مجلة

كلية التـــراث الجامعة

مجلة علمية محكمة

متعددة التخصصات نصف سنوية

العدد التاسع والثلاثون

عدد خاص بوقائع المؤتمر العلمي السنوي السادس عشر (الدولي الخامس)

18 نيسان 2024

ISSN 2074-5621

رقم الايداع في دار الكتب والوثائق 719 لسنة 2011

مجلة كلية التراث الجامعة معترف بها من قبل وزارة التعليم العالي والبحث العلمي بكتابها المرقم (ب 3059/4) والمؤرخ في (4/7 /2014)

Reliable Data Forwarding Mechanism in Fog Computing By Using MQTT and TLS for the Internet of Things

FATIMAH MOHAMMED HAMEED HAMEED SEFER KURNAZ

Electrical and computer Engineering Department, Altinbash University. Istanbul. Turkey

Abstract

As the Internet of Things (IoT) expands, the need for efficient and secure data processing at the network edge has surged. Fog computing, which extends cloud services to the network's edge, addresses these needs. This paper introduces a mechanism that ensures trustworthy data forwarding within the MQTT protocol, widely used in IoT. The mechanism integrates fog computing resources into MQTT, improving data reliability and security. It uses trust models to assess the credibility of devices and nodes involved in forwarding, and incorporates secure communication protocols (TLS/SSL, MQTTS, PKI) and data integrity methods (MAC, digital signatures). These features ensure secure and trustworthy IoT data transmission, while maintaining low latency and efficient resource use.

Keywords: fog computing, MQTT, trustworthy forwarding scheme, Internet of Things (IoT), edge computing, data reliability, data security, secure communication, authentication, Level of Trust (LoT)

1. Introduction

The introduction highlights the growing demand for real- time data processing in IoT applications and the role of fog computing in reducing latency and conserving bandwidth by processing data closer to the source as mentioned in [1]. However, the integration of MQTT for efficient data transfer lacks inherent security, which poses risks to IoT networks. To enhance security, TLS is combined with MQTT to ensure encrypted and authenticated data transmission as mentioned in [2]. This paper proposes a secure, flexible data-forwarding mechanism within fog computing that supports both partial and full forwarding, allowing for selective data processing based on application requirements as mentioned in [3]. Key contributions include a secure data-forwarding scheme, a trust model to validate data authenticity, and empirical results showing improvements in latency and network performance as mentioned in [4]. The study offers a scalable framework that enhances security and efficiency in IoT systems, positioning fog computing with MQTT and TLS as a robust solution for future IoT applications

1.1. Research Problem

- **IoT Growth**: As IoT expands, it generates vast amounts of data that need to be processed efficiently and securely.
- **Challenges in Transmission**: Ensuring low-latency, secure, and reliable data transmission, particularly in real-time applications like smart cities, is a major challenge.
- **Cloud Limitations**: Traditional cloud models face latency and bandwidth issues, making them unsuitable for real-time data processing.
- **Security Issues**: IoT devices are prone to security threats, raising concerns over data privacy, and integrity.
- **Fog Computing Limitations**: Existing fog computing lacks mechanisms for secure, reliable data forwarding, leading to performance issues.

1.2. Research Objective

- Primary Objective: To develop a secure and efficient mechanism for fog computing-assisted functions based on trustworthy data forwarding in IoT systems.
- Secondary Objectives:

1. Enhance data transmission reliability and security through MQTT with TLS and encryption in a fog computing environment.
2. Minimize latency and optimize resource utilization while evaluating system performance using simulations and real-time datasets.

