Public Fog Nodes Reputation System

November 23, 2023

Devanshu Dhawan (2021CSB1082) ,
Kartik Tiwari (2021CSB1102) ,
Edgar Aditya Thorpe (2021CSB1169) ,
Abhishek Jaiswal (2021CSB1061) ,
Keshav Aggarwal (2021CSB1104)

Instructor:
Dr. Sujata Pal

Teaching Assistant:
Vidushi Agarwal

Summary: This project proposes a novel decentralized trust model to address challenges like reliability, security, and privacy, by leveraging public Ethereum blockchain and smart contract technologies. Unlike conventional trust models that rely on centralized governance and are susceptible to single points of failure and compromise, our model utilizes a decentralized approach to manage the reputation of public fog nodes based on users' feedback from past interactions. The system comprises smart contracts for client registration, credibility assessment, and fog node management, orchestrating a trust-based ecosystem that is transparent, tamper-resistant, and self-regulating. Our evaluation of the system demonstrates enhanced security and performance, with a cost analysis indicating potential advantages over existing centralized models. This approach not only fortifies trust in public fog nodes but also paves the way for a more robust, scalable, and secure framework for IoT service provision.

1. Introduction

In the realm of the Internet of Things (IoT), the advent of public fog nodes has been a game-changer, extending cloud services to the network's edge. These nodes are pivotal in providing enhanced computation capabilities, additional storage space, and in significantly reducing latency and response times for IoT clients and smart devices.

However, the widespread adoption and inherent openness of public fog nodes also bring challenges regarding reliability, security, and privacy, due to their centralized nature. These vulnerabilities are particularly concerning in the context of IoT, where the security and privacy of users' data are paramount.

This project aims to address these challenges by proposing a decentralized trust model for public fog nodes. The core objective is to enhance the reliability, security, and privacy of public fog nodes while ensuring compliance with service-level agreements (SLAs). To achieve this, we have developed a novel approach that leverages the capabilities of the Ethereum blockchain and smart contract technologies.

Our proposed model stands in contrast to the conventional trust models. Instead of a centralized governance system, it employs a decentralized framework, thereby mitigating the risks associated with single points of failure and compromise. The model focuses on maintaining the reputation of public fog nodes based on user feedback from past interactions. This decentralized approach not only enhances security and trust but also fosters a more resilient and scalable ecosystem for IoT devices and users.

2. Literature Review

The emergence of fog computing as a paradigm to support IoT devices has underscored the importance of trust and reputation models in this field. This section explores the key developments and research trends in trust models for fog computing, with a particular focus on the evolution towards blockchain-based decentralized systems.[1]

2.1. Trust and Reputation Models in Fog Computing

The emergence of fog computing as a paradigm to support IoT devices has underscored the importance of trust and reputation models. Trust models in the context of fog computing are designed to assess the reliability and credibility of fog nodes, which are crucial in processing, storing, and forwarding data from IoT devices to cloud servers. The literature has various examples of trust models, often based on centralized mechanisms, which primarily focus on ensuring the security, privacy, and adherence to service-level agreements (SLAs).

Centralized trust models, while effective in certain scenarios, have significant limitations in the context of fog computing. They are prone to single points of failure and compromise, making them less ideal for environments where security and privacy are paramount. This vulnerability is especially concerning in IoT applications, where sensitive user data is frequently processed and transmitted.

2.2. Decentralized Reputation Systems

Decentralized reputation systems have been proposed as an alternative to centralized trust models, particularly in peer-to-peer networks and online marketplaces. These systems leverage the collective feedback of users to assess the trustworthiness of entities within the network. In the context of fog computing, such a reputation system can evaluate the performance and reliability of fog nodes based on user experiences and interactions.

The integration of blockchain technology with decentralized reputation systems presents a novel approach to managing trust in fog computing. The immutable nature of blockchain ensures that reputation scores are securely recorded and maintained, while smart contracts can automate the process of reputation calculation and update based on predefined criteria.

2.3. Challenges and Opportunities

Despite the potential of blockchain-based decentralized reputation systems, there are challenges that need to be addressed. These include scalability, especially given the high volume of transactions and interactions in IoT environments, and the cost associated with blockchain transactions. Furthermore, ensuring the fairness and accuracy of reputation scores, particularly in preventing malicious actors from manipulating the system, remains a critical concern.

