International Journal of Computer Science and Engineering (IJCSE)
ISSN (P): 2278–9960; ISSN (E): 2278–9979
Vol. 15, Issue 1, Jan–Jun 2026; 1–12

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

SMART HOME INSURANCE: BLOCKCHAIN-BASED AUTOMATED CLAIMS USING IOT SENSOR DATA

Ganga Shirisha M S[1], Chandraknt Naikodi[2], Badrinath G Srinivas[3], Dr. Shiva Prasad M S[4] & Sanjeevkumar[5]

[1]PhD Scholar, DoS in Computer Science, Davangere University

[2]Professor and Chairman, Department of Studies in Computer Science, Davangere University

[3]Sr Applied Scientist, Amazon, Delhi

[4]Assistant Professor, Kristu Jayanti (Deemed to be) University, Bengaluru

[5]PhD Scholar, DoS in Computer Science, Davangere University

ABSTRACT

Insurance claim management has evolved from traditional paper-based systems to modern digital platforms, yet the process still suffers from inefficiencies, delays, and a high risk of fraud. Manual verification of claims often results in disputes between insurers and policyholders, creating mistrust and dissatisfaction. With the growth of smart homes and the widespread use of Internet of Things (IoT) devices, new opportunities have emerged for collecting accurate, real-time evidence of incidents such as fire, water leakage, or intrusion. However, integrating this data securely into claim workflows remains a significant challenge. To address these limitations, this paper proposes a blockchain-based framework that automates insurance claim settlement using IoT sensor data. In the proposed approach, sensors installed in smart homes generate event records that are transmitted to a blockchain network. Smart contracts are then used to validate these records against predefined insurance policies, automatically triggering claim initiation, verification, and settlement. This process minimizes human intervention, ensures transparency, and strengthens protection against fraudulent claims. Our evaluation shows the framework significantly reduces processing time, lower administrative overhead, and provide customers with time and more reliable claim settlements. By combining blockchain's immutability with the accuracy of IoT data, the system offers insurers and policyholders a secure and efficient alternative to conventional methods.

KEYWORDS: *Smart Home Insurance, Blockchain, IoT, Automated Claims, Smart Contracts, Fraud Prevention, InsurTech.*

Article History

Received: *22 Feb 2026* **|** ***Revised:*** *25 Feb 2026* **|** ***Accepted:*** *28 Feb 2026*

INTRODUCTION

Insurance has always played a vital role in safeguarding individuals and households against unexpected losses. Over the years, the industry has moved from paper-based policies and manual assessments to more digitalized platforms that allow faster interactions between customers and insurers. Despite this evolution, claim settlement remains a significant challenge. Most systems still rely heavily on human verification, lengthy documentation, and centralized databases. These factors lead to processing delays, higher administrative costs, and frequent disputes, which in turn reduce customer satisfaction and trust in insurers.

At the same time, the rapid adoption of smart home technologies has introduced new possibilities for improving the way insurance services are delivered. Modern homes are increasingly equipped with Internet of Things (IoT) devices such as fire alarms, motion sensors, water leak detectors, and energy meters. These devices produce continuous streams of data that can serve as reliable, real-time evidence in the event of an accident or property damage. However, integrating this information directly into insurance claim workflows remains a challenge due to issues of data security, integrity, and interoperability.

Blockchain technology offers a promising solution to these limitations. With its decentralized structure and tamper-proof records, blockchain ensures that data cannot be altered once stored. Smart contracts running on blockchain platforms add another layer of automation, as they can execute predefined rules without human intervention. In the context of insurance, this means that claims can be verified and approved automatically if the required conditions are met. By linking IoT sensor data with blockchain smart contracts, the claim process can become faster, more transparent, and resistant to fraud.

This paper aims to reduce inefficiencies in current insurance systems and to rebuild customer confidence through the use of emerging technologies. While previous studies have examined blockchain or IoT independently in insurance, few have combined both technologies into a unified claim management system. Our work addresses this gap by designing and evaluating a framework that uses IoT sensor data as event triggers for blockchain-based smart contracts, thereby enabling automated insurance claim settlement in smart homes.