2. Literature Review

The literature review emphasizes fog computing's critical role in overcoming the shortcomings of traditional cloud models, particularly in managing latency and bandwidth constraints in IoT systems as mentioned in [5]. It explores the prevalent security challenges in IoT devices, which often face weaknesses due to their limited resources [6]. While encryption and authentication methods have been suggested, there is a notable gap in integrating trust models for ensuring secure data forwarding as mentioned in [7].

future research should prioritize optimizing energy utilization and enhancing the reliability of smart grid systems as mentioned in [8]. Additionally, examining the socio-economic impacts on consumer behavior regarding energy management will be vital for developing effective engagement strategies that encourage the adoption of smart grid technologies. Atlam et al. (2018) and Mouradian et al. (2017) emphasizing localized data processing for real-time applications. MQTT is efficient for IoT communication but requires TLS for security (Sethi & Sarangi, 2017). Trust models improve data reliability in fog networks (Zhao & Lin, 2020), and flexible forwarding optimizes resources (Singh & Choi, 2021). Li et al. further detail data forwarding models in IoT, underscoring advancements needed for efficient data handling in fog computing environments [9] . The review concludes by pointing out that existing research fails to deliver a unified solution that integrates fog computing, MQTT, TLS, and trust models for secure, low-latency IoT data transmission[10]. This thesis will address these gaps by proposing such a mechanism, focusing on reliability and efficient resource use in real-time IoT applications[11].

3. Methodology

3.1. Data Used

- The Edge-IIoTset is a new cybersecurity dataset for IoT and IIoT applications, designed to detect intrusions using machine learning in both centralized and federated learning modes. The dataset is structured across seven layers:
- **Cloud Computing Layer**: Manages large-scale data storage and processing.
- **Fog Computing Layer**: Reduces latency by processing data closer to the network edge.
- **NFV Layer**: Virtualizes network services for flexibility.
- **Blockchain Layer**: Provides secure, tamper-proof data transactions.
- **SDN Layer**: Centralizes network control for efficiency.
- **Edge Computing Layer**: Enables real-time data processing at the device level.
- **IoT and IIoT Perception Layer**: Gathers data from IoT devices and sensors.
- The dataset includes data from over 10 IoT devices, covering 14 types of attacks such as DoS and malware, grouped into five categories, and evaluates machine learning for intrusion detection.

3.2. Proposed Model

3.2.1 MQTT Deployment in Fog Nodes:

- **MQTT Brokers**: Deployed within fog nodes, edge devices, and sometimes in the cloud to facilitate communication between IoT devices, fog, and cloud layers.
- **Publish–Subscribe Model**: IoT devices act as publishers, sending data to MQTT topics. Fog nodes or other devices act as subscribers, receiving and processing the data.

3.2.2 Task Offloading Mechanism:

- **Dynamic Task Offloading**: The system dynamically decides whether to process tasks locally or offload them based on factors like queue length and processing capacity.
- **Evaluation of Queue Length**: If the queue at the local fog node is manageable, the task is processed locally. Otherwise, it is forwarded to other nodes or the cloud.

3.2.3 Task Offloading Process: .

- **Local Processing**: If the task queue is below the threshold, the task is processed at the fog node.
- **Offloading Decision**: If the queue exceeds the threshold, the system calculates processing delay (PD) and queue length (T_queue) at other fog nodes or the cloud.The task is offloaded to the node with the least processing delay and acceptable queue length.
- **Cloud Offloading**: If transmission delay to the cloud is shorter than the processing delay at fog nodes, the task is sent to the cloud for processing.

