AFQ-IoT: Adaptive, Federated, and Quantum-Resistant AI-Blockchain IoT Framework

Presented By

Shiva Shankar (2023202005)

shivashankar.gande@students.iiit.ac.in

Akshay Kohad (2023202007)

akshay.kohad@students.iiit.ac.in

Ashish Lakhmani (2023202008)

ashish.lakhmani@students.iiit.ac.in

International Institute of Information Technology,

Hyderabad

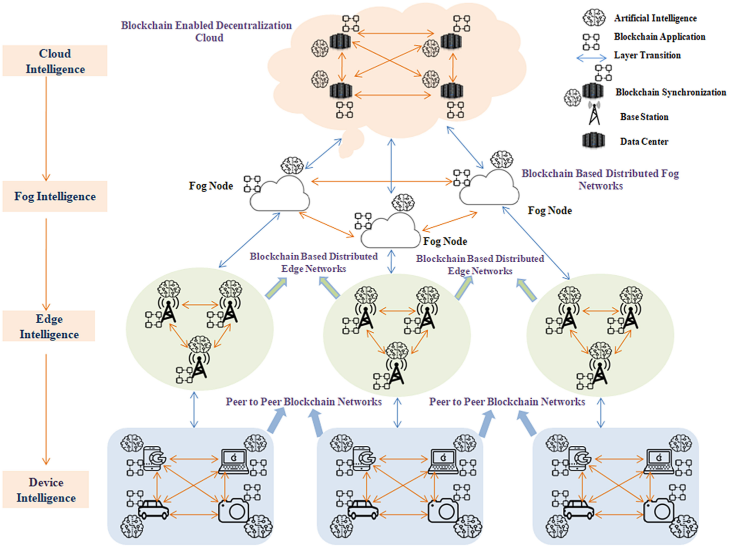
Outline

1. Introduction
   - Background
   - Network Model
   - Attack Model
   - Research Contribution
2. Literature Review
3. Summary of Techniques
4. Proposal
   - Motivation
   - Proposed Solution
5. Analysis
   - Security Analysis
   - Communication Analysis
   - Computation Analysis
6. Future Research Directions

Introduction: Background

- This paper discusses how the Internet of Things (IoT) connects various devices, such as smart homes and vehicles, to the internet, creating an interconnected network known as the Internet of Everything (IoE).
- While IoT is beneficial in improving productivity across multiple fields, it faces challenges like big data analytics, security, and centralization issues.
- To tackle these challenges, this paper suggests integrating both Artificial intelligence (AI) and Blockchain technology. IoT generates a huge mass of data, but AI assists in processing this data, and Blockchain offers secure and decentralized data storage. The aim of this collaboration is to establish a more secure, efficient, and scalable IoT framework, which is essential in addressing the existing challenges in data management and security.

Introduction: Network Model I


Cloud Intelligence
Fog Intelligence
Edge Intelligence
Device Intelligence
Blockchain Enabled Decentralization Cloud
Artificial Intelligence
Blockchain Application
Layer Transition
Blockchain Synchronization
Base Station
Data Center
Fog Node
Blockchain Based Distributed Fog Networks
Fog Node
Fog Node
Blockchain Based Distributed Edge Networks
Blockchain Based Distributed Edge Networks
Peer to Peer Blockchain Networks
Peer to Peer Blockchain Networks

Introduction: Network Model II

- **Device Intelligence: Role**: Data collection from IoT devices and sensors, **AI**: Local pre-processing and basic pattern recognition, **Blockchain**: Peer-to-peer security and privacy for direct device interactions.
- **Edge Intelligence: Role**: Initial data aggregation and processing from devices, **AI**: Feature extraction and data filtering close to the source, **Blockchain**: Secure, decentralized communication for efficient data handling at the edge.
- **Fog Intelligence: Role:** Intermediate layer for larger-scale data processing and decision-making, **AI:** Advanced data analysis and machine learning model training, **Blockchain:** Distributed ledger for secure, decentralized data management, addressing scalability.
- **Cloud Intelligence: Role:** Centralized, high-level data storage and analysis, **AI:** Intensive big data analysis in cloud data centers, **Blockchain:** Decentralized data storage for secure, scalable access and archival of IoT data.

Introduction: Attack Model

- **Data Breaches**: Blockchain’s cryptographic methods ensure data confidentiality, limiting access to authorized parties.
- **Malware and Unauthorized Access**: Blockchain’s immutable ledger logs all transactions, preventing data tampering and unauthorized modifications.
- **Data Tampering**: The decentralized consensus mechanism of Blockchain ensures any data changes are transparent and verifiable.
- **Centralization Vulnerabilities**: By decentralizing data storage, Blockchain reduces reliance on a single server, enhancing resilience against DDoS and single-point failures.