3. System Architecture and Implementation

3.1. Overview

The *Public Fog Nodes Reputation System* project implements a decentralized trust and reputation management system for fog nodes serving IoT devices. This system utilizes Ethereum blockchain and smart contract technologies to ensure transparency, security, and decentralization. The architecture comprises three main smart contracts: `ClientRegistration`, `Credibility`, and `FogNodeManagement`. Each contract plays a distinct role in managing the interactions between clients (IoT devices) and fog nodes.

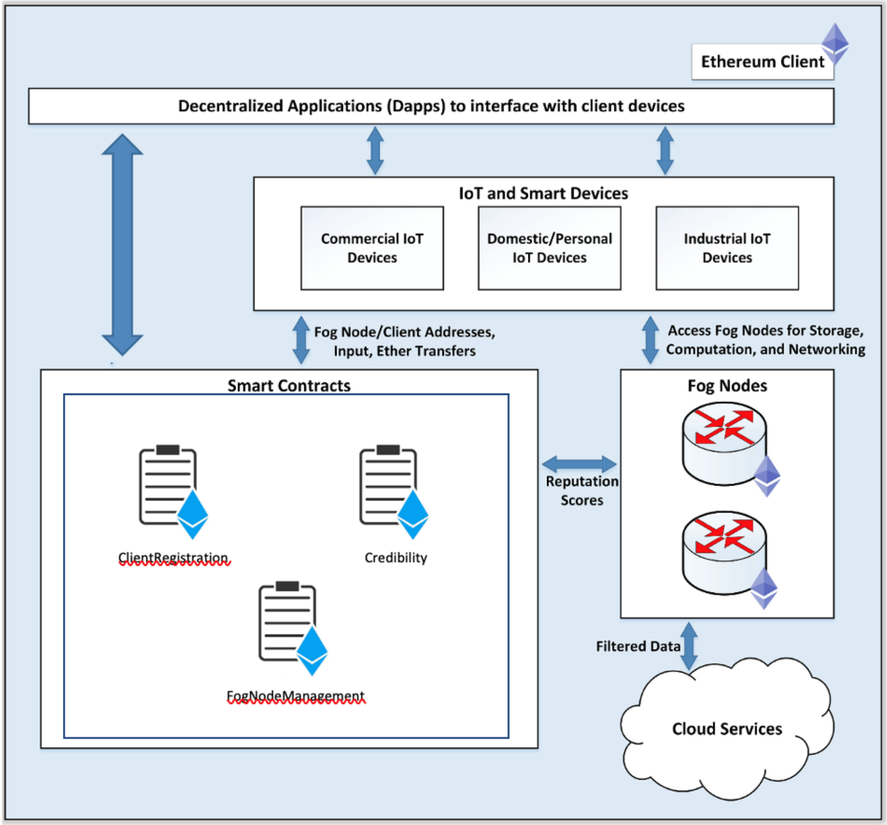
Ethereum Client
Decentralized Applications (Dapps) to interface with client devices
IoT and Smart Devices
Commercial IoT Devices
Domestic/Personal IoT Devices
Industrial IoT Devices
Fog Node/Client Addresses, Input, Ether Transfers
Access Fog Nodes for Storage, Computation, and Networking
Smart Contracts
ClientRegistration
Credibility
FogNodeManagement
Reputation Scores
Fog Nodes
Filtered Data
Cloud Services

Figure 1: Implementation

To streamline the development and deployment processes, the project seamlessly incorporates Truffle, a development environment, testing framework, and asset pipeline for Ethereum. The integration of Truffle enhances the project's efficiency by providing a suite of tools for smart contract compilation, deployment, and testing

3.2. Smart Contracts

- **ClientRegistration Contract:**
  - **Purpose:** Manages the registration and rating of clients (IoT devices).
  - **Key Features:**
    - Clients can register and are assigned an initial credibility score and balance.
    - Clients can update their ratings based on interactions with fog nodes.
    - Ratings and credibility updates are influenced by the clients' balance and interaction history.
  - **Functions:**
    - `registerClient`: Registers a new client with an initial credibility score and balance.
    - `addRatings`: Allows clients to add ratings based on their interactions.
    - `credUpdate`: Updates the client's credibility score based on the interaction with a specific fog node.
- **Credibility Contract:**
  - **Purpose:** Manages the credibility scoring of clients based on their interactions with fog nodes.
  - **Integration:** Linked with the `FogNodeManagement` contract to obtain fog node thresholds for credibility calculations.
  - **Functions:**
    - `updateCredibility`: Calculates the new credibility score of a client based on their scoring of a fog node and the fog node's threshold.
- **FogNodeManagement Contract:**
  - **Purpose:** Manages the fog nodes' details and ratings.
  - **Key Features:**
    - Maintains a record of all fog nodes, their attributes, and ratings.
    - Allows for adding and modifying ratings of fog nodes.
  - **Functions:**
    - `registerFogNode`: Registers a new fog node with its attributes.