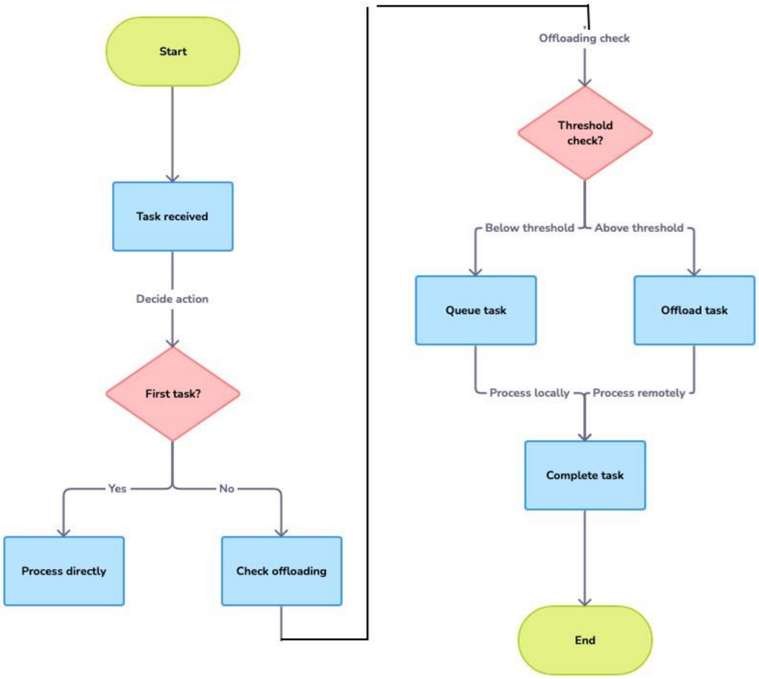


Figure 1: Flowchart of the process followed for this research work.

This flowchart shows how tasks are managed based on queue time. If the queue time is below a set threshold, tasks are processed locally; otherwise, they are offloaded for remote processing. The system optimizes task handling by balancing local and remote processing to improve efficiency, as show Figure 1.

3.2.4 Data Flow Management:

- **Optimized Data Flow**: The lightweight nature of MQTT makes it ideal for **real- time IoT data processing** in fog environments, where devices can publish sensor data efficiently without overloading the system.
- **Data Preprocessing and Filtering**: At the fog node, initial data filtering, compression, or basic analysis is performed. This reduces the amount of data that needs to be forwarded to the cloud, minimizing **bandwidth consumption**.
- **Load Balancing**: Multiple fog nodes ensure **load distribution** by using MQTT's **message queuing**. The system distributes tasks evenly to avoid any single node becoming a bottleneck, enhancing both performance and availability.

