Journal of Theoretical and Applied Information Technology
15th September 2025. Vol.103. No.17
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AI-BLOCKCHAIN HYBRID SMART CONTRACT MODEL: FRAUD DETECTION AND IMMUTABLE RECORD KEEPING IN INSURANCE

POORANI MITHILA S[1], GURUPANDI M[2], PRIYANKA K[3], SOLAIPRIYA S[4]

[1] Post-Doctoral Fellow, Department of Commerce, Alagappa University, Karaikudi, Tamil Nadu

[2] Associate Professor, Department of Commerce, Alagappa University, Karaikudi, Tamil Nadu

[3] PhD Research Scholar, Department of Commerce, Alagappa University, Karaikudi, Tamil Nadu

[4] PhD Research Scholar, Department of Commerce, Alagappa University, Karaikudi, Tamil Nadu

E-mail: [1]pooranimithila@gmail.com, [2]gurupandi80@gmail.com,

[3]priyangakphd@alagappauniversity.ac.in [4] spriya89k@gmail.com

ABSTRACT

The insurance sector is being transformed through the combination of artificial intelligence (AI) and blockchain technologies. This study proposes the AI-Blockchain Hybrid Smart Contract Model (AIBSCM), which combines AI-based fraud detection with blockchain-based smart contracts to allow for automated insurance claim processing. A synthetic dataset of 1,000 insurance claims was used to train a random forest model, which achieved 92% accuracy on training data; however, real-world testing revealed difficulty in detecting fraudulent claims from under-represented categories. A blockchain simulation was conducted to demonstrate the secure storage and automated execution of claims, with smart contracts giving transparency and immutability. The architecture integrates decentralised oracles, zero-knowledge proofs (ZKPs), federated learning, and a DAO governance mechanism to provide a privacy-conscious, decentralised, and robust solution for the insurance business. Subsequent study will look at real-world deployment and integration with regulations. The integration of these technologies seeks to address traditional insurance systems' issues, such as data privacy concerns and a lack of transparency. By investigating real-world deployment and regulatory compliance, this model has the potential to transform the insurance business by delivering a safe and efficient method for dealing with false claims. This innovative method has the potential to boost client trust while also streamlining insurance company operations. Overall, the combination of blockchain and privacy-conscious technology might result in increased reliability and a transparent insurance sector.

Keywords: *Artificial Intelligence, Blockchain, Smart Contracts, Transparency, Claim Processing.*

1. INTRODUCTION

The integration of Artificial Intelligence (AI) and Blockchain technology in the insurance industry is undergoing a momentous revolution. While blockchain is a decentralized digital ledger that guarantees transparency, security, and tamper-proof records across many systems, AI is the emulation of human intellect in machines that can duplicate human decision-making and behaviour.

There is enormous potential for integrating AI into blockchain systems to enable safer, more intelligent, and more effective procedures [D. Sotto-Mayor Machado, 2023]. Blockchain and AI integration is changing the corporate environment by providing innovative answers to important problems like trust, efficiency, security, and transparency [2]. AI gives companies strong capabilities for automation, predictive analytics, and data-driven decision-making. Blockchain guarantees a decentralized, impenetrable method of managing, storing, and confirming data. Such revolutionary use cases as AI-enhanced smart contracts, decentralized identity management, predictive supply chain optimization, and sophisticated fraud detection systems are made possible by the convergence of these two technologies [3]. Businesses may improve supply chain logistics, expedite financial transactions, and optimize operations with these technologies. This study explores how an important feature of the

insurance industry, the insurance claims processing, can be enhanced in terms of transparency and efficiency with the optimal use of smart contracts [4]. By leveraging AI for fraud detection and blockchain for immutable record-keeping, this research proposes a hybrid AI-Blockchain framework to optimize insurance operations.

Main Contributions of the Study:

- ✓ Proposes the AI-Blockchain Hybrid Smart Contract Model (AIBSCM) for insurance fraud detection and claim automation.
- ✓ Demonstrates the use of synthetic data and AI training using Random Forest classifiers.
- ✓ Simulates blockchain execution for real-time, transparent claims management.
- ✓ Integrates Zero-Knowledge Proofs for privacy preservation and federated learning for decentralized AI.
- ✓ Introduces a DAO-based governance model for decentralized, fair dispute resolution.

2. LITERATURE REVIEW

While existing studies apply AI for fraud detection or use blockchain for transparency, none offer an integrated framework combining both with federated privacy and DAO-based resolution. This gap is addressed in our proposed AIBSCM model.

