US 20230231909A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2023/0231909 A1**

MOON (43) **Pub. Date: Jul. 20, 2023**

(54) **SECURE AD-HOC DEPLOYMENT OF IOT DEVICES IN A SECURE PEER-TO-PEER DATA NETWORK**

(71) Applicant: **WhiteStar Communications, Inc.**, Durham, NC (US)

(72) Inventor: **BILLY GAYLE MOON**, Apex, NC (US)

(73) Assignee: **WhiteStar Communications, Inc.**, Durham, NC (US)

(21) Appl. No.: **17/685,315**

(22) Filed: **Mar. 2, 2022**

Related U.S. Application Data

(63) Continuation-in-part of application No. 17/580,365, filed on Jan. 20, 2022.

Publication Classification

(51) **Int. Cl.**

H04L 67/1087	(2006.01)
H04L 9/40	(2006.01)
H04L 67/133	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 67/1091*** (2013.01); ***H04L 63/0815*** (2013.01); ***H04L 67/133*** (2022.05); *G16Y 30/00* (2020.01)

(57) **ABSTRACT**

A secure executable container executed by a network device establishes a two-way trusted relationship in a secure peer-to-peer data network with a network entity, generates a secure key for the network device in the secure peer-to-peer data network, and associates the endpoint device with a federation identifier identifying the user entity in the secure peer-to-peer data network. The secure executable container also: establishes a two-way trusted relationship between the network device and a target network device; obtains, based on the two-way trusted relationship, cohort interface element definition describing commands executable by the target network device; and generates a data object identifying a selected command from the commands and identifying an identifier for the target network device as a subscriber to the data object, causing the target network device to securely retrieve and execute the selected command.