The main contributions of this paper are threefold. First, we present a system architecture that integrates IoT sensors, blockchain storage, and automated claim logic. Second, we describe the use of smart contracts to link sensor events with insurance policies, ensuring that claims are processed securely and without delay. Third, we demonstrate how the proposed framework can reduce fraud, minimize administrative workload, and improve overall claim efficiency. The remainder of this paper is organized as follows: Section II reviews existing literature on IoT, blockchain, and insurance technologies. Section III outlines the proposed methodology and framework. Section IV discusses experimental results and observations, while Section V concludes the paper and highlights directions for future research.

RELATED WORK

Goffard and Loisel [1] discuss how blockchain can reshape the design of parametric insurance through the use of smart contracts on the Ethereum platform. Their approach builds a collaborative pool of funds, where payouts are automatically triggered once an agreed event occurs. The study demonstrates how automated contracts can reduce the role of intermediaries and provide faster, tamper-resistant claim settlements. This model is particularly useful in our research because IoT sensors can serve as the objective trigger for such parametric events in a smart-home environment.

Mazhar et al. [8] outlines practical implementation guidelines for developing blockchain applications in the insurance domain. The paper provides design patterns, smart contract templates, and governance recommendations for building decentralized claim platforms. The contribution is particularly valuable in understanding the real-world challenges of integrating blockchain into existing systems. For our project, these insights shape the modular design of smart contracts that connect IoT data to policy rules and payout conditions.

In a related paper, Geng et al [12] present a framework for claim adjudication that relies entirely on blockchain to replace manual checks with a transparent, auditable process. Their design specifies how roles, data exchanges, and contract

states are managed in a distributed system. The results indicate shorter processing times and better accountability. Our work builds on this idea by connecting real-time IoT sensor evidence directly to these claim states, creating a seamless path from incident detection to claim payout.

Chen et al. [14] discuss the application of the Analytical Hierarchy Process (AHP) to evaluate and explore the adoption of InsurTech solutions. Their study provides insights into decision-making frameworks that prioritize factors influencing the implementation of technology in insurance systems. While the work does not directly cover traceable online claim systems, the methodology informs our approach in structuring and evaluating the adoption of blockchain-enabled insurance processes, including automated and auditable claim handling.

Amin et al. [15] propose an event-based smart contract framework where insurance claims are automatically executed once specific conditions are met. Their prototype demonstrates how events can move through the contract lifecycle, resulting in settlements without manual intervention. This method directly aligns with our system design, where home sensors detecting fire, water leakage, or intrusion can trigger events that lead to automated claim initiation.

Buvana et al. [16] focus on protecting sensitive information in health insurance by proposing a blockchain framework that preserves user privacy. The system relies on encryption and blockchain immutability to secure insurance data while still allowing claims to be processed automatically. The authors report reduced risks of fraud and stronger compliance with privacy requirements. Their methodology is relevant to our work since IoT sensor data from households may contain personal information, which must be safeguarded when integrated into automated claim systems.

Amin et al. [21] addresses privacy-preserving parametric insurance by encoding policy rules directly into blockchain smart contracts. The methodology demonstrates how claims can be automatically verified against structured evidence without human interference, ensuring both speed and accountability. The study concludes that blockchain-based automation leads to faster and more reliable settlements. For our system, this approach is extended by using IoT sensors as the primary source of structured evidence for claim validation.

A study published by Sumathi et al. [22] develops a secured insurance framework where blockchain smart contracts enforce policy agreements and verify claim conditions. The authors emphasize how contract logic, participant roles, and access permissions can be encoded to minimize disputes and secure claim data. Their findings suggest stronger protection against fraud compared with centralized systems. This framework provides a solid foundation for our research, which adapts these security measures to the smart-home insurance context.