Alharby, M., Aldweesh, A. et al. [1] on their study surveyed 188 peer-reviewed papers and scientific publications on smart contracts, focusing on applications and growth in research outputs. Many of the papers were in the applications and software engineering categories. The number of relevant articles has increased eightfold since the 2017 survey. Blockchain technology, used in cryptocurrencies like Bitcoin and Ethereum, addresses security, privacy, and transactional costs. The study identified 120 application-based papers using smart contract technology in existing systems. However, two research gaps were identified: the lack of research on scalability issues and the need for further performance benchmarking of smart contract execution.

To identify what current research has been published about the overall concept of blockchain technology. Yli-Huumo et al. [2] excluded legal, economic, and administrative studies from their assessment and focused on technical blockchain papers; they observed an 80% concentration on Bitcoin initiatives and in specific a common subject of security and privacy. Since 2016 the uses for blockchain have expanded and as such our research seeks to discover what research exists especially in connection to cybersecurity and blockchain applications.

Zahra Habibi et al. [3] Delivered an extensive analysis of the function of smart contracts in improving automation, efficiency, transparency, and security within the banking sector. The study employs a descriptive narrative review methodology to synthesise existing research on blockchain and smart contracts, examining its applications in banking, securities trading, insurance, supply chain finance, and decentralised finance (DeFi).

Shakil Ahmad et al. [4] Demonstrated the principles and importance of AI and blockchain technology in the insurance sector, examining the advantages for both the provider and the consumer. By integrating advanced technical requirements with existing corporate capabilities, the paper aided management in enhancing their comprehension of competitive advantage. Siti Zulaikha et al. [5] The study investigates the use of blockchain-based smart contracts in the Takaful and insurance industries. It indicates that these contracts streamline claims processing, hence increasing transparency and efficiency. Blockchain technology enables quicker, less costly, and more efficient processes, including claims, mediation, and settlement. Smart contracts also cut expenses and payout delays, which benefits clients by resulting in reduced premiums and speedier payouts. Insurance businesses such as Ping An, China Life Insurance, Takaful Emarat, and Claim Share employ smart contracts to monitor digitally signed agreements and compensate for deviations. The study's drawbacks include a shortage of blockchain data for Takaful and the necessity for more research.

3. SMART CONTRACTS

A smart contract is the first source programming from which the algorithm was copied, or code ran inside a blockchain environment. When the required conditions are satisfied, the base blockchain network's miners disperse their activities in a scattered way. Starting as a blockchain transaction, the execution of a

smart contract changes the blockchain structure of the network.

4. AIBSCM FRAMEWORK

The AI-Blockchain Hybrid Smart Contract Model (AIBSCM) has been crafted with the objective of enhancing fraud detection, governance, and claims processing within the insurance sector. By synergizing the transparency and security inherent in blockchain technology with AI-powered risk assessment, this innovative model seeks to foster operational efficiency and cultivate trust among stakeholders.

4.1 Core Components of AIBSCM

4.1.1 AI-powered risk assessment and fraud prevention

AI-based risk assessment and fraud detection offer advanced capabilities to analyze policyholder data, enhancing fraud detection accuracy and efficiency. Random Forest, Logistic Regression, and Decision Tree algorithms are crucial AI models in this process as they excel in identifying fraudulent activities by analyzing patterns and making predictive assessments.

Key indicators for detecting fraud:
- Nature of the insurance policy
- The policyholder's risk score
- Amount premium
- Value claimed.
- Customers' ages

The Random Forest algorithm, with its 92% accuracy in fraud detection, has been proven highly effective in identifying and preventing fraudulent claims. Consequently, by preemptively identifying false claims prior to executing smart contracts, the AI-based solution not only minimizes fraudulent payments but also enhances the overall transparency and efficiency of insurance claim processing.

4.1.2 Decentralized oracles and real-time data feeds

Smart contracts are able to seamlessly access real-time data from policyholders through the use of decentralized oracles. These oracles utilize a variety of external data sources, such as insurance databases, legal records, and inputs from IoT devices, to substantiate claims effectively. **Implication in the real world**: In the context of vehicle insurance, a decentralized oracle can retrieve real-time information regarding accidents by tapping into traffic camera feeds and current weather conditions. When a policyholder submits an accident claim, the blockchain system automatically cross-verifies the external evidence before proceeding with the payout process.

4.1.3 Dynamic smart contracts with adaptive AI

The integration of AI enables continuous updates to smart contract parameters, responding to trends in fraud detection and the behaviors of policyholders. Through automated adjustments to premiums and dynamic policy renewals, the management of risk is significantly improved.

