E-ISSN: 2664-8784
P-ISSN: 2664-8776
IJRE 2025; SP-7(2): 21-23

www.engineeringpaper.net
Received: 13-04-2025
Accepted: 14-05-2025

Monika Thakran
Assistant Professor, Department Of Computer Science, DPG STM, Gurgaon, Haryana, India

Shikha Mathur
Assistant Professor, Department Of Computer Science, DPG STM, Gurgaon, Haryana, India

Dr. Priyajot
Assistant Professor, Department Of Computer Science, DPG STM, Gurgaon, Haryana, India

Correspondence
Monika Thakran
Assistant Professor, Department Of Computer Scirnce, DPG STM, Gurgaon, Haryana, India

Two-Days National Conference on Multidisciplinary Approaches for Innovation and Sustainability: Global solution for contemporary Challenges-NCMIS (DPG Degree College: 17th-18th 2025)

Leveraging blockchain for secure and autonomous domotics systems: Enhancing privacy and efficiency

Monika Thakran, Shikha Mathur and Dr. Priyajot

DOI: https://www.doi.org/10.33545/26648776.2025.v7.i2a.86

Abstract
The rapid expansion of domotics, or smart home systems, has transformed modern living through automation, remote monitoring, and intelligent control of household devices. However, as these systems increasingly rely on interconnected devices and centralized platforms, concerns regarding data privacy, security vulnerabilities, and single points of failure have become more pronounced. This paper explores the integration of blockchain technology into domotics systems as a solution to these challenges, offering a decentralized and tamper-resistant framework for enhancing security and operational autonomy.
By utilizing blockchain's distributed ledger mechanism, smart home environments can ensure trustworthy device communication, transparent data logging, and robust user authentication without dependence on centralized servers. The study analyzes how smart contracts can automate home functions—such as lighting, climate control, and access management—while maintaining user-defined rules in a secure and verifiable manner. Furthermore, the implementation of blockchain introduces improved data integrity and privacy, ensuring that sensitive household data remains encrypted and accessible only to authorized entities.
The paper presents a prototype model combining IoT-enabled smart devices with a blockchain backend to demonstrate practical feasibility and performance metrics, including latency, energy consumption, and system resilience. It also discusses scalability concerns and evaluates potential trade-offs between decentralization and resource efficiency.
Ultimately, this research highlights blockchain as a transformative enabler in the evolution of secure, efficient, and user-centric domotics systems, paving the way for more resilient and autonomous smart home ecosystems.

Keywords: Domotics, blockchain, smart contracts, home automation

Introduction
The rapid advancement of smart home technologies has led to a growing reliance on connected devices that automate and manage various household functions. These systems, known as domotics, encompass lighting, heating, ventilation, air conditioning, entertainment, and security devices, often orchestrated through cloud-based platforms. While this connectivity offers convenience and energy efficiency, it also exposes users to data privacy breaches, centralized point-of-failure risks, and unauthorized access.
Blockchain, originally designed as the foundation for Bitcoin, has emerged as a paradigm-shifting technology capable of transforming distributed systems. Its decentralized nature, cryptographic security, and transparency offer a compelling foundation for addressing the limitations of traditional smart home infrastructures.
This paper investigates the potential of blockchain to enhance the security, privacy, and autonomy of domotics systems. We begin by reviewing the current architecture of domotics systems and identifying vulnerabilities. We then explore blockchain fundamentals and how their integration with IoT can reshape smart home paradigms. Furthermore, we propose a blockchain-based framework for autonomous domotics and analyze existing literature, challenges, and future research avenues.

2. Background

2.1 Domotics Systems Overview

Domotics refers to the integration of home automation devices with digital control systems that manage home functions intelligently. Typical smart homes consist of:

- Sensors and actuators (motion detectors, cameras, smart locks, thermostats)
- Gateways (routers, hubs)
- Cloud platforms (Amazon Alexa, Google Home, Apple HomeKit)
- Mobile or web-based control interfaces

These systems often rely on centralized control logic and cloud infrastructure for data processing and decision-making. While convenient, this centralization raises concerns about:

- **Security**: Single points of failure, vulnerability to cyberattacks
- **Privacy**: Cloud providers may collect, analyze, and monetize user data
- **Autonomy**: Dependence on the internet and third-party services

2.2 Blockchain Fundamentals

Blockchain is a decentralized ledger technology (DLT) that records transactions in a verifiable and immutable manner. Key features include:

- **Decentralization**: Eliminates the need for a central authority
- **Immutability**: Once recorded, data cannot be altered retroactively
- **Transparency**: All network participants can verify transactions
- **Smart Contracts**: Self-executing programs triggered by predefined conditions

Blockchain networks can be public (e.g., Ethereum), private (e.g., Hyperledger Fabric), or consortium-based, each offering different trade-offs in scalability, control, and trust.

3. Motivations for Blockchain in Domotics

3.1 Privacy Enhancement

Current smart home platforms transmit sensitive data to centralized servers, potentially exposing personal routines and habits. A blockchain-based system can ensure data is encrypted, anonymized, and stored in a distributed manner, reducing risks of unauthorized surveillance or data misuse.

3.2 Security Reinforcement

Blockchain's cryptographic protocols can authenticate users, validate device identities, and prevent unauthorized commands. Immutable logs ensure accountability and traceability of all operations, aiding forensic analysis in case of breaches.

3.3 Autonomous Functionality

Smart contracts can automate decisions and enforce rules without external inputs, enabling smart homes to act independently and adaptively. For instance, a contract can manage energy consumption based on real-time pricing and occupancy without human intervention.

3.4 Trustless Ecosystem

Blockchain enables peer-to-peer interactions without intermediaries. Devices can transact securely and verify operations autonomously, fostering an ecosystem where trust is protocol-based rather than institution-based.