Introduction: Research Contribution

- Privacy-Preserving Federated Learning for IoT Devices
- Quantum-Resistant Cryptographic Security
- Adaptive Consensus Mechanism for Efficient Resource Utilization
- Cross-Chain Compatibility for Multi-Domain Interoperability
- Localized Blockchain and Distributed AI for Enhanced Edge Processing
- Federated Trust Mechanism for Secure Collaborative Anomaly Detection
- Energy-Efficient Quantized AI Models for Scalable Large-Scale Analysis

Literature Review I

- **Rathore et al. (2019):**
  Focus: Blockchain and deep learning (DL) integration for secure IoT.
  Contribution: Blockchain-secured DL model for data privacy and decentralized security.
  Limitation: Limited scope on Blockchain-AI integration for broader IoT applications.

- **Atlam et al. (2018):**
  Focus: AI-IoT integration for data security and analysis
  Contribution: Framework improving data privacy with AI in IoT.
  Limitation: Lacks emphasis on Blockchain's role.

- **Wright et al. (2018):**
  Focus: Integration of Blockchain and AI to address scalability and data processing in IoT.
  Contribution: Proposed a hybrid architecture using Blockchain's decentralized ledger and AI to optimize data flow and efficiency in IoT.
  Limitation: Limited focus on security and privacy; lacked application across multi-layered IoT architectures like fog and cloud.

Literature Review II

- **Qian et al. (2018):**
  Focus: IoT network security.
  Contribution: Blockchain-based network security for traffic monitoring and identity verification.
  Limitation: Minimal focus on AI.

- **Xu et al. (2017):**
  Focus: Decentralized IoT resource management.
  Contribution: Blockchain framework for efficient resource handling and scalability.
  Limitation: Limited exploration of AI for IoT data analysis.

- **Zheng et al. (2017):**
  Focus: Taxonomy of Blockchain technologies.
  Contribution: Classification of Blockchain types and consensus algorithms relevant to IoT.
  Limitation: No emphasis on AI-Blockchain integration for IoT.

Summary of Techniques

Research Work	Techniques Used	Advantages	Disadvantages
Rathore et al. (2019)	Blockchain + DL	Privacy, Decentralized Security	Limited IoT Integration
Atlam et al. (2018)	AI + IoT	Data Privacy, Analysis	Minimal Blockchain Focus
Xu et al. (2017)	Blockchain for Resource Management	Scalability, Efficiency	Limited AI Use
Qian et al. (2018)	Blockchain for Network Security	Identity Verification, Security	Minimal AI Application
Zheng et al. (2017)	Blockchain Taxonomy	Detailed Blockchain Overview	Lacks AI-IoT Focus
Wright et al. (2018)	Hybrid Blockchain + AI	Scalability, Data Flow	Limited Security, No Multi-layer IoT

Proposal: Motivation

In the following paper titled ”BlockIoTIntelligence: A Blockchain-enabled Intelligent Internet of Things Architecture Based on Artificial Intelligence” we will see a framework that integrates blockchain with AI to solve the critical IoT problems of centralization, security, and latency. That said, there are still challenges, especially regarding AI energy efficiency, interoperability, data management, and privacy. This shows us that we have to enhance the BlockIoTIntelligence model to indeed be flexible, sustainable and privacy delinquent to be feasible for broader use cases in the real IoT world. To tackle these issues, we propose an updated architecture, called AFQ-IoT with :

- Federated Learning for Privacy and Efficiency
- Adaptive AI-Driven Consensus Mechanism
- Cross-Chain Compatibility for Interoperability
- Quantum-Resistant Cryptography for Future-Proof Security
- Adaptive AI Models for Real-Time Decision Making

Proposal: Proposed Solution I

- **Federated Learning for Privacy and Efficiency**:
  Objective: Protect data privacy and reduce IoT network energy use.
  Approach: Train AI models locally on devices, sharing only model updates instead of raw data.
  Justification: Reduces data transfer and keeps sensitive info on devices, ideal for privacy-sensitive fields like healthcare.
- **Adaptive AI-Driven Consensus Mechanism**:
  Objective: To cut down on Blockchain for IoT energy consumption.
  Approach: Eliminate Proof of Work (PoW) and find less energy intensive methods like PoS and DPoS.
  Justification: Scales Blockchain for IoT's energy constrained environment, notably in case of massive networks.
- **Cross-Platform Interoperability**:
  Objective: Ensure Cross Ecosystem Integration of IoT Devices.
  Approach: Include basic compatible protocol and middleware (Zigbee, MQTT, LoRaWAN. etc.).
  Justification: It breaks down barriers between systems, allowing BlockIoTIntelligence to become more flexible and support more IoT devices.

Proposal: Proposed Solution II

- **Quantum-Resistant Cryptography for Long-Term Security**:
  Objective: Safeguard IoT data and transactions from future quantum-based threats.
  Approach: Use quantum-resistant algorithms, like lattice-based cryptography, within the blockchain.
  Justification: Traditional encryption could be broken by quantum computing. Quantum-resistant cryptography ensures lasting data security, essential for areas like finance and healthcare that need ongoing data protection.