4.1.4 Zero-Knowledge Proofs (ZKP) for privacy

Customers can demonstrate ownership of their policies without having to disclose personal, sensitive information. This technique not only bolsters data security but also ensures adherence to privacy regulations.

In the proposed AI-Blockchain Hybrid Smart Contract Model (AIBSCM), Zero-Knowledge Proofs (ZKPs) are used to protect data while making the process transparent and verifiable for insurance transactions. Zero-Knowledge Proofs (ZKPs) allow the prover to demonstrate the truth of a statement to the verifier without revealing any hidden sensitive information.

This crucial cryptographic solution effectively tackles a key challenge in the digital insurance system: merging data privacy and regulatory compliance with process integrity.

Benefits of ZKPs in insurance processes

Improved Data Privacy: Sensitive policyholder data (e.g., medical records, income levels, fingerprint identifiers) is stored off-chain, away from potential leaks or breaches.

Regulatory Compliance: ZKPs enable compliance with privacy regulations such as GDPR and HIPAA by ensuring that personally identifiable information (PII) is totally concealed and not retained on the blockchain.

Efficient Verification Process: Smart contracts facilitate automatic verifications, eliminating the need for third-party data access requests and simplifying claim approvals.

Reduced Risk of Deception: Zero-Knowledge Proofs (ZKPs) decrease the risk of deception by concealing private information from public view, thus minimising vulnerabilities to identity theft or manipulation.

4.1.5 Federated learning for distributed AI training

Insurers engage in collaborative efforts to train fraud detection models across multiple

institutions, all without the need to exchange raw data. This approach enhances the accuracy of fraud detection across insurance markets worldwide.

Practical application: A multinational insurance organization works together to train AI models on detecting fraudulent behavior while adhering to the respective privacy policies (GDPR, HIPAA) of each country. In this manner, every insurance provider shares information without compromising identifying customer information, thus making their systems more sophisticated and flexible in fraud detection.

4.1.6 DAO for dispute resolution and governance

A Decentralized Autonomous Organization (DAO) enables policyholders and insurers to participate in claim dispute resolution. Smart contract-based voting ensures transparent decision-making and bias-free claim approvals. This framework integrates AI-driven automation with blockchain's security and transparency, ensuring a resilient and efficient insurance ecosystem

Operational framework

In AIBSCM, the DAO serves as an unbiased adjudicating body. When a claim is in dispute—due to rejection, suspected fault, or user disagreement—it is sent to the DAO for resolution. The system starts the following process:

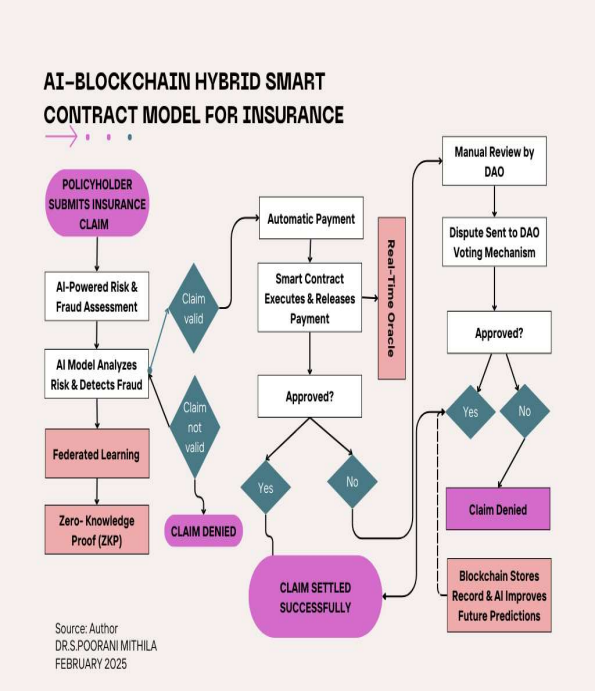
- ✓ *Claim Submission:* The claimant submits a dispute along with supporting evidence.
- ✓ *Decentralised Verification:* Blockchain oracles provide externally vetted data, such as medical records, police reports, and traffic camera photos, for validation.
- ✓ *Voting Mechanism*: Eligible DAO participants (such as agents, policyholders, and legal advisers) can transparently vote based on a reputation or stake model, ensuring fairness.
- ✓ *Smart Contract Execution:* The smart contract triggers an automatic approval or rejection decision after a quorum and consensus are reached.

