DESIGN AND DEVELOPMENT OF A MECHANISM TO SECURE DATA IN FOG-BASED IOT ENVIRONMENT

A Summary of Thesis

submitted in fulfillment of the requirements forthe

degree of

Doctor of Philosophy

IN

INFORMATION TECHNOLOGY

Submitted by

Jasleen Kaur

Enrolment No.: 190/14

Under Supervision of

Dr. Alka

Submitted to

DEPARTMENT OF INFORMATION TECHNOLOGY
SCHOOL FOR INFORMATION SCIENCE AND TECHNOLOGY
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A CENTRAL UNIVERSITY)
VIDYA VIHAR, RAEBARELI ROAD,
LUCKNOW-226025, UTTAR PRADESH, INDIA

2023

ABSTRACT

Since its inception, the Internet of Things (IoT) sector has experienced exponential growth. Today, almost every individual is connected to the Internet. This alarming growth in Internet-enabled devices points toward the generation of high amounts of data in demand of processing, computation, and storage. In this situation, cloud computing emerges as a viable solution that enables its users to utilize its abundant resources as per the pay-as-you-use model. Though cloud computing technology works quite efficiently in the present digital scenario, but at the same time, it fails to deliver prompt responses in the case of latency-sensitive smart applications such as healthcare, traffic management systems, etc. Hence, the need for real-time responses in time-critical scenarios led to the introduction of fog computing technology in 2012.

Fog computing is a highly virtualized platform that provides computing, storage, and networking services between end devices and traditional cloud computing data centers, typically but not exclusively located at the edge of the network. Instead, the computing facilities may lie anywhere between the device-to-cloud continuum, which significantly minimizes the service latency. But, as every coin has a flip side, fog computing technology also presents unique issues and challenges due to its highly differentiating fundamental characteristics. For instance, introducing a processing layer between the cloud and end users increases the attack surface, making the sensitive user data traveling through the fog-IoT setup prone to fall prey to adversaries. Therefore, a comprehensive security setup for the fog-IoT scenario becomes inevitable.

In this light, the researcher has addressed security issues in the fog-IoT paradigm in the proposed thesis. To begin, a Systematic Literature Review (SLR) highlighting security-related aspects of the said environment is conducted. The researcher has framed four research questions to provide an overview of the orientation of security experts toward security at the fog level. These pre-defined research questions are answered by exploring 134 primary studies. Subsequently, the researcher has also identified different fog computing security factors and sub-factors through the SLR and discussion with experts. The sub-factors are the mechanisms that may be deployed to deal with the corresponding security factors.

Further, the identified fog computing security factors are prioritized using an integrated Multi-Criteria Decision-Making (MCDM) methodology named Neutrosophic Analytical Hierarchy Process (NAHP). The main idea behind prioritization is to specify the order in which the identified fog security factors should be addressed for efficient security management in the said environment. The prioritization paves the way for the researcher by defining a sequence in which identified fog computing security factors need to be addressed. This is helpful for the effective overall security of the fog computing environment. As per the study, 'privacy' is highly prioritized, and thus 'privacy preservation' is taken up as a research premise of the proposed thesis.

In this direction, the researcher has proposed an encryfuscation model that deals with privacy at the fog level. The two highly prioritized sub-factors of privacy, viz., obfuscation and encryption techniques, are selected for the same. The researcher has introduced the Secure Service Offloader (SSO) as the offloading decision-making entity in the fog-IoT paradigm. The SSO takes the job request as the input and offloads the same to either fog or cloud, depending upon

the severity of the job. Further, a suitable privacy preservation scheme out of obfuscation and encryption is implemented before sending the job data to the fog/ cloud layer.

In addition, the researcher has also proposed privacy preservation schemes, namely a data obfuscation approach, a location obfuscation approach, and a BlowCurve encryption mechanism for implementing the proposed encryfuscation model. As per the proposed model, the data being offloaded to the fog layer needs to be obfuscated before its transmission. For this, the proposed data obfuscation approach converts the Actual Sensed Data (ASD) into Obfuscated Sensed Data (OFSD).

The model also confirms that the location coordinates are obfuscated in both cases of either the service being offloaded to fog or cloud. The proposed location obfuscation approach takes the Actual Location Coordinates (ALC) and User Privacy Preference Range (UPPR) as input and provides Obfuscated Location Coordinates (OFLC). The OFLC is calculated on the basis of UPPR, say Low Sensitivity Range (LSR), Medium Sensitivity Range (MSR), and High Sensitivity Range (HSR). The proposed data obfuscation and location obfuscation approaches are simulated over MATLAB R2021a, and their insignificant run times justify their applicability in time-critical fog scenario.

Further, as per the proposed encryfuscation model, the sensor data needs to be encrypted before getting offloaded to the cloud. Thus, the researcher has proposed a dynamic, user-centric, and lightweight encryption algorithm named BlowCurve, that puts the user in charge of his/her private information. The strength of the dynamic key is as per the user-selected privacy level. The proposed algorithm is simulated using Python 3 (Jupyter 6.0.0 notebook). The

execution time gives a strong indication of its applicability in the latency-sensitive fog-IoT context.

In addition, the proposed data obfuscation, location obfuscation, and BlowCurve encryption approaches have also been validated statistically by applying the t-test: two sample for means for unequal variances at a 5% level of significance. As per the validation results, the proposed approaches have significantly better results than the compared approaches.

Moreover, to guarantee a fully-private fog-IoT network, the researcher has proposed a Machine Learning (ML)-based stacked ensemble model named Privacy-Preserving Attack Detection Framework (P2ADF). It detects two prominent privacy-oriented attacks, Man-in-the-Middle (MiTM) and Denial-of-Service (DoS)/ Distributed DoS (DDoS) in the said environment. It operates in two phases. In the first phase, the proposed feature set reduction approach reduces the feature set and provides it as an input to the proposed stacked ensemble ML model that operates in the second phase.

Additionally, the researcher has deployed the proposed model at a specific fog node called fog learner to meet the latency requirements of the fog environment. The sole responsibility of the fog learner is to analyze the fog traffic for the specified privacy-based attacks and block the same. It also updates the attack record at the cloud level. This aids in effective privacy-preservation in the fog environment.