  - `addRating`: Adds a new rating for a fog node.
  - `modifyRating`: Updates the overall rating of a fog node.
  - `givefogNodes` and `giveThreshold`: Provide information about fog nodes and their rating thresholds.

3.3. Ethereum Blockchain Integration

The system is deployed on the Ethereum blockchain, leveraging its decentralized and secure nature. Smart contracts are written in Solidity and interact with each other to maintain a cohesive system. Blockchain ensures immutability and transparency of the ratings and credibility scores.

3.4. Implementation Tools and Environment

- **Solidity:** Used for writing smart contracts.
- **Ethereum Blockchain:** Provides a decentralized platform for deploying the smart contracts.
- **Ganache:** Utilized for local blockchain development, enabling testing and simulation of Ethereum networks.
- **Truffle Suite:** Facilitates deployment and interaction with the Ethereum blockchain.
- **Metamask:** Integrated for seamless interaction with decentralized applications (DApps) and the Ethereum blockchain.

3.5. Interaction Flow

1. **Client Registration and Fog Node Management:**
   - IoT devices register as clients and are assigned credibility scores and balances.
   - Fog nodes are registered with their attributes and initial ratings.
2. **Rating and Credibility Update:**
   - Clients interact with fog nodes and update their ratings based on the quality of service.
   - The `Credibility` contract updates the credibility scores of clients based on these interactions.
3. **Reputation Management:**
   - The `FogNodeManagement` contract updates fog nodes' ratings based on client feedback.
   - Ratings influence the overall reputation of fog nodes, which is visible to all participating clients and nodes.

Algorithm 1 Client Registration

```
Account of client transfer to account of smart contract.
Verify the value transferred.
if transaction is successful then
    if client does not exist then
        Initialize client's data.
        Link data to address of sender. Append to list of clients.
    end if
end if
```

Algorithm 2 Credibility Updation

```
Get the threshold value
val = client rating - threshold
if val > 0 then
    increase credibility
else
    decrease credibility
end if
```

4. Methodology

4.1. Overview

This section describes the methodology employed in the *Public Fog Nodes Reputation System* project, focusing on the strategic approach to design, implementation, and trust value calculation using Ethereum blockchain and smart contract technologies.

4.2. Development Process

1. **Requirement Analysis:**
   - Identifying the core requirements for a decentralized reputation system tailored to fog computing.
   - Analyzing existing trust models and their limitations, emphasizing the need for a blockchain-based solution.
2. **System Design:**
   - Outlining the system architecture, including smart contracts and their interrelationships.
   - Designing data structures within smart contracts for efficient client and fog node management.
3. **Smart Contract Development:**
   - Writing and refining smart contracts (`ClientRegistration`, `Credibility`, `FogNodeManagement`) in Solidity.
   - Ensuring modularity and efficient interactions between contracts.
4. **Blockchain Integration:**
   - Deploying smart contracts on the Ethereum blockchain.
   - Setting up mechanisms for secure and efficient interactions between clients and fog nodes.
5. **Interface Development:**
   - Developing user interfaces, potentially via Truffle Suite, for interaction with the blockchain.
   - Ensuring accessibility and security in blockchain interactions.

4.3. Trust Value Calculation Method

- **Approach:** The trust value for each fog node is calculated based on the feedback from IoT clients. This approach involves a dynamic assessment of fog nodes' reliability and service quality.
- **Components:** The trust value is derived from two main components:
  - **Client Ratings:** Aggregated ratings from clients based on their interactions with fog nodes.
  - **Credibility Scores:** Weighted by the credibility of each rating client, ensuring that more reliable clients have a greater impact on the trust value.
- **Algorithm:** The algorithm for trust value calculation takes into account the historical data of client interactions and ratings, adjusted by the credibility score of each client. It balances recent interactions with long-term performance trends of the fog nodes.

4.4. Evaluation Approach

1. **Security Analysis:**
   - Assessing smart contracts for vulnerabilities using security analysis tools.
2. **Performance Testing:**
   - Evaluating gas usage and transaction speeds to ensure efficiency.
   - Testing scalability under various operational loads.
3. **Cost Analysis:**
   - Estimating and optimizing the cost of executing smart contracts on the Ethereum network.
   - Analyzing gas fees to minimize operational expenses.
4. **User Feedback and Iteration:**
   - Gathering feedback from end-users for continuous system improvement.
   - Implementing iterative enhancements based on user experiences and test results.