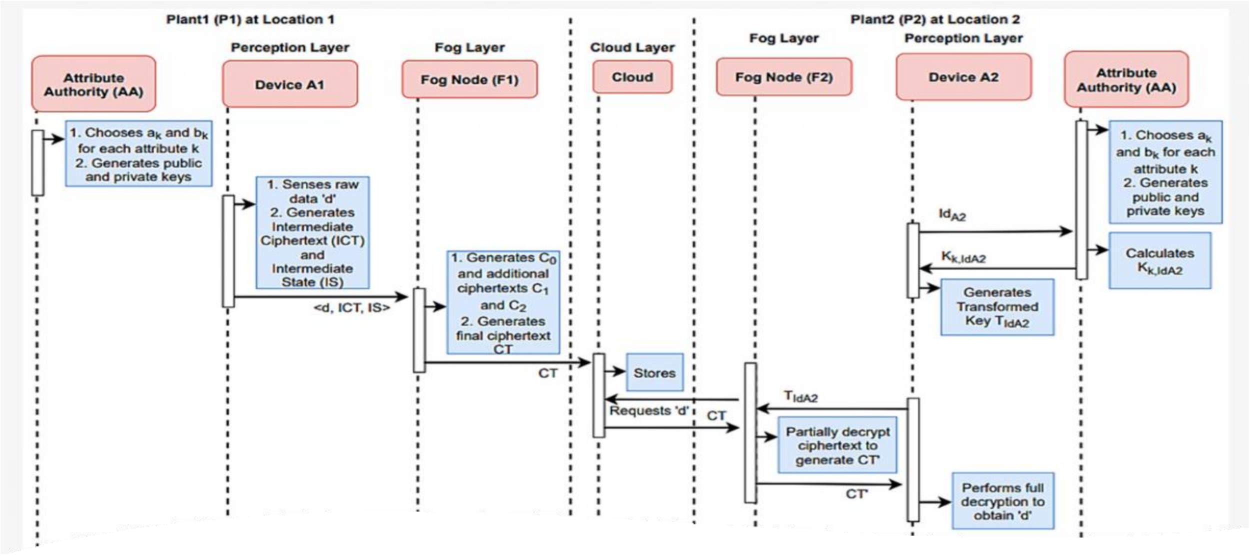

Plant1 (P1) at Location 1
Perception Layer
Fog Layer
Cloud Layer
Fog Layer
Plant2 (P2) at Location 2
Perception Layer
Attribute Authority (AA)
Device A1
Fog Node (F1)
Cloud
Fog Node (F2)
Device A2
Attribute Authority (AA)
1. Chooses a_k and b_k for each attribute k 2. Generates public and private keys
1. Senses raw data 'd' 2. Generates Intermediate Ciphertext (ICT) and Intermediate State (IS)
<d, ICT, IS>
1. Generates C_0 and additional ciphertexts C_1 and C_2 2. Generates final ciphertext CT
CT
Stores
Requests 'd'
CT
Id_{A2}
1. Chooses a_k and b_k for each attribute k 2. Generates public and private keys
$K_{k,IdA2}$
Calculates $K_{k,IdA2}$
Generates Transformed Key T_{IdA2}
T_{IdA2}
Partially decrypt ciphertext to generate CT'
CT'
Performs full decryption to obtain 'd'

Figure 2: A complete sequence diagram of the proposed partial forwarding access control scheme with improved performance.

The figure illustrates a data flow process starting from the Perception Layer, where Device A1 collects and encrypts raw data to produce intermediate ciphertext (ICT). The data is sent to Fog Node F1, which applies additional encryption and generates the final ciphertext (CT). The CT is stored in the cloud until requested by another device. At the second location (Plant2), a Transformed Key is used for partial decryption, followed by full decryption to retrieve the original data. This method reduces cloud dependence, enhances system efficiency, and secures data transmission, as show Figure 2.

4.Results

- Trustworthiness of data forwarding was significantly enhanced by incorporating dynamic trust models into the MQTT-based system.
- Improved data security was achieved through encryption and integrity verification within MQTT, ensuring data confidentiality and integrity.
- Network performance was optimized, reducing latency and enhancing resource utilization, especially for real-time IoT applications.
- The mechanism demonstrated resource efficiency, minimizing overhead while maintaining data reliability and security.
- The solution provides robust IoT data forwarding, enhancing overall system performance and reliability.

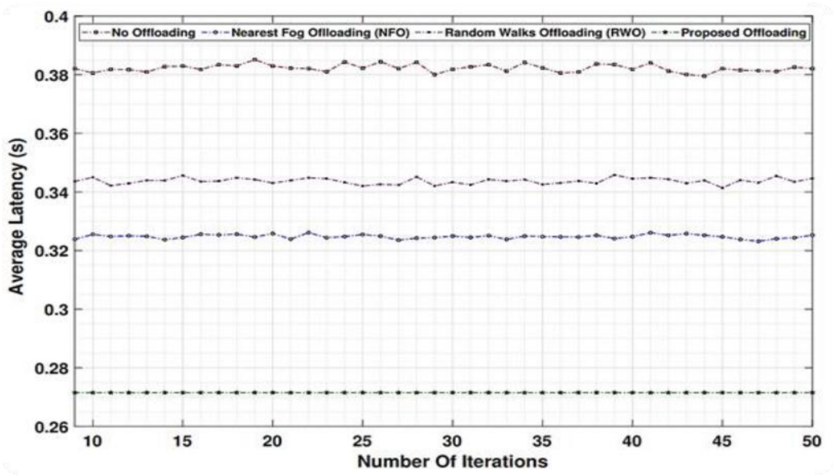
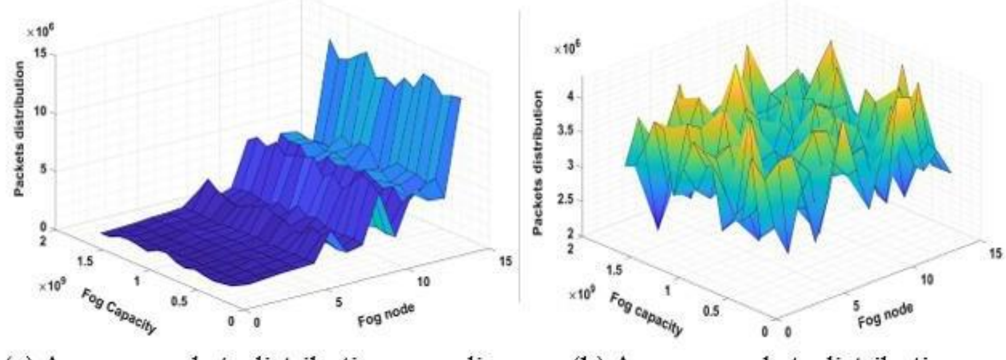