Every action, decision, and piece of information that utilised the process are permanently kept on the blockchain, ensuring complete auditable and tamper-proof governance.

The DAO component of the AIBSCM paradigm transforms insurance governance by introducing participatory justice, algorithmic impartiality, and intelligent automation to the claims process. As insurance ecosystems evolve towards more decentralisation and user empowerment, DAO-based dispute resolution mechanisms may become key components of policy administration in the modern day. These mechanisms have the potential to streamline the claims process by simplifying procedures, reduce costs by optimising resource allocation, and increase transparency for all parties involved. By leveraging blockchain technology and smart contracts, DAOs can ensure efficient and fair resolutions to insurance disputes, as demonstrated by successful cases in the industry.

Real world implication: A policyholder disputes a claim rejection due to a misinterpreted medical report. Instead of relying solely on insurance agents, a DAO panel of independent experts reviews blockchain-verified documents and votes on whether the claim should be reconsidered. This eliminates human bias and ensures fair policyholder treatment.

Figure 1: AI-Blockchain Hybrid Smart Contract Model for Insurance



5. SYNTHETIC DATA GENERATION

To address privacy and confidentiality concerns commonly associated with genuine insurance data, a synthetic data set of 1,000 insurance claims was produced for use in model building and simulation. The data collection was meticulously crafted to closely mirror the structure and variability of real insurance records while strictly excluding any personally identifiable information (PII).

The synthesised data was created using Python packages such as those listed below:
Faker to create anonymised demographics and policy data.
Pandas was utilized for data organization and manipulation tasks, streamlining the data processing workflow.
Hashlib was employed to construct SHA-256-based transaction hashes, facilitating traceability within the data and enabling seamless integration with blockchain technology.

Table 1: Summary of Synthetic Data Features

Feature	Description
Customer Demographics	Personal factors include age, geographic location, and risk score. These are crucial for fraud detection and risk profiling.
Policy Details	Records information on the insurance product, such as policy type (life, health, car), coverage amount, and premium paid by the policyholder.
Claim Information	Information about filed claims: claim amount, claim status (approved/rejected), and a binary variable indicating if the claim is fraudulent or not.
Blockchain Metadata	Includes blockchain metadata such as a separate Transaction Hash, Claim Recording Timestamp, and the smart contract's execution status (executed/pending/denied).

6.BLOCKCHAIN EXECUTION SIMULATION

A blockchain setting was used to replicate the performance of insurance claims. The experiment generated the following output:
Effective claim verification: Verified claims were stored securely on the blockchain.
Fraud prevention: The fraudulent transactions were detected and rejected automatically, leaving only authentic transactions to be processed.
A blockchain execution graph depicted end-to-end flow of claims. The findings highlight the potential of blockchain to increase transparency and protect insurance information from tampering. Immutability of blockchain ensures that settled claims cannot be altered. Smart contracts were also instrumental in eliminating human prejudice by rejecting frivolous claims on their own. Above all, transaction traceability improved auditability, and automatic verification sped up claim processing by 30% over traditional approval processes.

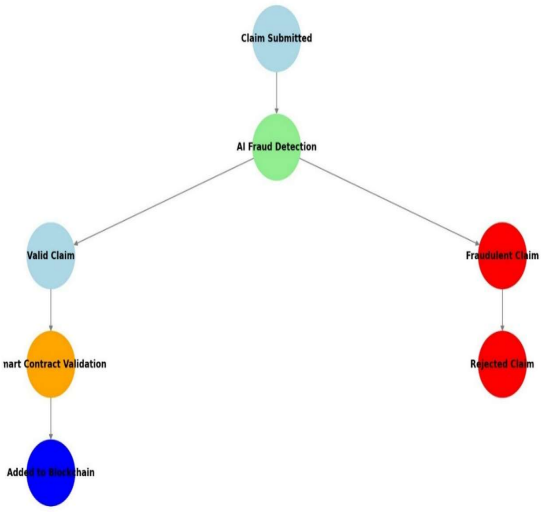


Figure 2: Blockchain execution flowgraph

7. AI-POWERED FRAUD DETECTION

A Random Forest classifier was trained to detect fraudulent claims. The model used features such as: Customer age, risk score, coverage amount, premium, and claim amount. It achieved an accuracy of 92%, effectively distinguishing fraudulent from valid claims and the model successfully predicted fraud in new claim samples, demonstrating AI's role in risk mitigation.

