iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59228

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

Fog Computing for Data Security and Privacy in Health-Care System

Rajesh Kumar V[1], Visvasprabhakar R[2], Prasanna Venkatesh A[3], Hari Krishnan[4]
[1, 2, 3, 4]*Dept of Computer Science and Business Systems, Sethu Institute of Technology, Pulloor, Kariapatti – Virudhunagar 626 115*

Abstract: ***The application of the Internet of Things has been greatly expanded; meanwhile, real-time and efficient communication has become an important feature of the Internet of Things. However, the centralized characteristics of cloud computing cannot meet the needs of low latency and high computing efficiency. To solve these issues, we utilized fog computing which is a new distributed computing paradigm that extends cloud services to the edge of the network, with mobility and low latency. Nevertheless, fog computing also brings new security issues, especially identity authentication. Authentication and key exchange are significant challenges that need to be taken into consideration in fog computing. We proposed the architecture of the mutual authentication key establishment scheme based on elliptic curve cryptography for fog computing. After mutual authentication, the cloud server can transfer the remaining verification work to fog nodes. Fog nodes will be responsible for authenticating the device and distributing the established session key, thereby reducing the computational cost of the cloud server. After mutual authentication is completed, the cloud server, fog nodes, and devices can communicate with each other. The Security of the proposed scheme proved that it is strong enough against several attacks.***
Keywords: FairPlay, malware, fraudulent apps, Google Play, review activities, search rank fraud.

I. INTRODUCTION

With the rise of 5G, the amount of data generated by healthcare IoT devices has increased significantly. Besides, cloud computing has greatly expanded the potential applications of wearable medical sensors (WMS)-based systems due to its high storage capacity and flexible processing services [1]. Consequently, the storage and security of such extensive data have become major concerns [2]. Researchers and institutions around the world have been working on prototypes to leverage WMS technology and services offered by the cloud. The benefit of keeping medical data in a centralized cloud environment is that the PHR can be shared easily [3]; however, cloud computing still faces several issues for sensitive applications, such as:(1) Data retrieval times for urgent situations are unreasonably long.(2) Sending data to the cloud for calculations frequently requires lots of energy consumption and associated costs, especially given the volume of data produced by sensors. (3) A typical cloud service has a severe delay and low sustained performance compared to a distributed computing architecture with numerous computing nodes in various locations.

II. PROBLEM IDENTIFICATION

In health-care environments, the adoption of fog computing paradigms for data processing and storage introduces challenges related to ensuring secure communication between various entities such as medical devices, sensors, and cloud servers. One critical aspect of maintaining security is establishing authenticated key agreement schemes tailored for fog computing infrastructures.

However, existing key agreement schemes may not adequately address the unique requirements and constraints of health-care environments, which demand stringent security, low latency, and efficient resource utilization. Addressing this problem requires a comprehensive understanding of the security requirements in health-care environments, the characteristics of fog computing, and the cryptographic techniques suitable for key agreement in resource-constrained settings. Additionally, the proposed schemes need to be rigorously evaluated through simulation or practical deployment to assess their effectiveness, scalability, and performance under real-world conditions.

III. OBJECTIVES

1) Evaluate proposed method against existing schemes.
2) Assess security features and communication efficiency
3) Focus on reducing cloud-fog communication costs

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

IV. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things are satisfied, then next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

A. Transactions on Cloud Computing

This paper conducts a comprehensive review of existing key agreement schemes suitable for secure data transmission in fog computing environments. It analyzes various schemes based on their cryptographic techniques, security properties, efficiency, and suitability for health-care applications.

B. ACM Computing Surveys

This survey paper provides an overview of security challenges in fog computing environments, including authentication and key agreement. It reviews various authentication and key agreement schemes proposed for fog computing and evaluates their effectiveness in addressing security concerns in health-care applications.

C. A Comparative Analysis of Search Engine Ranking Algorithms

This paper presents a survey of secure data transmission techniques in fog computing with a focus on their applicability to health-care scenarios. It reviews authenticated key agreement schemes and evaluates their suitability based on security requirements, computational overhead, and scalability.

V. BLOCK DIAGRAM & CIRCUIT DIAGRAM

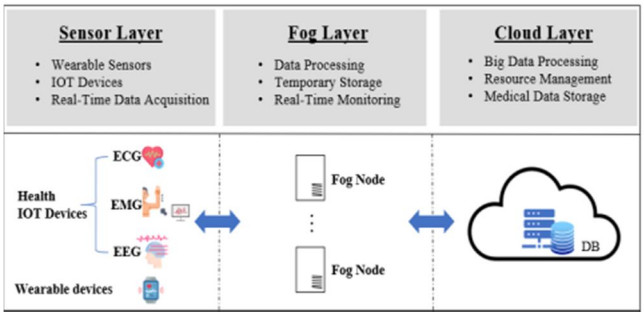


Fig. 1. Block Diagram of system

VI. ADVANTAGES

1) The proposed scheme can minimize computational overhead on fog devices by employing lightweight cryptographic algorithms and optimized key agreement protocols.
2) This optimization enhances the efficiency of data transmission and processing, enabling real-time communication and analysis in health-care applications without undue burden on resource-constrained devices.
3) The proposed system can dynamically adapt to changes in network topology, device configurations, and user access patterns in fog computing environments

