# A Secure and Efficient Authenticated Key Agreement Protocol Based on Elliptic Curve for Securing the Fog Computing Environment

By

**Kholoud Ismail Odeh Saleh**

Supervisor

**Dr. Zeyad Dasouqi Mohammad**

Co-Supervisor

**Dr. Ahmad Abusukhon**

**Al-Zaytoonah University of Jordan, 2020**

## ABSTRACT

Fog computing is a paradigm distributed between cloud data centers and end devices as an intermediate layer. It provides the ability to compute, network, and store cloud-based services more closely to end devices which are highly distributed at the network edge along with latency-sensitive service requirements, Moreover, fog computing has many applications like Smart Home, Healthcare, Connected Vehicles, Smart Grids and Augmented Reality. These applications based on Fog Computing can be confusing in authenticate and secure the session between participating parties and how to prevent unauthorized access to the nodes data and connections especially after load balancing technique which distribute workload between fog nodes to utilize the usage of resources, improve the response time and avoids the heavily loaded on the nodes while others are in idle state. Thus, as nodes are deployed in an uncontrolled environment, secure these fog nodes is a significant problem to address before load balancing is performed. Therefore, this thesis proposed a secure authenticated key agreement protocol based on Elliptic Curve for Securing the Fog Computing environment. The proposed protocol designs a mutual authentication protocol between fog nodes to generate a common session key for securing the communication between fog nodes in the case of performing a load balance among fog nodes.

The proposed protocol based on the ECC and implicit certificate instead of the traditional certificate to save network bandwidth. The proposed protocol is a two-pass message exchange that provides entity authentication and key confirmation. The proposed protocol can satisfy an explicit key authentication in an indirect way to prevent denial of service and has a confirmation procedure by calculating the static public key to verify the other nodes. Also, we analyze the proposed protocol security attributes. Further, the Scyther tool is a verification method used to prove the security of the proposed protocol and ensure that it is protected in the formal security models such as the CK and eCK models. Furthermore, this study presents a security comparison between the proposed protocol with other works and demonstrations that the proposed protocol satisfies the security attributes in the fog environment.

**Keywords:** Cloud Computing, ECC; Fog Computing; Security models; Scyther tool.

.