A Secure and Efficient Key Management and User Authentication Scheme for Fog Computing

By

SHIVENDRA SAXENA
Roll No. B150105CS

Under the Supervision of

Dr. Sangram Ray
Assistant Professor

PROJECT REPORT
Submitted to
NATIONAL INSTITUTE OF TECHNOLOGY SIKKIM
for the award of the degree of
Bachelor of Technology
in
Computer Science and Engineering
May 2019

Department of Computer Science and Engineering

National Institute of Technology Sikkim

(An Institute of National Importance, under MHRD, Govt. of India)
Ravangla, South Sikkim – 737139, Sikkim, India

CERTIFICATE

It is hereby certified that the dissertation report entitled ***“A secure and efficient key management and user authentication scheme for fog computing”*** submitted by **Shivendra Saxena** bearing Roll No. B150105CS for the fulfillment of the requirement for the award of the degree **Bachelor of Technology in Computer Science and Engineering** at National Institute of Technology Sikkim is an original record of her own work carried out during the period August 2015 to May 2019 under my sole supervision and has not been reiterated in any other form of degree or diploma.

Dr. Sangram Ray
Assistant Professor & HOD
Department of Computer Science and Engineering
National Institute of Technology Sikkim
Ravangla, Sikkim-737139, India

ACKNOWLEDGEMENT

I am tremendously indebted to my supervisor **Dr. Sangram Ray, Assistant Professor and Head of the Department, Department of Computer Science and Engineering**, National Institute of Technology Sikkim for his invariable guidance and assistance during the course of thesis and its evolvement. His advice and suggestions have been prized in the development and progress of the content. Furthermore the skills and knowledge which I have gained throughout this period I perceive that as very valuable and significant for my future.

I take this opportunity to acknowledge the Director, Prof. M. C. Govil, all Deans, all departmental professors, research scholars and staff who have provided the necessary infrastructure and their valuable experience throughout this entire curriculum and led to my piecemeal growth as a student.

Finally I express my deepest gratitude to my family & friends for their untiring encouragement and unconditional support.

Shivendra Saxena

List of Contents

List of Tables

List of Figures

Abstract

Fog computing is a decentralized computing infrastructure in which data, applications, compute as well as data storage are scattered in the most logical and efficient place among the data source (i.e., smart devices) and the cloud. It gives better services than cloud computing because it has better performance with reasonably low cost. Since, the cloud computing has security and privacy issues, and fog computing is an extension of cloud computing, it is therefore obvious that fog computing will inherit those security and privacy issues from cloud computing. Recently, a scheme on secure key management and user authentication for fog computing services, SAKA-FC was proposed by Wajid et al. which is a three-factor authentication scheme with privacy preservation for remote user based on ECC, hash functions, fuzzy extractor and symmetric bivariate polynomial function. In this report the scheme proposed by Wajid et al. is analyzed and found that it is not resilient against fog server insider attack and denial of service attack. Further, to eradicate all of the above mentioned attacks, an enhanced, lightweight and secure scheme is proposed. The proposed scheme is verified using both formal and mathematical security analysis, and simulated using AVISPA that shows all the protocols are well secure against all relevant security attacks. The performance analysis depicts that the proposed scheme is more efficient and lightweight than other existing schemes.