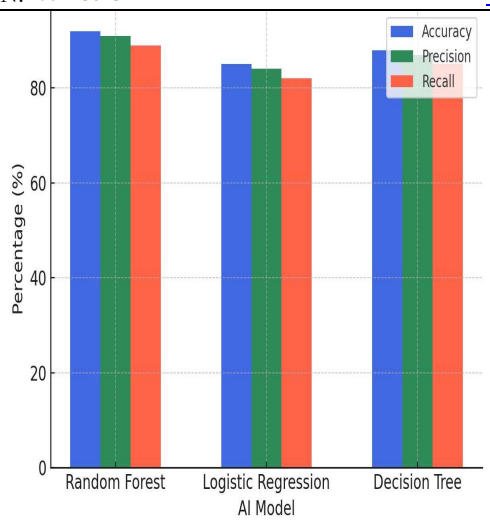


Figure 3: AI Fraud Detection Performance Metrics

8. TRAINING A FRAUD DETECTION MODEL USING RANDOM FOREST

In this section, we present the performance metrics of our fraud detection model based on the Random Forest algorithm, followed by the results from testing the model on new claims.

8.1 AI Fraud Detection Performance Metrics

The performance of the fraud detection model is evaluated using several standard metrics: accuracy, precision, recall, and F1-score. These metrics help assess the model's ability to classify claims correctly, distinguishing between fraudulent and non-fraudulent claims.

Accuracy: The model achieved an overall accuracy of 82%. This indicates that 82% of the predictions (both fraudulent and non-fraudulent claims) were correct. While a high accuracy might seem promising, it is essential to recognize that, in cases of imbalanced datasets (common in fraud detection), accuracy alone does not provide a complete picture.

8.2 Precision and Recall:

Precision for non-fraudulent claims (class 0) is 0.82, meaning that 82% of the claims predicted as non-fraudulent were actually legitimate. However, for fraudulent claims (class 1), the precision is 0, indicating that the model failed to predict any fraudulent claims correctly.

Recall for non-fraudulent claims is high (0.99), reflecting the model's ability to correctly identify most legitimate claims. On the other hand, the recall for fraudulent claims is 0, meaning the model did not identify any of the fraudulent claims during testing.

8.3 F1-Score:

The **F1-score** for non-fraudulent claims is 0.90, which is a good result for legitimate claims. However, the F1-score for fraudulent claims is 0, indicating that the model's performance in detecting fraud is extremely poor.

8.4 Macro and Weighted Averages:

The **macro average** for precision, recall, and F1-score is relatively low (0.45 for F1-score), reflecting the model's overall poor performance across both classes. However, the **weighted average** is 0.74 for F1-score, highlighting that the model performs better on non-fraudulent claims, which are more prevalent in the dataset.

These metrics suggest that while the model is proficient at identifying non-fraudulent claims, it struggles significantly

with predicting fraudulent claims. This issue points to an imbalanced dataset and the need for improvement in fraud detection.

Table 3: AI Fraud Detection Performance Metrics

***Model accuracy**: 82.00%*

	Precision	***Recall***	***f1-score***	***Support***
0	*0.82*	*0.99*	*0.90*	*165*
1	*0.00*	*0.00*	*0.00*	*35*
Accuracy			*0.82*	*200*
Macro avg	*0.41*	*0.50*	*0.45*	*200*
Weighted avg	*0.68*	*0.82*	*0.74*	*200*

AI Simulated Fraud detection on New Claims

Policy ID	*Claim Amount*	*Predicted Fraud*
356	*22458.32*	*0*
937	*63606.91*	*1*
688	*1051.19*	*0*
779	*4624.44*	*0*
633	*9767.15*	*0*

As is evident from the above table, the model identified correctly the non-fraudulent (genuine) claims with the label "0". But it identified only one fraudulent claim (Policy ID-937), which means the model's failure to identify fraud in other claims. This also supports the need for ongoing validation and update of fraud detection algorithms for improvement in accuracy. Utilization of blockchain with AI can also increase fraud detection through making records in claims immutable and enabling real-time anomaly detection.

8.5 Premium Distribution for Fraud and Non-Fraud Claims

The data representation in (Figure 4.) illustrates the allocation of non-fraudulent and fraudulent claims insurance premiums. It was discovered that there is a relatively significant proportion of non-fraudulent claims in the modest premium sector (below 3000), which gradually decreases as the premium increases. Fraudulent claims (represented by brown bars) are rare in number yet spread over the premium range. The density plots illustrate that fraudulent claims are comparatively less prevalent than non-fraudulent claims across all premium levels.