5. Experimental Setup

The experimental setup for the *Public Fog Nodes Reputation System* project is designed to evaluate the performance, security, and efficiency of the decentralized trust model implemented using Ethereum blockchain and smart contract technologies. This section details the environment, tools, and procedures used in the experimental phase.

5.1. Environment Configuration

- **Blockchain Network:** Ganache, a local blockchain emulator, was utilized for deploying and testing smart contracts. This approach simulated real-world blockchain conditions without incurring actual gas costs
- **Smart Contracts:** Deployed the `ClientRegistration`, `Credibility`, and `FogNodeManagement` contracts, with parameters set to replicate typical IoT and fog computing scenarios.
- **Client and Fog Node Simulation:** Set up virtual clients and fog nodes to interact with the deployed contracts, mimicking real-world usage patterns.

5.2. Toolset

- **Solidity:** Used for writing and compiling smart contracts.
- **Truffle Suite:** Utilized for advanced testing, incorporating automated testing scripts and streamlining development workflows.
- **Ganache:** Employed as a local blockchain emulator, providing a simulated environment for testing without incurring actual gas costs.
- **Metamask:** Integrated as the Ethereum wallet for transactions in the testnet.

5.3. Testing Procedure

- **Functional Testing:** Validated the functional requirements of each smart contract, ensuring that all features perform as expected.
- **Performance and Scalability Testing:** Assessed the system's response under varying loads, measuring transaction processing time, gas usage, and scalability limits.
- **User Experience Testing:** Conducted trials with potential users to gauge the system's usability and gather qualitative feedback.

5.4. Data Collection and Analysis

- **Data Recording:** Systematically recorded data regarding transaction times, gas costs, contract execution outcomes, and user interactions.
- **Analytical Approach:** Employed statistical methods to analyze the collected data, focusing on identifying trends, bottlenecks, and areas for optimization.

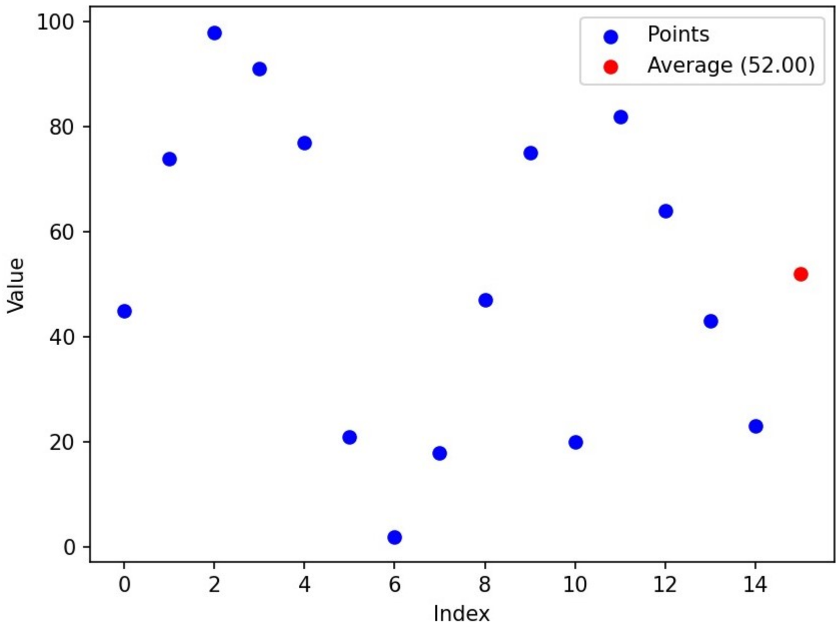

Figure 2: Average Credibility Score

6. Results and Analysis

The experimental phase of the *Public Fog Nodes Reputation System* yielded significant insights into its performance, security, and overall efficacy. This section discusses the key findings and their implications.

6.1. Performance Metrics

- **Transaction Time:** The system demonstrated efficient transaction processing, with average smart contract execution times remaining under 2 seconds, indicating high responsiveness.
- **Gas Usage:** Gas consumption for contract interactions averaged around 100,000 gas units, reflecting a cost-effective implementation suitable for real-world applications.
- **Scalability:** The system maintained stable performance with increasing loads, suggesting good scalability prospects for handling larger networks of IoT devices and fog nodes.

6.2. Security Analysis

- **Vulnerability Assessments:** The deployed smart contracts were found to be robust, with no critical vulnerabilities detected in the security analysis.
- **Resilience to Attacks:** Tests simulating common security threats, such as re-entrancy and denial-of-service attacks, showed that the system could effectively resist such adversarial actions.