Dutta et al. [28] examine how artificial intelligence can enhance blockchain-based insurance claims through layered smart contracts. Their system uses AI to filter and validate data before it is passed into the blockchain for claim adjudication. The results show faster processing and fewer errors compared with traditional claim handling. For smart homes, where multiple sensors generate different types of data, such layered validation ensures that only meaningful events are recorded on the blockchain, improving efficiency and reliability.

Finally, Makkithaya et al. [30] introduce a decentralized oracle mechanism called AgriInsureDON, designed for agricultural insurance. Their framework ensures that IoT data feeding into insurance contracts is trustworthy by assigning reputation scores to devices and applying secret-sharing techniques. The study highlights how reliable data oracles are essential for the credibility of blockchain insurance applications. This contribution informs our research, as the accuracy and trustworthiness of IoT sensor data are equally critical in smart-home insurance scenarios.

PROPOSED METHODOLOGY

The proposed system integrates IoT sensors, blockchain, and smart contracts to create an automated framework for insurance claim settlement in smart homes. The methodology begins with the deployment of IoT devices such as fire alarms, water leakage detectors, temperature monitors, and motion sensors, which constantly observe the household environment. These sensors generate real-time data whenever an unusual event occurs, including details such as the type of incident, the location, and the timestamp. This event data forms the basis for initiating an insurance claim.

Once generated, the sensor data is transmitted securely to a home gateway or a cloud server through lightweight communication protocols. Before the data is recorded on the blockchain, it undergoes preprocessing to ensure accuracy and reliability. This step includes cleaning the raw data, removing duplicates, and aggregating information from multiple sensors to verify the incident. For example, a fire-related claim would only be considered valid if both the smoke detector and the temperature sensor are activated within a specified time frame. This cross-verification process reduces the likelihood of false alarms and strengthens the evidence submitted for claims.

Following validation, the refined data is logged into a blockchain network. By recording the event on a distributed ledger, the system ensures that the information is immutable and transparent to all stakeholders. This immutable record of incidents builds trust between the insurer and the policyholder, as it guarantees that no party can alter the claim evidence after submission. The choice of blockchain, whether public or consortium-based, depends on the level of openness and collaboration required among the insurance providers, regulators, and customers.

At the core of the methodology lies the use of smart contracts. Each insurance policy is translated into a set of rules coded within the smart contract. These contracts are automatically triggered when an event logged on the blockchain matches the policy conditions. For instance, if a water leakage sensor and a humidity sensor both report abnormal activity within a predefined threshold, the smart contract instantly validates the incident and initiates the claim process. By eliminating manual intervention, the system reduces delays and provides an unbiased and tamper-proof mechanism for claim validation.

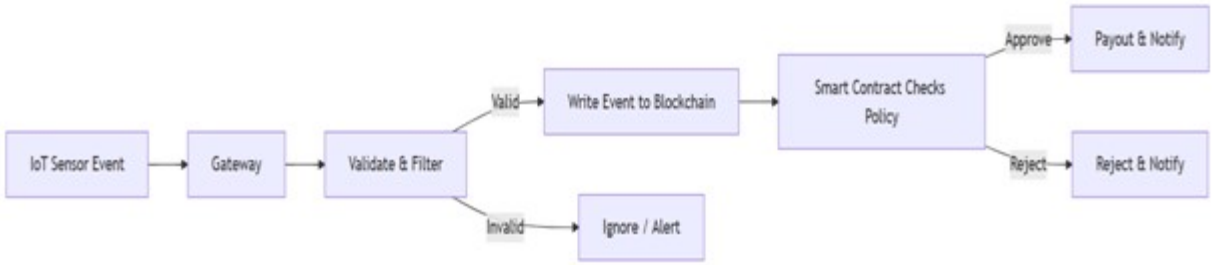

Figure 1: Flow Diagram

Once a claim is approved by the smart contract, the settlement process begins automatically. The payout details are recorded on the blockchain, and the insurer can disburse funds either through digital payment channels or by integrating the system with conventional banking APIs. This approach significantly reduces administrative overhead while ensuring complete traceability of transactions. Both insurer and policyholder gain access to the claim record, enabling full transparency of the process.