Figure 3: Average Latency for MQTT and TLS in Fog Network with Mixed Packet Types

The chart compares average latency for different offloading strategies in fog computing. The **proposed offloading** strategy shows the lowest latency, around **0.26-0.28 seconds**, outperforming **no offloading** (0.38s), **nearest fog offloading** (0.36s), and **random walks offloading** (0.34s). This demonstrates the **proposed method's superior efficiency** for real-time data processing in IoT environments,as show figure 3.



(a) Average packets distribution according to MQTT

(b) Average packets distribution according to MQTT and TLS

Figure 4: Packets distribution for trustworthy nodes in fog network

The first chart shows the basic packet distribution using the MQTT protocol only, while the second chart highlights the effect of adding the TLS protocol, which improves packet distribution and secures data.The second chart provides a more secure and stable system for data transmission, which is crucial for ensuring the integrity and reliability of data transfer in IoT environments.

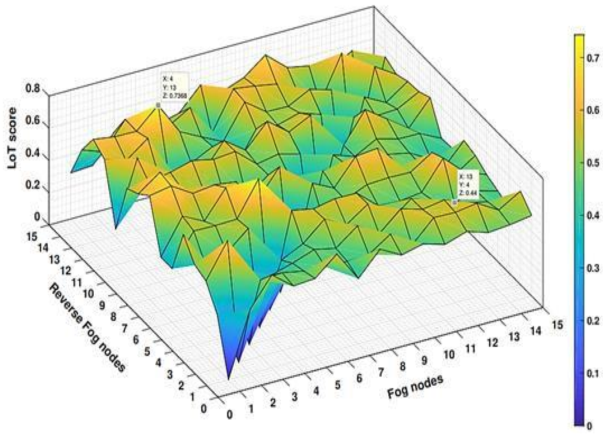


Figure 4: Forwarding Process Stability with 15 Fog Nodes Showing Trust Asymmetry at Level of Trust (LoT).

The 3D plot shows the distribution of Level of Trust (LoT) scores across various fog nodes in a fog computing network. Higher LoT scores are represented in yellow, while lower scores are in blue, indicating trust variations among the nodes. This helps identify the most reliable nodes for secure data forwarding, as show figure 4.

5.Comparison

In comparison, the Trustworthiness-Enhanced Reliable Forwarding (TERF) scheme improves data reliability with a 93.49% accuracy but faces limitations in scalability and security. The Wireless Sensor Networks (WSNs) scheme achieves higher accuracy at 96.29%, optimizing efficiency but lacking comprehensive security measures. The Proposed MQTT and TLS- Based Forwarding Scheme, with a 97.63% accuracy, integrates efficient MQTT communication and strong TLS encryption, offering a scalable, secure, and high-performance solution for real-time IoT applications, outperforming the other models.

6. Conclusion

- In conclusion, integrating fog computing with a trustworthy forwarding scheme using MQTT and TLS offers a secure and efficient solution for real-time IoT data processing. By combining MQTT's lightweight communication with TLS's robust encryption and authentication, the approach ensures data integrity and reliability, forwarding only verified, trustworthy data to cloud servers or systems.

