claim status. Once the claim is confirmed, the claim adjuster is able to perform final checks to determine whether the claim is approved or rejected by checking the documents. A claim adjuster is required to ensure the validity of the document while the smart contract makes the decision about whether it is approved or rejected through business logic as described in algorithm 3.

VI. Implementation And Validation

A. Implementation

The implementation of Forti-Ins combines multiple programming languages and software. Solidity is used to write a smart contract and is connected with Metamask to interact with the Ethereum blockchain. IPFS is used as a peer-to-peer

Algorithm 2 Claim Request

```
Require: Healthcare Provider Account $HCP$, Visit ID $V_{ID}$
Ensure: Claim Submitted through Smart Contract $SC$.
$HCP$ has a valid account
$HCP$ Writes description of patient health status.
$CID \leftarrow$ Upload documents and letters on IPFS.
$HCP$ includes $CID$ and $V_{ID}$ and patient information.
$HCP$ submit claim request.
$SC$ verifies $HCP$ privileges and patient account
$SC$ verifies $V_{ID}$ is not claimed or under process
if $V_{ID}$ is claimed then
    $SC$ notifies $HCP$ that $V_{ID}$ is claimed.
    $SC$ terminate the process.
else
    $SC$ checks the insurance plan coverage.
    if insurance plan covers $V_{ID}$ then
        $SC$ initializes new visit id and assigns $V_{ID}$ to it.
        $SC$ assign pending status to the new $V_{ID}$.
        $HCP$ makes request in internal system and associated with $HCP$ credential, location and $V_{ID}$.
        Internal system validates $HCP$ credential and location.
        if $HCP$ credential and location is valid then
            the claim marked as valid $V_{ID}$ via $SC$.
        else
            the claim marked as not valid $V_{ID}$ via $SC$.
        end if
    else
        $SC$ declines the claim requests and send a message informing $HCP$ of insurance not covered this visit.
    end if
end if
```

Algorithm 3 Insurer Claim Process

```
Require: Valid Claim Adjuster $C_{adj}$, Claim ID $C_{ID}$
Ensure: Accept or Decline claim request
$SC$ validates $C_{adj}$ privilege.
if $C_{adj}$ has insurer privilege. then
    $C_{adj}$ selects $C_{ID}$.
    $C_{adj}$ checks $SC$ result for specific $C_{ID}$.
    $C_{adj}$ determines whether accept, reject.
    if $C_{adj}$ accepts $C_{ID}$. then
        $C_{adj}$ update $V_{ID}$ with approved
        $SC$ stores the data on the blockchain and update $C_{ID}$ and $V_{ID}$ status.
    else
        $C_{adj}$ rejects $C_{ID}$ or request additional documents.
        Terminate the process.
    end if
else
    $SC$ rejects $C_{adj}$ to access as insurer client.
    Terminate the process.
end if
```

distributed file storage system. Python is utilized to make web interfaces through the Flask framework. A smart contract is deployed on the Goerli testnet.

B. Validation

1) Cost and Time Analysis: Forti-Ins utilizes a range of innovative technologies to bolster security and optimize cost considerations within public blockchains. In this context, the deployment of smart contracts on the Goerli testnet facilitates seamless interaction with the blockchain while offering real-time gas cost analysis and ensuring compatibility with the network. The average confirmation time for transactions stands at 10.80 seconds. Furthermore, the integration of IPFS assists in optimizing costs associated with blockchain operations. As indicated in Table II, the incurred expenses are deemed both economically efficient and advantageous, with an approximate value of 0.00000000008727013 ETH. This table reinforces the notion that the cost aspect has been effectively addressed and minimized.

2) Privacy and Data Security: The data within the system is strictly confined to authorized individuals or entities, ensuring exclusive access privileges. Moreover, once the data is immutably stored, any further alterations are precluded. Consequently, the implementation of Forti-Ins substantiates a robust framework for fortifying data security and upholding stringent privacy protocols within the healthcare insurance context. Furthermore, the utilization of cryptographic addresses serves to heighten privacy by obfuscating real-person identities, thereby contributing to an enhanced level of confidentiality.