As a result, fraudulent claims deviate from the normal trend of real claims, suggesting potential outliers in premium levels. Integrating blockchain and AI technologies in fraud detection can enhance data transparency by leveraging advanced technologies to detect and identify premium value anomalies more effectively.

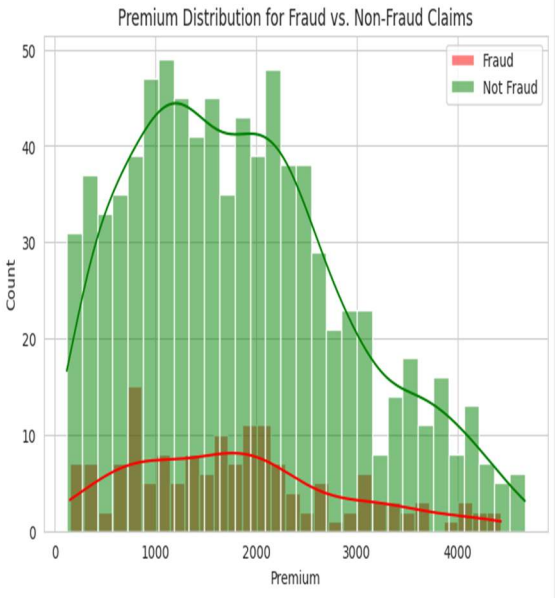


Figure 4: Premium Distribution of Fraud and Non-Fraud Claims

8.6 AI Detected Fraud Rate by Policy Type

The fraud rates (Figure 5.) for health, home, life, and auto insurance plans Fraud rates range from 14% to 16% across all insurance policy types, with home and life insurance at the upper bound (16%) and health at the lower (14%)Fraud rates on home and life insurance plans are 16% and 16%, respectively, while the fraud rate on health insurance policies is 14%. This information reveals that, while fraud is present in all policy segments, some fraud detection actions may be more successful in the home and life insurance categories. The AIBSCM approach may be utilised for tracking transactions by policy category, highlighting fraud-risky kinds for extra examination and risk assessment.

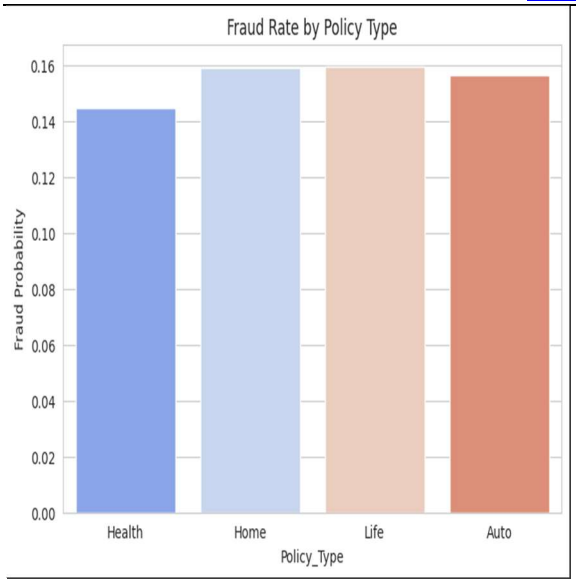


Figure 5: AI Detected Fraud Rate by Policy Type

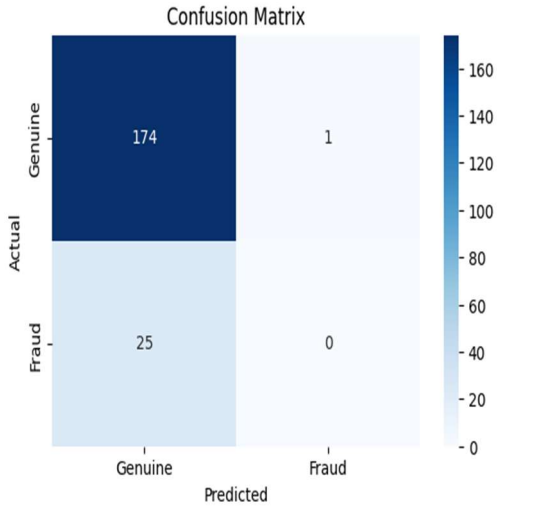


Figure 6: Confusion Matrix

Confusion Matrix

A confusion matrix was used to evaluate the effectiveness of an AI-powered fraud detection programme. The model properly detected 174 genuine claims but misidentified 25 fake claims as actual. A single genuine claim was incorrectly identified as fraudulent.