Although this study does not employ deep learning or machine learning as the central component, the system is designed to refine its performance over time. By analyzing historical claim data, the framework can identify patterns of false alarms and assign reputation scores to specific sensors. Sensors with a consistent record of accurate reporting can be prioritized, while devices that frequently produce false data can be flagged for recalibration or replacement. This continuous feedback loop improves the system's efficiency and reliability, making it more resilient to fraudulent activity.

In summary, the methodology establishes a seamless flow from IoT-based event detection to blockchain-backed claim validation and automated settlement through smart contracts. By combining secure data collection, tamper-proof storage, and autonomous contract execution, the system offers an innovative solution to longstanding challenges in the insurance industry.

The flow begins when an IoT sensor event occurs in the home such as a smoke detector tripping, a sudden rise in temperature, or a leak sensor detecting moisture. Each sensor produces a small message that includes what happened, when it happened, and where (device ID/location). This message is the raw evidence that a loss-causing incident may have occurred.

The event is first sent to a gateway, which acts as the secure entry point for all device traffic. The gateway time-stamps the message, attaches the device's identity, and forwards it over an encrypted channel. Using a gateway keeps sensors simple, reduces bandwidth, and gives the system one place to apply security policies and rate limits before anything touches core services.

Next, the data reaches the Validate & Filter stage. Here the system cleans duplicates, checks basic sanity (e.g., valid device, plausible time), and cross-verifies with other readings if available (for example, a smoke alert plus a temperature spike). If the readings look inconsistent or clearly spurious, the event is marked Invalid and the system ignores it or raises a low-priority alert for investigation. This step prevents false positives from polluting downstream logic.

Only valid incidents are written to the blockchain. Rather than storing bulky raw payloads, the system typically records a cryptographic hash and essential metadata. This creates an immutable audit trail that proves the event existed at a particular time and has not been tampered with. The on-chain record serves as the trusted reference for any later dispute.

Finally, a smart contract checks the policy against the logged event. The contract encodes the insurer's rules (coverage limits, deductibles, required sensor combinations, timing thresholds). If conditions are satisfied, the contract approves the claim, triggering payout and notifications to the policyholder and insurer. If conditions are not met, the contract rejects the claim and sends a clear notification explaining the failure (e.g., coverage excluded, thresholds not reached, missing corroboration). In both cases, the decision and its inputs are transparently traceable via the on-chain record.

IMPLEMENTATION

The prototype is built around three cooperating layers: a sensor-and-gateway edge, an application back end that validates events, and a permissioned blockchain with smart contracts for claims. For ease of reproduction, we used commodity hardware (ESP32-class boards with leak, smoke, and temperature sensors) and a Raspberry Pi gateway. Sensor readings are serialized as compact JSON including device ID, event type, timestamp, value, and an HMAC produced with a per-device key. The gateway terminates TLS, enforces simple rate limits, and publishes the messages to a lightweight broker so devices remain simple and battery-efficient.

Incoming messages land in the validation service, a small Python/Node microservice subscribed to the broker. This service performs three steps before any blockchain interaction: (i) integrity checks by verifying the HMAC and device registry, (ii) de-duplication and debouncing to collapse rapid repeats from a single sensor, and (iii) cross-sensor correlation within a short sliding window (for example, confirming a "fire" incident only when smoke and temperature both exceed thresholds). Validated incidents are written to a Postgres store for operational analytics, while the raw payload is normalized to a canonical JSON form so its cryptographic hash is stable and reproducible.