3) Availability and Auditability: Forti-Ins leverages a combination of distributed file storage and blockchain technologies to ensure data availability in the healthcare provider context. By harnessing the inherent data decentralization capabilities of blockchain, Forti-Ins establishes a resilient and distributed storage infrastructure. Moreover, the immutable and transparent nature of blockchain mechanisms guarantees data auditability, facilitating robust verification and accountability. Additionally, the adoption of a decentralized approach ensures data portability with a secure and globally accessible data ecosystem.

4) Anonymity and Access Control Management: The integration of blockchain and smart contract technologies presents a robust framework to achieve heightened anonymity and establish effective access control management [17]. Within the blockchain context, participants use pseudonyms or cryptographic addresses instead of real names to conduct interactions, ensuring a degree of privacy. Furthermore, smart contracts play a pivotal role in facilitating interactions among diverse entities and provide the capacity for implementing access control mechanisms, exemplified by role-based access control (RBAC) as adeptly employed by Forti-Ins to govern secure entity interactions.

5) Fake and Double Claim Detection and Prevention: Fort-ins utilizes a smart contract with versatile functionalities to prevent fake and duplicate claims. By implementing a claim ID

TABLE II: Cost Analysis.

Action	File type or File size	Tx Hash	Tx Fees
Smart Contract Deployment	Contract Deployment	0x13752d2ee646fda0c5db197887fa2ed1609d44a84c480946a37f703447cf3ff1	0.000000006022652585 ETH
Submit Claim	Transactional data	0xf50cda274edeb9945a27974b31b1d7320f17d7ed73aa5baf42b92545447be2bc	0.000000000147869845 ETH
Grant HCP Privilege	Transactional data	0x2cba53a290d2b565fc1801c75f8af98afc9b79378701e14af236a909127d938b	0.00000000044030023 ETH
Grant Insurance Privilege	Transactional data	0x41c4c341abafb67e36074d4809c659f16eda4f5a4f8ca03a708cb95b00dd0876	0.00000000044763312 ETH
Approve Claim	Transactional data	0xb7459e30bc7e2ba57cc9a564a6dedc08e35a46e2992277f175b2665af48366e5	0.000000000266615037 ETH
Claim Document	58 MB	0x647b43dd20a0995a0941514fe1b2fb4c997e08613f76f6a4ef48a9fd4426196b	0.000132832171067828 ETH

associated with a boolean flag, a true value indicates one of the insurers has granted approval to a claim. Therefore, the other insurers are precluded from processing a settled claim. In addition, multiple authentications and verification are provided, both internally and through smart contracts, as described in the proposed algorithm subsection, which can prevent fake claims. Fort-ins enhances the insurers' experience while also reducing financial losses resulting from fraudulent claims, thus reaffirming the system's robustness and fiscal responsibility. This innovative approach ensures the utmost reliability and cost-effectiveness, making Fort-ins an outstanding solution in the domain of insurance claim management.

VII. Conclusion and Future Directions

Forti-Ins integrates blockchain, smart contracts, and distributed file systems to manage healthcare insurance in a secure and cost-effective manner. Blockchain is utilized to store data such as claims, memberships, CIDs of documents, and smart contracts for authenticity, claim automation, and fake and double claim prevention. IPFS is utilized to store the file documents, return CIDs, and forward them to the blockchain to ensure integrity and cost effectiveness.

In further research for Forti-Ins, risk assessment can be provided with the use of deep learning to ensure precise insurance costs. Customized policies are also provided through the analysis of personal health data.

References

[1] M. Khan, A. Hassan, and M. I. Ali, "Secured insurance framework using blockchain and smart contract," *Scientific Programming*, vol. 2021, pp. 1–11, 11 2021.

[2] C. Deng, Y. Yan, K. Wang, H. Xia, Y. Yang, and Y. Sun, *Blockchain-Based Power-Out Insurance Design and Practical Exploration*, 09 2021, pp. 357–372.

[3] N. Kshetri, "Blockchain-based smart contracts to provide crop insurance for smallholder farmers in developing countries," *IT Professional*, vol. 23, no. 6, pp. 58–61, 2021.