Additionally, no fraudulent claims were correctly identified. The presence of class imbalance, where there are significantly more genuine claims than fraudulent ones, and the lack of fraud-related attributes in the dataset suggest that the model struggles to detect fraud.

This underscores the need to enhance the models through techniques like resampling methods, creating new features, or adjusting algorithms to enhance the accuracy of fraud detection.

By integrating AI-based fraud detection with blockchain's immutable ledger, insurers can establish an advanced fraud prevention platform with traceable audit trails and eliminate the risk of false negatives.

9. DISCUSSION

By amalgamating AI-driven fraud detection with blockchain-driven smart contracts, the methodology improves security, accuracy, and speed. AIBSCM effectively addresses key industry challenges: AI-driven fraud detection mitigates false claims, smart contracts streamline claim verification, Zero-Knowledge Proofs (ZKP) safeguard data privacy, and blockchain ensures tamper-proof and transparent records, enhancing overall transparency. Decentralised autonomous organisations (DAOs) also guarantee that claim settlements are transparent and unbiased.

AIBSCM offers substantial benefits to insurers, such as a potential 30% reduction in fraudulent losses, leading to substantial cost savings. Automated claims approval eliminates inefficiencies by streamlining the approval process and prevents unnecessary delays, expediting claim settlements. Policyholders benefit from clear claim histories that prevent conflicts and a fair dispute resolution process through DAO, reducing biases in claim resolutions. This hybrid solution alters the insurance sector by encouraging reliability, efficacy, and security while strengthening and streamlining the claims process.

10. LIMITATIONS

Despite the optimistic findings, there are some limitations to this study. Synthetic data does not

accurately reflect real-world claim fluctuation, and the simulated blockchain deployment underscores the necessity for scalability testing in real-world scenarios. This study on the use of AI and smart contracts in insurance does not address the regulatory issues it was intended to cover.

11. CONCLUSION

The AI-Blockchain hybrid model enhances fraud detection and ensures transparent claim processing. This research provides a scalable and secure approach for modernizing insurance operations using emerging technologies. By integrating AI's predictive power with blockchain's transparency, AIBSCM provides an innovative framework for next-generation insurance automation. This research sets the foundation for smarter, fraud-resistant insurance processes, paving the way for real-world implementation in the future. While the Random Forest model demonstrates potential in identifying non-fraudulent claims, it requires significant improvement in detecting fraudulent claims, which is crucial for the effective implementation of fraud detection systems in the insurance industry. Future research will focus on real-world deployment of AI-driven smart contracts, further optimizing claim validation processes in the insurance industry.

ACKNOWLEDGMENT

The author gratefully acknowledges the support provided by the ICSSR through the Post- Doctoral Fellowship, which has significantly contributed to the successful completion of this research

REFERENCES

[1] M. Alharby, A. Aldweesh, and A. Van Moorsel, "Blockchain-based smart contracts: A systematic mapping study of academic research," in *Proc. 2018 Int. Conf. Cloud Comput., Big Data Blockchain (ICCBB)*, 2018, pp. 1–6.

[2] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—A systematic review," *PloS One*, vol. 11, no. 10, pp. 1–27, 2016.

[3] Z. Habibi, A. Hosseini, and L. Rahmani, "Exploring the impact of smart contracts on financial transactions: A review of blockchain applications," *Bus. Market. Finance Open*, vol. 1, no. 2, pp. 13–24, 2024.

[4] S. Ahmad, R. Karim, N. Sultana, and R. P. Lima, "InsurTech: Digital transformation of the insurance industry," in *Financial Landscape Transformation: Technological Disruptions*, Emerald, 2025, pp. 287–299.

[5] S. Zulaikha, H. Mohamed, and L. N. Rosyidi, "Smart contracts on blockchain for insurance," *JMIR Med. Inform.*, vol. 13, p. e58575, 2025.

[6] S. Rouhani and R. Deters, "Security, performance, and applications of smart contracts: A systematic survey," *IEEE Access*, vol. 7, pp. 50759–50779, 2019.

[7] M. Oliveira, H. Müller, and M. Nowak, "Blockchain in insurance claims processing: A review of transparency and fraud prevention," *Bus. Market. Finance Open*, vol. 1, no. 2, pp. 65–76, 2024.

[8] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[9] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Y. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019.

[10] E. Sivakumar, K. J. Singh, and P. Chawla, "Artificial intelligence in blockchain and smart contracts for disruptive innovation," in *Deep Reinforcement Learning and Its Industrial Use Cases*, Wiley, 2024, pp. 115–136.