- **Adaptive AI Models for Real-Time Decision Making** :
  Objective: To extend responsiveness and international decision making precision.
  Approach: Employ adaptive models such as reinforcement learning or transfer learning to rapidly adapt to incoming variations in data and network scenarios.
  Justification: Provides the ability to respond in real time, which is important in applications where you want to receive immediate insights (e.g., traffic or predictive maintenance).

Analysis: Security Analysis

- **Federated Learning for Privacy:**
  It enables local AI model training on IoT devices and shares only model updates which protect sensitive data and reduce privacy risks.
- **Adaptive AI-Driven Consensus:**
  Adjusts blockchain protocols based on network risk levels—switching to secure protocols like Proof-of-Stake (PoS) in high-risk situations and conserving resources with Proof-of-Authority (PoA) during low-risk times.
- **Cross-Chain Compatibility:**
  Facilitates secure data exchange across IoT domains, preventing data silos and enabling verified, authorized data sharing for sensitive, multi-domain applications.
- **Quantum-Resistant Blockchain:**
  Uses quantum-safe cryptography to secure IoT data against future quantum-based threats, ensuring long-term transaction security.
- **Quantum-Resistant Smart Contracts:**
  Enforces access control with quantum-safe smart contracts, securing data integrity and regulatory compliance by ensuring only authorized access to critical IoT data.

Analysis: Communication Analysis

- **Federated Learning and Reduced Data Transmission:**
  Federated Learning and Less Data Transmission Federated learning at the device level is leveraged to reduce the amount of data sent up to central nodes in the AFQ-IoT. It reduces the communication complexity by sending only model updates(sliced data) to upper layers rather than slice data. This design saves bandwidth and improves privacy.
- **Cross-Chain Protocols for Inter-Domain Communication:**
  With fog layer cross-chain compatibility enables secure sharing data across different IoT domains without creating any bottleneck. This decentralised method lessens the communication needs between layers through localised exchanges of data and thereby reduces the overall communication burden of the system.
- **Localized Blockchain for Efficient Data Verification:**
  he edge layer employs a localized blockchain, allowing data verification to happen mostly within the edge layer and minimizing data transfer to the cloud layer. The processing done here minimizes latency and instead of system to system which make it suitable for time require IoT applications and improves the response times.

Analysis: Computation Analysis

- **Quantized AI Models:**
  The cloud layer uses smaller, optimized AI models to process large IoT data quickly and with less computing power, essential for real-time, large-scale analysis.
- **Adaptive Consensus Mechanism:**
  It can alter the protocols of a blockchain based on its load. During low load periods, simpler protocols (PoA, etc.) are used and more complex protocols (PoS, etc.) during high load periods. This adaptive mechanism enables the crypto network to save energy and computational resources.
- **Distributed AI in Fog Layer:**
  It is responsible for local resource allocations on the devices which results in less bottleneck as devices will be able to share their workloads effectively, hence contributing to their overall functionality and for making them lesser dependent on centralized servers.
- **Quantum-Resistant Cryptography:**
  It selectively employs secure cryptography only at the device layer at the level of critical transactions while introducing minimal compute overhead and no degradation of performance.

Future Research Directions

- Development of Lightweight Quantum-Resistant Cryptographic Protocols
- Adaptive Federated Learning with Real-Time Model Update Mechanisms
- Integration of Edge AI for Enhanced Local Processing and Reduced Latency
- Exploration of Secure AI Model Aggregation Techniques
- Investigation of Self-Healing Mechanisms for IoT Networks

References I

1 S. Rathore, Y. Pan, J.H. Park, ”BlockDeepNet: A blockchain-based secure deep learning for IoT network,” *Sustainability*, vol. 11, 2019, p. 3974. http://dx.doi.org/10.3390/11143974.

2 H.F. Atlam, R.J. Walters, G.B. Wills, ”Intelligence of things: opportunities and challenges,” in *3rd Cloudification of the Internet of Things (CIoT)*, 2018, pp. 1–6. http://dx.doi.org/10.1109/CIOT.2018.8627114.

3 K.L. Wright, M. Espinoza, U. Chadha, B. Krishnamachari, ”SmartEdge: A smart contract for edge computing,” in *IEEE International Conference on Internet of Things (iThings), Green Computing and Communications (GreenCom), Cyber, Physical and Social Computing (CPSCom), Smart Data (SmartData)*, 2018. https://ieeexplore.ieee.org/document/8726601.

4 Z. Zheng, S. Xie, H.N. Dai, X. Chen, H. Wang, ”Blockchain challenges and opportunities: a survey,” *International Journal of Web Grid Services*, vol. 14, no. 4, 2018, pp. 352–375.

5 Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, M. Pustišek, ”Towards decentralized IoT security enhancement: A blockchain approach,” *Computers and Electrical Engineering*, vol. 72, 2018, pp. 266–273. https://www.sciencedirect.com/science/article/pii/S0045790618300508.

6 C. Xu, K. Wang, M. Guo, ”Intelligent resource management in blockchain-based cloud datacenters,” *IEEE Cloud Computing*, vol. 4, no. 6, 2017, pp. 50–59. http://dx.doi.org/10.1109/MCC.2018.1081060.

Thank you very much!