VII. CONCLUSION

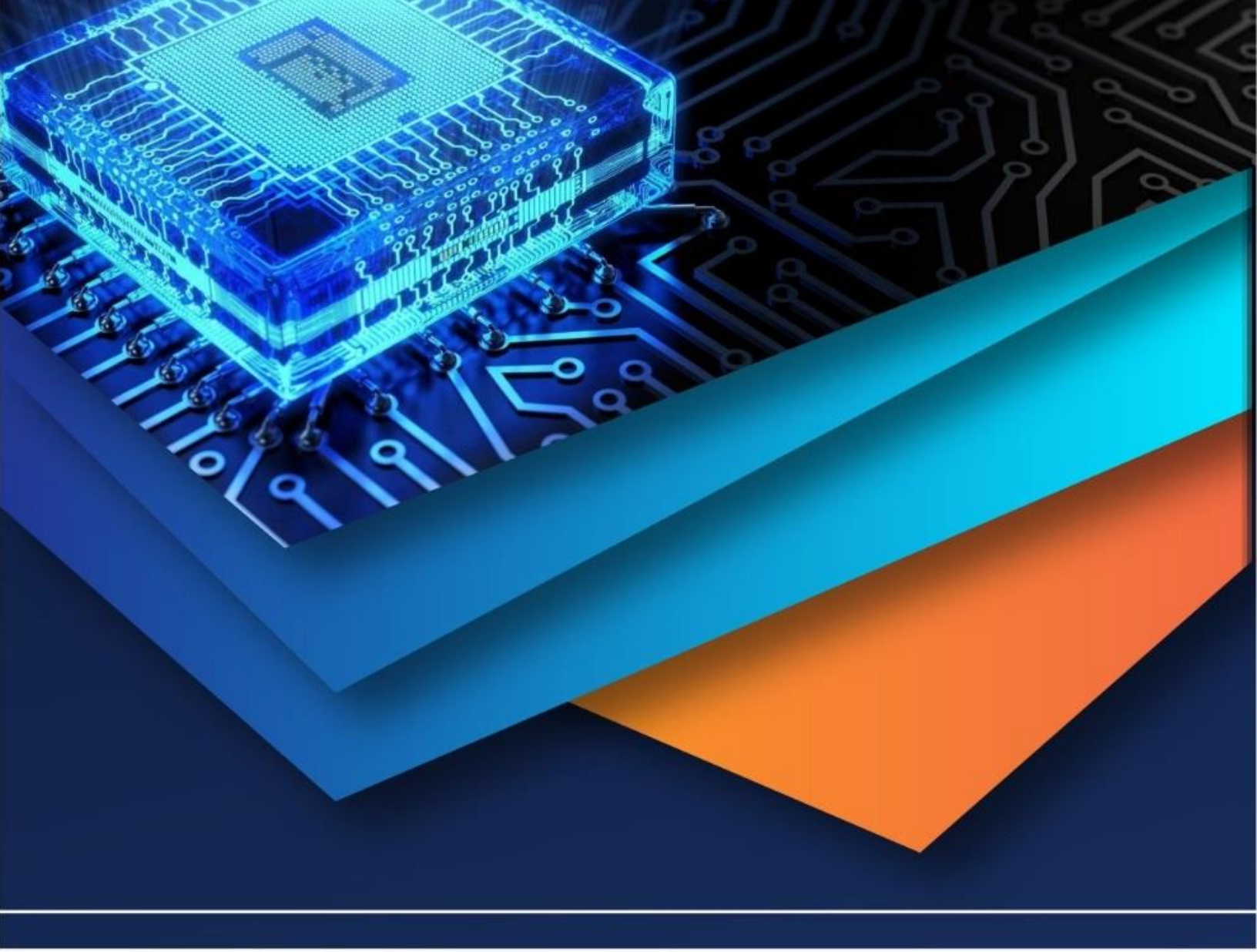
In conclusion, Fog computing helps doctors to make decisions during an emergency for time-critical Healthcare applications. It also helps to protect sensitive data with reduced delay in comparison to the standalone cloud-based application. However, data privacy and system compatibility are essential challenges that must be addressed when considering how medical records can be delivered. In the case of inadequate network security, fog nodes, and devices can be hacked, and communication can be intercepted. The mutual authentication key establishment proposed herein is a safe and efficient information security mechanism for fog computing architecture in a healthcare environment. In this method, fog nodes can be applied to validate the device's authenticity, thereby reducing the computational cost of the cloud server.

©IJRASET: All Rights are Reserved

REFERENCES

[1] Securing fog computing for Internet of Things applications: Challenges and solutions. IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 601–628,1st Quart., 2019.
[2] Authenticated key agreement scheme for fog-driven IoT healthcare system. Wireless Netw.,vol. 25, no. 8, pp. 4737–4750, Nov. 2019.
[3] An enhanced pairing-based authentication scheme for smart grid communications. Journal of Ambient Intelligence and Humanized Computing, 2021.
[4] A robust authentication and access control protocol for securing wireless healthcare sensor networks. Journal of Information Security and Applications, vol. 52, Article ID 102502, 2020.
[5] Securing IoT-based RFID systems: a robust authentication protocol using symmetric Cryptography. Sensors, vol. 19, no. 21, p. 4752, 201.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)