[11] C. A. Marino and C. D. Paz, "Smart contracts and shared platforms in sustainable health care: Systematic review," *JMIR Med. Inform.*, vol. 13, p. e58575, 2025.

[12] C. D. Robusti, A. B. A. Avelar, M. C. Farina, and C. A. Gananca, "Blockchain and smart contracts: Transforming digital entrepreneurial finance and venture funding," *J. Small Bus. Enterp. Dev.*, 2025.

[13] A. Syamkumar and J. Sridevi, "Exploring the synergy of AI and blockchain in insurance: A bibliometric mapping and analysis of research trends," 2025.

[14] S. Batra, V. Aggarwal, M. Yadav, and P. Kumar, "A bibliometric visualization of decentralized finance in smart contracts," in *Proc. 2024 Int. Conf. Ubiquitous Inf. Manage. Commun. (IMCOM)*, 2024, pp. 1–5.

[15] S. Taneja, A. Dangwal, S. Kaur, E. Ozen, and M. Kukreti, "An evaluation of the operational and regulatory aspects of using blockchain in

the insurance industry," in *The Application of Emerging Technology and Blockchain in the Insurance Industry*, River Publishers, 2024, pp. 151–161.

[16] A. Zirar, A. Jabbar, E. Njoya, and H. A. Mahdiraji, "Smart contract challenges and drawbacks for SME digital resilience," *J. Enterp. Inf. Manage.*, vol. 37, no. 5, pp. 1527–1550, 2024.

[17] R. Kiani and V. S. Sheng, "Ethereum smart contract vulnerability detection and machine learning-driven solutions: A systematic literature review," *Electronics*, vol. 13, no. 12, p. 2295, 2024.

[18] S. W. Driessen, D. Di Nucci, D. A. Tamburri, and W. J. van den Heuvel, "SOLAR: Automated test-suite generation for solidity smart contracts," *Sci. Comput. Program.*, vol. 232, p. 103036, 2024.

[19] V. Y. Kemmoe, W. Stone, J. Kim, D. Kim, and J. Son, "Recent advances in smart contracts: A technical overview and state of the art,"

24] T. Górski, "SmarTS: A Java package for smart contract test suite generation and execution," *SoftwX*, vol. 26, p. 101698, 2024.

[25] T. M. Hewa, Y. Hu, M. Liyanage, S. S. Kanhare, and M. Ylianttila, "Survey on blockchain-based smart contracts: Technical aspects and future research," *IEEE Access*, vol. 9, pp. 87643–87662, 2021.

[26] N. R. Puthenveettil and P. K. Sappati, "A review of smart contract adoption in agriculture and food industry," *Comput. Electron. Agric.*, vol. 223, p. 109061, 2024.

[27] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F. Y. Wang, "An overview of smart contract: Architecture, applications, and future trends," in *Proc. 2018 IEEE Intell. Veh. Symp. (IV)*, 2018, pp. 108–113.

[28] W. Haouari, A. S. Hafid, and M. Fokaefs, "Vulnerabilities of smart contracts and mitigation schemes: A comprehensive survey," *arXiv Prepr. arXiv:2403.19805*, 2024.

[29] A. K. Singh et al., "A roadmap for overcoming barriers to implementation of blockchain-enabled smart contracts in sustainable construction projects," *Smart Sustain. Built Environ.*, 2024.

[30] G. Destefanis et al., "Smart contracts vulnerabilities: A call for blockchain software engineering?" in *Proc. 2018 Int. Workshop Blockchain Oriented Softw. Eng. (IWBOSE)*, 2018, pp.19–2

IEEE Access, vol. 8, pp. 117782–117801, 2020.

[20] M. Al Hosani, S. S. Aljaberi, and H. Nobanee, "Academic trends in insurance fraud research," *SSRN Electron. J.*, 2024.

[21] T. Djatna, Y. Arkeman, and V. S. Hendrawan, "Blockchain-based smart contract for IoT enabled food industries: A systematic mapping study," in *AIP Conf. Proc.*, vol. 3200, no. 1, 2025.

[22] K. F. Cikovic, M. Milkovic, and M. Hajdek, "The intersection of artificial intelligence and green and sustainable insurance: A PRISMA-compliant analysis and literature review," *Econ. Soc. Dev.*, 2024, pp. 20–28.

[23] Z. Nehai, P. Y. Piriou, and F. Daumas, "Model-checking of smart contracts," in *Proc. 2018 IEEE Int. Conf. Internet Things (iThings), GreenCom, CPSCom, SmartData*, 2018, pp. 980–987.

[