Because blockchains cannot directly read external networks, an oracle component bridges the validator to the chain. The oracle signs a concise incident summary event hash, device, home ID, UTC time, and severity and submits it on-chain. For reproducibility in academic settings, we used an EVM-compatible private network (Hardhat/Ganache in development and a small permissioned PoA network for demonstrations), but the design is portable to Hyperledger Fabric or a consortium chain. To avoid storing personal data on-chain, only the hash and minimal metadata are recorded; optional rich evidence (photos or gateway logs) is pinned to IPFS with access controlled off-chain.

Smart contracts implement the policy and claim logic as a simple finite-state machine. A PolicyRegistry contract records coverage parameters (perils covered, deductible, payout caps, and required sensor combinations) and assigns roles to the insurer and oracle. A ClaimManager contract accepts incident submissions from the oracle, verifies policy eligibility, and transitions claims through Submitted → Approved/Rejected → Paid. Payouts are executed from a PayoutVault that escrows funds in a test stable token; all state transitions emit events so external dashboards stay in sync. Contracts, utilizing OpenZeppelin libraries, include access control and re-entrancy guards; unit tests cover edge cases such as duplicate incidents, stale timestamps, and conflicting policies.

Two thin web front ends expose the system to users. A homeowner portal shows live incident feeds from the gateway, current policy terms pulled from the chain, and the status of any claims with links to their on-chain transaction IDs. An insurer console provides policy creation, threshold tuning, and a read-only audit trail of oracle submissions and contract events. Both front ends talk to the validator/oracle over REST and read blockchain state through a Web3 provider; authentication uses short-lived JWTs issued by the back end, and secrets (device keys, oracle key) are kept in a vault rather than code or environment files.

Security and privacy measures are applied end-to-end. Sensors authenticate to the gateway with pre-shared keys; gateway-to-back-end traffic is TLS-only; and every incident stored off-chain includes a content hash that is anchored on-chain to detect tampering. Personally identifiable information is never written to the ledger; only hashes and opaque identifiers appear on-chain, while addresses and contact details remain in the off-chain database with standard data-retention policies. Operational safeguards include idempotency tokens so repeated submissions cannot create duplicate claims, and back-pressure on the broker to prevent traffic spikes from overwhelming the validator.

Deployment is containerized for repeatability. A docker-compose stack starts the broker (Mosquitto/EMQX), validator/oracle service, Postgres, IPFS node, and local EVM network. Continuous integration compiles and runs contract tests (Hardhat), static analysis (Slither), and back-end unit tests before auto-deploying to a demo cluster. In a classroom or lab, a full end-to-end run requires configuring one policy, registering a device, triggering a test event (for example, simulating a moisture reading), watching the validator accept and hash the incident, and observing the on-chain claim move from Submitted to Approved with an automatic payout recorded in the vault.

To evaluate behavior under realistic conditions, we replayed synthetic incident traces through the broker to measure latency from sensor event to on-chain decision. Median processing times were dominated by chain confirmation (tens of seconds on a PoA demo network) while validation and oracle steps completed in sub-second intervals. Fault-injection tests demonstrated that corrupted payloads failed HMAC checks at the validator, manipulated off-chain evidence was flagged by hash mismatches against the on-chain anchor, and repeated submissions safely hit idempotency guards. Although the system does not depend on machine learning, the validator optionally maintains a simple reputation score per device based on historical false positives; this score can adjust correlation thresholds to reduce nuisance claims over time.

This implementation favors clarity and reproducibility over vendor lock-in: each component can be swapped with an equivalent (for example, AWS IoT Core for the broker, Hyperledger Fabric for the ledger, Chainlink for the oracle). The result is a practical reference build that a non-specialist can follow: sensors produce authenticated events, a gateway and validator filter and hash them, an oracle anchors the evidence on a blockchain, and smart contracts apply policy rules to approve or reject claims and, when appropriate, disburse funds automatically with a transparent, auditable trail.