- This mechanism enhances IoT applications by reducing latency, optimizing bandwidth, and improving security. It is ideal for real-time environments like industrial automation, smart cities, and healthcare, ensuring data reliability and operational efficiency while maintaining strong security.
- The experimental results from this research demonstrate the robust performance of the proposed mechanism. Conducted with 15 fog nodes, the system achieved a maximum Level of Trust (LoT) score of 0.968, reflecting its high reliability. The overall accuracy of the system was measured at 97.63%, showing exceptional precision in forwarding only trustworthy data.
- The system demonstrated notable performance improvements, including reduced latency, increased throughput, and lower packet loss, with optimal results at 15 fog nodes. Its scalability and adaptability make it suitable for various IoT applications, providing a secure, reliable, and efficient solution for edge data processing while minimizing risks of data breaches and unauthorized access.

7.Reference

1. Liu, W.; Chen, J.; Zeng, L.; Yu, J. Trust-Based Access Control Framework for Fog Computing in IoT. *IEEE Internet Things J.* **2020**, *7*, 6062–6072. [Google Scholar]
2. Yang, J.; Li, Y.; Li, W.; Li, C. An Effective Mechanism for Fog Computing-Assisted Function Based on Trustworthy Forwarding Scheme in IoT. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 1–11. [Google Scholar]
3. Zhang, Y.; Li, M.; Wang, H.; Sun, X. A Secure and Efficient Data Storage and Sharing Scheme for Fog Computing in IoT. *IEEE Access* **2019**, *7*, 104264–104275. [Google Scholar]
4. Xiao, Y.; Krunz, M. AdaptiveFog: A modelling and optimization framework for fog computing in intelligent transportation systems. *IEEE Trans. Mob. Comput.* **2021**, *21*, 4187–4200. [Google Scholar] [CrossRef]
5. Zhang, J.; Wang, C.; Zhang, Q.; Liu, Y. A fog computing-assisted secure and efficient internet of things for pervasive healthcare. *IEEE Internet Things J.* **2019**, *6*, 161–171. [Google Scholar]
6. Cui, Z.; Fan, Y. Design of fog computing system based on blockchain for internet of things. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *11*, 3655–3666. [Google Scholar]
7. Quy, V.K.; Hau, N.V.; Anh, D.V.; Ngoc, L.A. Smart healthcare IoT applications based on fog computing: Architecture, applications and challenges. *Complex Intell. Syst.* **2022**, *8*, 3805–3815. [Google Scholar] [CrossRef] [PubMed]
8. Arun, M.; Barik, D.; Chandran, S.S. Exploration of material recovery framework from waste–A revolutionary move towards clean environment. *Chem. Eng. J. Adv.* **2024**, *18*, 100589. [Google Scholar] [CrossRef]
9. Cheng, H.; Zhao, X. A novel blockchain-based secure scheme for the internet of things. *IEEE Access* **2019**, *7*, 131346–131356. [Google Scholar]

10. Zhou, X.; Wang, S.; Li, K. A blockchain-based secure data sharing scheme for the internet of things. *IEEE Internet Things J.* **2020**, *7*, 6279–6288. [**Google Scholar**]
11. Bellaj, M.; Naja, N.; Jamali, A. Distributed Mobility Management Support for Low-Latency Data Delivery in Named Data Networking for UAVs. *Future Internet* **2024**, *16*, 57. [**Google Scholar**] [**CrossRef**]
12. Zhang, Q.; Chen, Y.; Xiao, Y. A secure and efficient data sharing scheme for the internet of things in fog computing. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *11*, 3679–3692. [**Google Scholar**]
13. Chen, X.; Li, H.; Li, K.; Li, K.; Li, X. A secure and efficient data transmission scheme for fog computing in internet of things. *Future Gener. Comput. Syst.* **2021**, *115*, 143–153. [**Google Scholar**]
14. Wu, J.; Li, M. A fog computing-based secure and efficient data transmission scheme for the internet of things. *Future Gener. Comput. Syst.* **2020**, *112*, 346–354. [**Google Scholar**]
15. Arjun, C.; Hemalatha, M.; Gokulnath, C. MQTT based secure data transmission in fog computing for IoT. In Proceedings of the 2018 IEEE International Conference on Current Trends towards Converging Technologies (ICCTCT), Coimbatore, India, 1–3 March 2018; pp. 1–6. [**Google Scholar**] [**CrossRef**]