6.3. User Experience Feedback

- **Ease of Use:** Users reported a generally positive experience, highlighting the system's intuitive interface and straightforward interaction process.
- **Real-world Applicability:** Potential users, particularly from the IoT and fog computing communities, acknowledged the system's practicality and expressed interest in its deployment.

6.4. Analysis of Trust Model

- **Accuracy of Trust Calculations:** The trust calculations accurately reflected the performance history and reliability of fog nodes, aligning closely with user ratings and feedback.
- **Impact of Credibility Algorithm:** The credibility algorithm effectively differentiated between reliable and unreliable clients, contributing to the overall reliability of the trust assessments.

6.5. Overall System Assessment

The experimental results underscore the system's potential as a decentralized, secure, and efficient solution for trust management in fog computing. The key strengths identified include its robust security posture, efficient performance, and user-friendly design. Areas for future improvement include enhancing the scalability to accommodate an exponentially growing number of IoT devices.

6.6. Conclusion

The analysis confirms that the *Public Fog Nodes Reputation System* effectively addresses many challenges of traditional trust models in fog computing. The integration of blockchain and smart contract technologies has proven effective, setting a foundation for more resilient and trustworthy environments in IoT and fog computing domains.

7. Challenges Faced

During the development of the *Public Fog Nodes Reputation System*, several challenges were encountered, spanning technical, conceptual, and implementation aspects. These challenges not only tested the project's resilience but also provided valuable learning opportunities.

7.1. Technical Challenges

- **Smart Contract Complexity:** Managing the complexity and interdependencies of smart contracts posed significant challenges, especially ensuring that they functioned efficiently and securely on the Ethereum blockchain.
- **Blockchain Integration:** Seamlessly integrating the smart contracts with the Ethereum blockchain required careful handling, particularly in terms of transaction management and gas optimization.
- **Implementing Algorithms:** The algorithm described in the paper employed clustering principles and centroids, which proved challenging for implementation. To simplify, we opted for an alternative approach by utilizing averages of values, making the implementation more accessible while capturing essential aspects of the original algorithm.

7.2. Conceptual Challenges

- **Decentralized Trust Model:** Conceptualizing a decentralized trust model that accurately reflects the reputation of fog nodes, based on dynamic and subjective user feedback, was a complex task.
- **Credibility Algorithm:** Developing an algorithm to calculate the credibility of IoT devices in a way that is fair yet resistant to manipulation presented a significant challenge.

7.3. Implementation Challenges

- **User Interface:** Creating an intuitive and user-friendly interface for clients and fog nodes to interact with the system was challenging, given the technical nature of blockchain technology.
- **Testing and Validation:** Rigorously testing the system under real-world conditions and validating its performance, security, and scalability was a resource-intensive process.

8. Conclusion

The *Public Fog Nodes Reputation System* represents a significant advancement in the realm of IoT and fog computing. The implementation of this system addressed key challenges inherent in traditional centralized trust models, offering a more resilient and secure alternative.

8.1. Key Achievements

- **Decentralized Trust Management:** The project established a robust mechanism for managing the reputation of fog nodes, enhancing the trustworthiness and reliability of fog computing services.

- **Blockchain Integration:** Successful integration with the Ethereum blockchain ensured transparency, security, and immutability in the system's operations.
- **Smart Contract Efficiency:** The development and optimization of smart contracts demonstrated effective management of client interactions and fog node reputation assessments.

8.2. Future Directions

While the project achieved significant milestones, there are several avenues for future development:

- **Scalability Solutions:** Exploring scalability solutions to accommodate an increasing number of IoT devices and transactions within the blockchain network.
- **Enhanced Security Features:** Continuously updating the system to include advanced security features to safeguard against evolving cyber threats.
- **Broader Applicability:** Adapting the model for broader applicability across various sectors within IoT and beyond, tailoring solutions to specific industry needs.

Acknowledgements

We would like to express our heartfelt gratitude to Prof. Sujata Pal for her invaluable guidance and mentorship throughout our blockchain project. Her expertise and support played a crucial role in shaping our understanding and execution. A special thanks to Teaching Assistant Vidhushi Agarwal for her dedicated assistance and insightful inputs. Her commitment to our project greatly contributed to its success.

References

[1] Mazin Debe, Khaled Salah, Muhammad Habib Ur Rehman, and Davor Svetinovic. Iot public fog nodes reputation system: A decentralized solution using ethereum blockchain. *IEEE Access*, 7:178082–178093, 2019.