[4] A. Amponsah, A. Adekoya, and B. Weyori, "Blockchain in insurance: Exploratory analysis of prospects and threats," *International Journal of Advanced Computer Science and Applications*, vol. 12, 01 2021.

[5] M. Abramowicz, *Blockchain-Based Insurance.* Oxford University Press, 2019. [Online]. Available: http://sdl.edu.sa.sdl.idm.oclc.org/middleware/Default.aspx?USESDL=true&PublisherID=AllPublishers&BookURL=https://sdl.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edsoso&AN=edsoso.9780198842187.003.0011&site=eds-live

[6] A. Anand and S. H. Bokhari, "Blockchain: Insurance use cases, challenges and solutions." *MiddleEast Insurance Review*, pp. 24 – 25, 2022. [Online]. Available: http://sdl.edu.sa.sdl.idm.oclc.org/middleware/Default.aspx?USESDL=true&PublisherID=AllPublishers&BookURL=https://sdl.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=157168878&site=eds-live

[7] E. Chondrogiannis, V. Andronikou, E. Karanastasis, A. Litke, and T. Varvarigou, "Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations," *Blockchain: Research and Applications*, vol. 3, no. 2, p. 100049, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2096720921000440

[8] W. Zhang, C.-P. Wei, Q. Jiang, C.-H. Peng, and J. Zhao, "Beyond the block: A novel blockchain-based technical model for long-term care insurance," *Journal of Management Information Systems*, vol. 38, pp. 374–400, 04 2021.

[9] F. Loukil, K. Boukadi, R. Hussain, and M. Abed, "Ciosy: A collaborative blockchain-based insurance system," *Electronics*, vol. 10, no. 11, 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/11/1343

[10] N. Jha, D. Prashar, O. I. Khalaf, Y. Alotaibi, A. Alsufyani, and S. Alghamdi, "Blockchain based crop insurance: A decentralized insurance system for modernization of indian farmers." *SUSTAINABILITY*, vol. 13, no. 16, p. 8921, 2021. [Online]. Available: http://sdl.edu.sa.sdl.idm.oclc.org/middleware/Default.aspx?USESDL=true&PublisherID=AllPublishers&BookURL=https://sdl.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edswsc&AN=000690046200001&site=eds-live

[11] K. Alnavar and C. Babu, "Blockchain-based smart contract with machine learning for insurance claim verification," in *2021 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)*, 2021, pp. 247–252.

[12] J. Gera, A. R. Palakayala, V. K. K. Rejeti, and T. Anusha, "Blockchain technology for fraudulent practices in insurance claim process," in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, 2020, pp. 1068–1075.

[13] G. Saldamli, V. Reddy, K. S. Bojja, M. K. Gururaja, Y. Doddaveerappa, and L. Tawalbeh, "Health care insurance fraud detection using blockchain," in *2020 Seventh International Conference on Software Defined Systems (SDS)*, 2020, pp. 145–152.

[14] P. Varalakshmi, B. Sivasankari, R. A. Kumar, K. M. Nithish Kumar, and T. V. Venthan, "Development of healthcare insurance claim mechanism using blockchain technology," in *2022 1st International Conference on Computational Science and Technology (ICCST)*, 2022, pp. 835–840.

[15] V. Aleksieva, H. Valchanov, and A. Huliyan, "Implementation of smart contracts based on hyperledger fabric blockchain for the purpose of insurance services," in *Proc. International Conference on Biomedical Innovations and Applications (BIA)*, 2020, pp. 113–116.

[16] L. Ismail and S. Zeadally, "Healthcare insurance frauds: Taxonomy and blockchain-based detection framework (block-hi)," *IT Professional*, vol. 23, no. 4, pp. 36–43, 2021.

[17] M. N. Alruwaill, S. P. Mohanty, and E. Kougianos, "Hchain: Blockchain based healthcare data sharing with enhanced security and privacy location-based-authentication," in *Proceedings of the Great Lakes Symposium on VLSI 2023*, ser. GLSVLSI '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 97–102. [Online]. Available: https://doi.org/10.1145/3583781.3590255