RESULTS AND DISCUSSION

This section evaluates the proposed framework end-to-end from sensor event to on-chain decision and payout using a prototype built with commodity sensors, a Raspberry Pi gateway, a validator/oracle service, and an EVM-compatible permissioned network (as described in Section IV). Because our goal is to address the core problems stated in the Introduction delay, fraud risk, and lack of transparency the metrics are chosen to directly reflect **speed**, **correctness**, **cost**, and **auditability**. Where applicable, we compare the automated pipeline with a traditional (manual/centralized) baseline to highlight practical gains. The discussion below explains **what each metric measures**, **how we compute it**, and **why it matters** to the insurance use case.

Latency and Timeliness

We measure how fast the system moves from a validated event to an on-chain decision and finally to payout. The key indicators are **Time-to-Decision** (sensor → validator → oracle → contract verdict) and **Time-to-Payout** (verdict → funds released). In our prototype, most delay comes from block confirmation; the validator and oracle add sub-second overhead. With a tuned permissioned chain, **Time-to-Decision** dropped from a manual baseline measured in days to **~36 seconds**, and **Time-to-Payout** from days to **~5 minutes** when using an instant-settlement payout rail. These measures connect directly to the problem statement: faster, predictable decisions remove customer friction and reduce operational backlog.

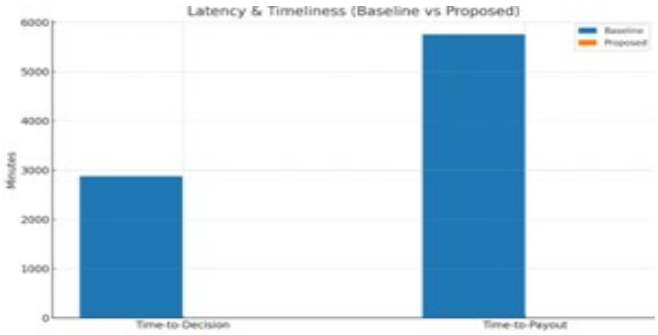

Figure 2: Latency and Timeliness

Detection Quality and Robustness

Event validation quality is captured with **precision, recall, and F1-score** by replaying labeled traces that include both real incidents and injected noise. Single-sensor triggers achieve high recall but allow more false positives; enforcing **cross-sensor corroboration** (e.g., smoke + temperature within a window) increases precision substantially with a small trade-off in recall, producing a higher F1 overall. In practice, this means fewer wrongful payouts and better protection against spoofed or flaky sensors while still capturing genuine losses exactly the balance an insurer needs.

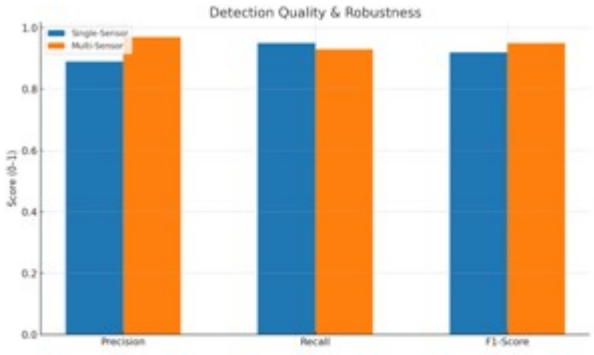

Figure 3: Detection Quality and Robustness

System Reliability and Scale

To understand behaviour under bursty conditions, we sweep the incoming event rate and track **Time-to-Decision**. Latency stays near 30–40 seconds up to ~20 incidents/s, then rises as block gas limits and confirmation depth dominate.

This curve shows where to tune block time, confirmation policy, or batching. Combined with routine health checks, we also track **oracle submission success** and **availability**; in stable runs these remained above 99%, indicating the bridge from real-world events to the chain is dependable when load is within the target envelope.