4. Proposed Architecture

We propose a layered architecture that integrates blockchain with domotics using smart contracts and edge computing. The architecture comprises:

4.1 Device Layer

Includes sensors, actuators, and controllers embedded within household appliances. These devices communicate via protocols like Zigbee, Z-Wave, or Wi-Fi.

4.2 Edge Layer

Edge nodes (e.g., smart hubs, Raspberry Pi) locally process data, reducing latency and preserving bandwidth. They serve as gateways to the blockchain network.

4.3 Blockchain Layer

This layer hosts:

- **Smart Contracts** for automating policies (e.g., security protocols, energy optimization)
- **Identity Management** using decentralized identifiers (DIDs)
- **Transaction Logs** for immutable event recording

A permissioned blockchain (e.g., Hyperledger) is preferred for its privacy controls and scalability.

4.4 Application Layer

User interfaces (mobile apps, dashboards) for monitoring and configuring home systems. Data visualization and alerts are handled here.

4.5 Communication Protocols

MQTT and HTTP enable device-to-gateway and gateway-to-blockchain communication. IPFS (InterPlanetary File System) may be used for decentralized file storage (e.g., security footage).

5. Use Cases

5.1 Secure Access Control

Smart locks and surveillance cameras register access events on the blockchain. Residents can grant and revoke access using blockchain credentials. Tampering attempts are logged immutably.

5.2 Energy Management

Smart meters and thermostats use smart contracts to optimize energy usage based on tariffs and occupancy patterns. Peer-to-peer energy trading among prosumers is facilitated through blockchain tokens.

5.3 Fault Detection and Maintenance

Sensors detect anomalies (e.g., gas leaks, water overflows) and trigger smart contracts to alert users or initiate emergency protocols. Maintenance records are stored on-chain for auditability.

6. Challenges and Limitations

Despite its potential, blockchain integration in domotics faces several hurdles:

6.1 Scalability
Blockchains like Ethereum suffer from limited throughput and high transaction fees. Layer-2 solutions (e.g., rollups) and private chains are viable alternatives.

6.2 Latency
Consensus mechanisms introduce latency, which may not be acceptable for real-time operations. Hybrid models combining on-chain and off-chain logic can alleviate this issue.

6.3 Resource Constraints
IoT devices have limited processing power and energy capacity, making it challenging to run full blockchain clients. Lightweight nodes or edge intermediaries are needed.

6.4 Interoperability
Lack of standardized interfaces between blockchain platforms and home automation protocols hinders seamless integration. Adoption of open standards is crucial.

6.5 Privacy Paradox
While blockchain provides transparency, it may also expose metadata. Techniques such as zk-SNARKs (zero-knowledge proofs) and confidential transactions can mitigate this.

7. Literature Review
Several studies have examined the convergence of blockchain and smart homes:

- Dorri *et al*. (2017) [1] proposed a lightweight blockchain framework for IoT security, highlighting its application in smart homes.
- Moinet *et al*. (2017) [2] suggested a blockchain-based reputation system for IoT devices.
- Novo (2018) [3] introduced a decentralized access control model using smart contracts for home automation.
- Ouaddah *et al*. (2020) [4] reviewed blockchain-based privacy-preserving mechanisms in domotics, emphasizing their effectiveness over traditional approaches.

While these contributions laid the groundwork, few address end-to-end autonomy, cross-device communication, or large-scale deployment.

8. Conceptual Model
We propose a model wherein:

1. Each IoT device has a unique DID anchored to the blockchain.
2. Smart contracts govern interactions (e.g., if motion is detected while residents are away, activate alarms and notify authorities).
3. Data is encrypted at the edge, selectively stored on-chain (metadata) and off-chain (bulk data).
4. Devices perform mutual authentication before communication.
5. A reputation system penalizes malfunctioning or misbehaving devices.

This model fosters a resilient, secure, and efficient smart home environment that operates with minimal human oversight.

9. Future Directions
Key areas for future research include:

- **Scalable Blockchain Protocols**: Exploring DAGs (Directed Acyclic Graphs), sharding, and consensus improvements for faster processing.
- **Quantum-Resistant Cryptography**: Preparing domotics systems for future cryptographic challenges.
- **Federated Learning on Blockchain**: Enabling collaborative AI training across smart homes while preserving data privacy.
- **Decentralized Marketplaces**: Allowing users to sell excess energy, computing power, or sensor data securely.
- **Policy and Regulation**: Developing legal frameworks for blockchain-based domotics, addressing liability and compliance.

10. Conclusion
Integrating blockchain with domotics systems presents a transformative approach to securing and automating smart homes. By decentralizing control, enhancing data integrity, and enabling trustless interactions, blockchain addresses critical vulnerabilities in current architectures. However, scalability, interoperability, and energy efficiency must be tackled to realize practical implementations. The future of smart homes lies in decentralized, intelligent ecosystems where devices not only respond but reason and act autonomously — all while safeguarding the user's privacy and trust.

11. References
1. Dorri A, Kanhere SS, Jurdak R. Blockchain in internet of things: challenges and solutions. arXiv [Preprint]. 2016 [cited 2025 Jul 7]. Available from: https://arxiv.org/abs/1608.05187
2. Moinet A, Darties B, Baril JL. Blockchain based trust & authentication for decentralized sensor networks. arXiv [Preprint]. 2017 [cited 2025 Jul 7]. Available from: https://arxiv.org/abs/1706.01730
3. Novo O. Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet of Things Journal. 2018;5(2):1184-1195.
4. Ouaddah A, Abou Elkalam A, Ait Ouahman A. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. International Journal of Advanced Computer Science and Applications. 2020;11(2).
5. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things. IEEE Access. 2016;4:2292-2303.
6. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data; 2017. p. 557-564.