TASK 1
Paper Title:
Authenticated Key Agreement Scheme for Fog Computing in a Health-Care Environment

Paper Link: https://ieeexplore.ieee.org/document/10122505

Name: Sania Azhmee Bhuiyan
Course Title: Parallel, Distributed and High-Performance Computing (HPC)
ID:23266033
Team: 16
Course Instructor: Annajiat Alim Rasel

1 Summary

This paper mostly focuses on the Internet of Things (IoT) and its requisite real-time and efficient communication demands specifically on healthcare system. On of the problem working with cloud computing is meeting the ongoing demands of low-latency and high-computing efficiency needs of IoT applications. Thus, this study incorporates fog computing, though we have already been introduced to it. This paper establishes an innovative mutual authentication key establishment scheme grounded in elliptic curve cryptography (ECC), aiming to address the security challenges introduced by fog computing, particularly in the context of identity authentication. The proposed architecture involves mutual authentication, allowing the cloud server to delegate verification tasks to fog nodes, ultimately diminishing the computational burden on the central server. Security assessments applied the random oracle model and the extended Canetti-Krawczyk (eCK) threat model, establishing the system against various attacks.

In the context of healthcare applications, the study emphasizes the significance of IoT networks in the emerging Healthcare where wireless sensor networks and IoT devices play a crucial role in continuous health monitoring. The traditional cloud model faces challenges in processing the vast amount of real-time data generated by these devices. Fog computing, through intermediary fog nodes, is positioned as a solution to enhance service quality by providing computing and storage services closer to end-users. Privacy preservation in fog computing is acknowledged as a critical consideration, with concerns addressed through authentication approaches. The paper reviews existing authentication methods, noting their limitations, and introduces the proposed ECC-based scheme as a more secure and efficient alternative. The proposed ECC-based protocol is positioned as an advancement, promising improved security and reduced computational overhead.

1.1 Motivation:

The paper addresses the limitations of cloud computing, especially in healthcare scenarios where the centralization of data in the cloud raises concerns about data retrieval times, energy consumption, and response delays.

1.2 Contribution:

The paper proposes an elliptic curve cryptography-based mutual authentication key establishment scheme for fog computing in Healthcare system addressing security challenges in identity authentication. It introduces a novel architecture allowing fog nodes to assume verification tasks, reducing the computational load on the cloud server.

1.4 Conclusion

The proposed architecture efficiently authentication responsibilities to fog nodes after mutual authentication, thereby easing the computational load on the central cloud server. The security analyses conducted under the random oracle model and extended Canetti-Krawczyk threat model confirm the scheme's resilience against diverse attacks. Its security measures could be a solution for securing communication in healthcare IoT applications, contributing to the advancement of secure fog computing frameworks to overcome this challenge in healthcare systems and enabling improved medical services through secure data transmission.

2 Limitation

2.1 First Limitation/Critique

The proposed fog computing architecture introduces an intricate key establishment mechanism but falls short in addressing scalability concerns. The paper does not thoroughly explore the system's performance when scaled to accommodate a larger number of fog nodes and devices especially in healthcare scenarios which is common to have a multitude of connected devices. The study's lack of emphasis on scalability limits its practical applicability, potentially hindering its effectiveness in scenarios with extensive fog computing deployments.

2.2 Second Limitation/Critique

The paper discusses security measures against various attacks, but it does not discuss properly about the potential vulnerabilities arising from hardware or software failures. In a real-world deployment, devices and fog nodes may encounter unexpected failures, and the paper does not thoroughly address the system's resilience in such situations.

3 Synthesis

Explain how ideas in the paper relate to potential applications or future scopes.

The paper contributes a novel fog computing architecture for secure healthcare applications, emphasizing mutual authentication and key establishment. While scalability concerns and resilience to failures are notable limitations, the proposed mechanism shows promise in enhancing data security in time-critical healthcare scenarios. The integration of a random oracle model and the extended Canetti-Krawczyk threat model adds a layer of security, and the focus on reducing computational costs between cloud servers and fog nodes is commendable. Future applications could benefit from further research addressing scalability issues and incorporating fault-tolerant measures. The proposed fog computing approach has the potential to revolutionize healthcare decision-making by providing secure, efficient, and real-time data transmission. The emphasis on secure communication in emergency situations aligns with the growing importance of technology in healthcare.