DESIGN AND DEVELOPMENT OF TRUST-BASED MECHANISMS FOR SECURING FOG-IOT ENVIRONMENT

A Summary of Thesis

submitted in fulfillment of the requirements forthe

degree of

Doctor of Philosophy

IN

COMPUTER SCIENCE

Submitted by

Richa Verma

Enrolment No.: 1305/15

Under Supervision of

Dr. Shalini Chandra

Submitted to

DEPARTMENT OF COMPUTER SCIENCE

SCHOOL FOR INFORMATION SCIENCE AND TECHNOLOGY

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY

(A CENTRAL UNIVERSITY)

VIDYA VIHAR, RAEBARELI ROAD,

LUCKNOW-226025, UTTAR PRADESH, INDIA

2023

ABSTRACT

In recent years, the technological world has experienced a revolutionary shift due to the emergence of the Internet of Things (IoT). This increasing popularity of the IoT sector has contributed to the exponential growth of user data across the web. This huge amount of data generated by the IoT devices presents computation, storage and processing requirements. These requirements are fulfilled by the cloud computing technology. But, IoT applications such as e-healthcare systems, smart cities, intelligent transportation systems, etc., are latency-sensitive and demand prompt responses. Unfortunately, cloud computing is not able to serve these new computational demands appropriately and prevents the applications from reaching their full advantages.

To overcome this shortcoming, fog computing has emerged as a computing infrastructure that provides storage and processing facility close to end-users. It is an analytical and processing platform that complements the cloud environment by extending its resources physically and computationally closer to end devices. Additionally, it has gained traction both in academics and industry because of its characteristics like heterogeneity, mobility, location awareness, etc., which help generate timely responses for latency-sensitive applications.

Besides the various benefits of fog computing, there also exist certain setbacks that restrict its acceptability. The introduction of fog computing adds a new layer to the primary computing architecture. This additional layer increases the attack surface and makes it prone to fall prey to adversaries. Furthermore, the fog-IoT paradigm also deals with users' sensitive data. Thus, it becomes inevitable to address security at the fog level. Additionally, fog-IoT communications involve several communicating parties such as fog

service providers, network service providers, third-party smart applications, etc., which makes the sensitive data travel through variating trust domains. Thefore,due to the absence of a centralized trusted party, ensuring trust is obligatory for an infallibly secure fog environment.

Thus, the thesis attempts to deliver trust-based solutions for securing the fog-IoT environment. In this direction, the researcher conducted a Systematic Literature Review (SLR) to analyze the role of security in fog setup. The prime focus of the review is to assess the security status in the domain. The review summarizes the literature procured from five renowned libraries. A total of 735 initial studies were gathered, out of which 102 articles qualifying inclusion criteria, were selected for final full-text review. These 102 studies are reviewed with respect to the research questions framed in the early phase of SLR. The outcome of the survey is shaped in the form of the answers to the research questions and reveals the prominence of security in the said frame.

Further, different fog computing security factors and sub-factors are idenified through the extensive review and discussion with experts. In addition, the order of addressing identified fog computing security factors and sub-factors plays a vital role in efficient security management. Therefore, an integrated Multi-Criteria Decision Making (MCDM) methodology named Interval-Valued Intuitionistic Fuzzy Set-Analytical Hierarchy Process (IVIFS-AHP) is applied for ranking them. As per the results, ‘trust’ is highly prioritized and thus is selected as the scope of the thesis.

It is imperative that in order to handle trust, griping its sub-factor is very important. Therefore, considering the sub-factors of trust ‘reliability’ has shown up at rank one. Thus, the researcher has proposed a FogBus3 framework comprising the IoT layer, the

Reliability-Aware Fog Layer (RAFL), and the Cloud layer. The IoT layer consists of IoT devices that are capable of generating requests. The RAFL categorizes IoT jobs according to the predefined classes of service and takes the offloading decision. The jobs that are offloaded to fog utilize the proposed IoT-Fog Agreement Algorithm (IFAA) to guarantee the agreement amongst the communicating fog nodes. The proposed IFAA algorithm establishes agreement amongst the communicating fog nodes through a consensus mechanism. Also, the jobs categorically offloaded to cloud are executed by cloud itself. The approach is simulated over MATLAB R2021a and an improvement of 41% in terms of execution time is observed.

Furthermore, as dependability holds the second spot amongst ranked sub-factors of trust, a transitive interpretation of dependability in the fog-IoT domain is proposed. The interpretation presents a roadmap for managing dependability by deploying load balancing in the fog computing environment. Thus, a Honey Bee Inspired-Load Balancing (HBI-LB) approach is proposed for balancing the load in the fog-IoT setup. The proposed HBI-LB is simulated over CloudSim 3.0.3-based Cloud Analyst tool. The results reveal that the proposed approach significantly improves the average response time. Thereby, making the said environment more dependable.

In addition, to guarantee a trustworthy fog-IoT paradigm, the researcher has also proposed a machine learning centric Reputation-based Trust Enhancement framework (RepuTE) for filtering reputation-related attacks in the said setup. The proposed framework aims to filter the most prevalent reputation-based attacks, say, Sybil and DDoS/DoS attacks from the fog traffic. The proposed framework deploys a soft-voting ensemble model for detecting the said attacks. The trained classification model is deployed over a dedicated fog node named master fog node and operates in phases.

Initially, a novel feature set selection technique proposed by the researcher selects the best-performing feature set. Then, three machine learning algorithms namely K-Nearest Neighbor (KNN), Extra Tree Classifier (ETC), and Quadratic Discriminant Analysis Classifier (QDA) are parallelly trained over the reduced feature set. The predicted outputs from these three base learners are then fed to the voting classifier for providing the final classification result. The experimental results show that the proposed model efficiently differentiates between normal and attack records.

In addition, the proposed IFAA and HBI-LB mechanisms have also been validated statistically by applying the t-test: Paired Two Sample for Means and t-test: Two Sample for Means for unequal variances respectively at a 5% level of significance.As per the validation results, the proposed approaches have significantly better results than the compared approaches.