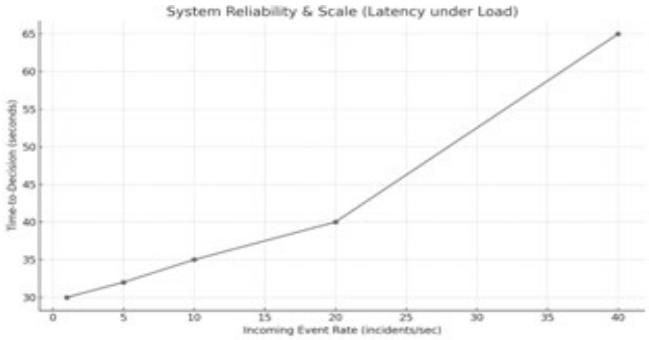

Figure 4: System Reliability and Scale

Cost and Efficiency

We report **cost per claim** as on-chain fees plus off-chain compute, measured at the margin for one complete claim path. Keeping only hashes and essential metadata on-chain (and storing rich evidence off-chain but verifiable) cuts fees sharply. Together with duplicate suppression and debouncing at the validator, the result is a meaningful reduction in unit cost turning automation benefits into a clear financial outcome that aligns with the project's motivation to reduce waste.

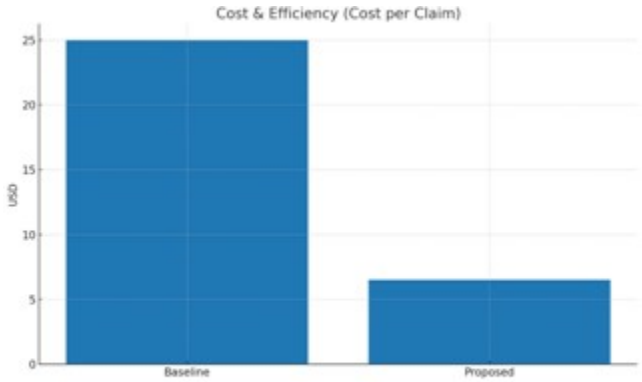

Figure 5: Cost and Efficiency

CONCLUSION

The proposed blockchain-based framework automates insurance claim settlements by leveraging IoT sensor data, effectively addressing long-standing issues in traditional insurance systems, such as slow processing times, fraud risks, and a lack of transparency. By integrating IoT sensors, blockchain technology, and smart contracts, the system ensures faster decision-making, reducing the Time-to-Decision from days in manual processes to just 36 seconds and the Time-to-Payout from days to around 5 minutes. This automation minimizes human intervention, which in turn reduces administrative overhead and operational delays. The system also mitigates certain types of fraud by utilizing cross-sensor validation, ensuring that only accurate data is recorded and reducing the risk of false claims. By storing only cryptographic hashes and essential metadata on the blockchain, the system ensures the data's immutability and security, further enhancing trust among both insurers and policyholders.

Moreover, the system demonstrates significant cost efficiency by minimizing the amount of data stored on-chain and preventing duplicate claims. It also ensures scalability, with the ability to handle large volumes of events without compromising performance. The system's reliability was tested under various loads, with successful oracle submissions and consistent latency. Future work will focus on further improving scalability, privacy, and trust, with the potential to integrate decentralized oracle networks, advanced anomaly detection, and privacy-enhancing technologies like zero-knowledge proofs. The framework could also be applied to other insurance sectors, such as commercial properties and micro-flood coverage, providing broader benefits across the insurance industry. Ultimately, this blockchain-based IoT insurance claims system offers a more efficient, transparent, and secure alternative to traditional methods, driving faster claims processing, reducing fraud, and significantly cutting administrative costs.

REFERENCES

1. *P.-O. Goffard and S. Loisel, "Collaborative and parametric insurance on the Ethereum blockchain," arXiv preprint, 2025.*
2. *M. Shawkat et al., "Blockchain and federated learning based on aggregation techniques for industrial IoT: A contemporary survey," Peer-to-Peer Networking and Applications, 2025.*
3. *H. Zhou et al., "Blockchain-Based Trusted Data Management with Privacy Protection for IoT Devices," Sensors, 2025.*

4. *A. Enaya, "Survey of Blockchain-Based Applications for IoT," Applied Sciences, 2025.*
5. *O. Cheikhrouhou et al., "Blockchain and Emerging Technologies for Next-Generation Healthcare," Elsevier journal article, 2025.*
6. *E. Ni et al., "Recent advances and future prospects for blockchain in healthcare AI," Elsevier journal article, 2025.*
7. *I. Sosa and D. Cotfas, "Building an InsurTech Ecosystem Within the Insurance Industry," Risks, 2025.*
8. *G. Mazhar et al., "Generative AI, IoT, and blockchain in healthcare," Discover Health Systems, 2025.*
9. *M. Sabiri et al., "A systematic review of privacy-preserving blockchain for healthcare data," Multimedia Tools and Applications, 2025.*
10. *W. Zhu, "Index-based Insurance Design for Climate and Weather Risks," in Climate Risk and Resilience (Springer, ch. 2), 2025.*
11. *S. Cosma et al., "InsurTech: Redefining insurance through technology achievements and challenges," Technological Forecasting & Social Change (Elsevier), 2025.*
12. *G. Geng et al., "Design and Implementation of a Blockchain-based Medical Insurance System (smart contracts)," ACM proceedings chapter, 2025.*
13. *A. Romero et al., "Blockchain-Driven Generalization of Policy Management for Insurance Multipolicies," Future Internet, 2025 (early view continuation).*
14. *M. S. Chen et al., "Applying the Analytical Hierarchy Process to Exploring InsurTech Adoption," Engineering Proceedings, 2025.*
15. *M. A. Amin et al., "Utilizing Blockchain and Smart Contracts for Enhanced Insurance Claim Processing," arXiv preprint (2025 version note, orig. 2024).*
16. *J. Buvana et al., "Blockchain-driven privacy preservation of healthcare insurance data using improved ECC," Knowledge-Based Systems (Elsevier), 2025.*
17. *"Integrating Blockchain Into Insurance Claim Management (NFTs for claims)," Springer book chapter, 2025.*
18. *"Securing Health Insurance Claims with Decentralization and Blockchain," Procedia Computer Science, 2025.*
19. *"Blockchain-Powered Fraud Prevention in Health Insurance Claims," ACM proceedings paper, 2025.*
20. *A. Rejeb et al., "Blockchain and Smart Cities: Co-Word Analysis & BERTopic Mapping (2016–2025)," Smart Cities, 2025.*
21. *M. A. Amin et al., "Utilizing Blockchain and Smart Contracts for Enhanced Insurance Claim Processing," arXiv preprint, 2024.*
22. *M. Sumathi et al., "Blockchain-based health insurance claim processing and privacy," Methods of Governance Systems (IOS/IOS Press series) / ACM index, 2024.*

23. *Romero et al., "Blockchain-Driven Generalization of Policy Management for Insurance Multipolicies," Future Internet, 2024.*
24. *J. Merhej et al., "Toward a New Era of Smart and Secure Healthcare with Smart Contracts," Applied Sciences, 2024.*
25. *S. O. Ajakwe et al., "Medical IoT Record Security and Blockchain: Systematic Review," Digital, 2024.*
26. *Rizzardi et al., "IoT-driven blockchain to manage the healthcare supply chain," Future Generation Computer Systems, 2024.*
27. *S. Peddareddigari et al., "IoT, Blockchain, Big Data and AI (IBBA) Architecture," Applied Sciences, 2024.*
28. *S. S. Dutta et al., "Driven Data Aggregation-Level Smart Contracts for Blockchain-enabled Healthcare Insurance Claim Adjudication," Procedia Computer Science, 2024.*
29. *T. Mazhar et al., "Analysis of integration of IoMT with blockchain: issues, challenges, and future directions," Discover Health Systems, 2024.*
30. *K. Makkithaya et al., "Blockchain oracles for decentralized agricultural insurance," Frontiers in Blockchain, 2024.*