June 04, 2018

BLOCKCHAIN BASED WI-FI ONBOARDING SIMPLIFICATION, IDENTITY MANAGEMENT AND DEVICE PROFILING FOR IOT DEVICES IN ENTERPRISE NETWORKS

Byju Pularikkal

Santosh Patil

Swami Anantha

Sourav Chakraborty

BLOCKCHAIN BASED WI-FI ONBOARDING SIMPLIFICATION, IDENTITY MANAGEMENT AND DEVICE PROFILING FOR IOT DEVICES IN ENTERPRISE NETWORKS

AUTHORS:
Byju Pularikkal
Santosh Patil
Swami Anantha
Sourav Chakraborty

ABSTRACT

A consortium blockchain fabric is provided as a Digital Network Architecture Center (DNAC) Application (APP) stack running in a Cloud Neutral Facility. This consortium blockchain fabric achieves two important functions: Verification of Internet of Things (IoT) Vendor Installed Identity and IoT Device Network Usage Profile.

Verification of IoT Vendor Installed Identity. IoT device vendors will be part of the IoT consortium that maintains the blockchain fabric. The manufacturer installed identity credentials of the devices are registered on the blockchain. This allows the enterprises to verify the manufacturer installed identity of the device at the time of onboarding.

IoT Device Network Usage Profile. These are the traffic flow characteristics of the IoT application. The IoT service provider is responsible for registering the network usage profile on the blockchain fabric. IoT service providers will be consortium members. In many cases, the IoT vendor and the IoT service provider will be the same entity.

DETAILED DESCRIPTION

A significant portion of IoT devices today use Wi-Fi® network access for connectivity. While the IoT device ecosystem uses various access technologies for connectivity such as LORA, Bluetooth®, NarrowBand IoT (NB IOT) radio etc., Wi-Fi is expected to continue playing a significant role in access connectivity for IoT devices. This is particularly true for IoT devices such as surveillance cameras, printers etc., which require

Published by Technical Disclosure Commons, 2018

high bandwidth connectivity. Onboarding and management of Wi-Fi enabled IoT devices currently face the following two key challenges:

Authentication: IOT devices need to present a set of identity credentials to get access to the Wi-Fi network. Today, the most commonly used credentials are pre-shared keys. These need to be provided by the IoT service operators or device vendors to the Enterprise IT. There is no scalable well-defined process to approach this.

Identity Management: The IoT device ecosystem is so fragmented that every vendor uses their own solutions. The lack of a federated identity makes IoT service enablement challenging.

Enterprise Network Onboarding: This issue is related to credential management. Often, the process of allowing the device into the network involves tedious manual administration on the IT side. IoT devices will not have the capability to support portal based sign-up for onboarding since it requires manual intervention.

Network access entitlement: There are some mechanisms available today to learn the network access requirements for an IoT device (for example, Manufacture Usage Description (MUD)-identifier based). However, this is not a flexible and scalable solution and relies on manufactures to support it.

IoT industry leaders already have realized the benefits of leveraging blockchain for identity management and various other use cases such as supply chain management, asset tracking etc. These solutions may be built using a consortium blockchain fabric or private blockchain fabric.

Presented herein is a Consortium blockchain fabric implemented on Maglev as a Digital Network Architecture Center (DNAC) Application (APP) stack running in a Cloud Neutral Facility. This Consortium blockchain fabric can be facilitated as a Cloud Service offering running on DNAC Cloud to IoT ecosystem partners. While the consortium blockchain can be leveraged for several IoT services, the following focuses on following several key aspects:

Verification of IoT vendor installed Identity: IoT device vendors will be part of the IoT consortium that maintains the blockchain fabric. The manufacturer installed identity credentials of the devices will be registered on the blockchain. This will allow the

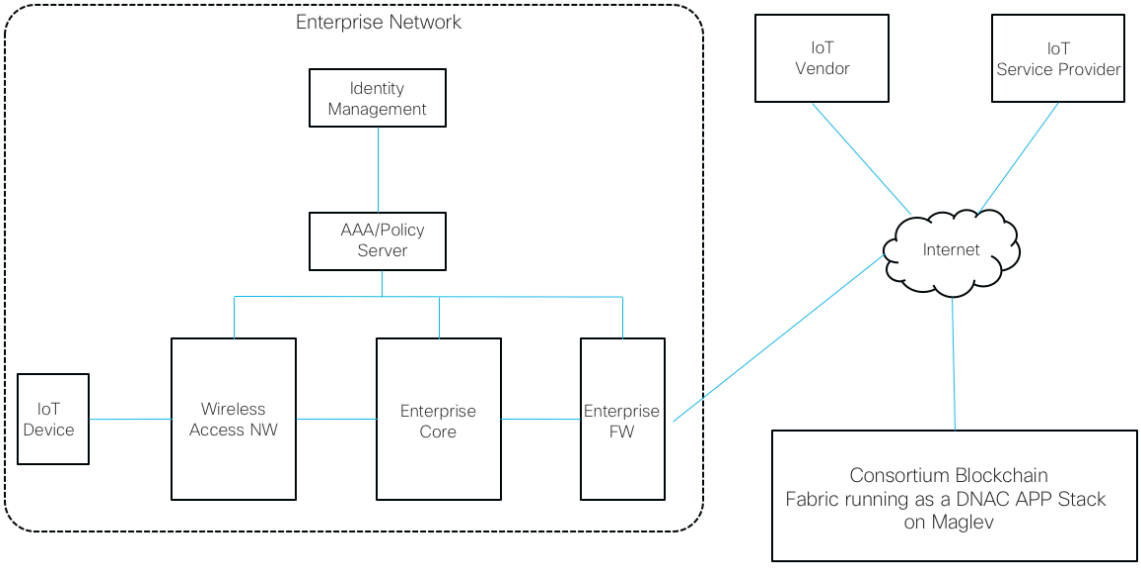
enterprises to verify the manufacturer installed identity of the device at the time of onboarding.

IoT Device Network Usage Profile: This is the traffic flow characteristics of the IoT application. The IoT service provider is responsible for registering the network usage profile on the blockchain fabric. IoT service providers will be consortium members. In many cases, IoT vendor and IoT service provider will be the same.

This solution can support secured and simplified IoT onboarding for Wi-Fi enabled IoT devices in an Enterprise network. On the device side, the solution leverages Wi-Fi Alliance Hotspot 2.0 (Passpoint) capabilities to simplify the onboarding. Enhancements may be used in Passpoint to support "zero touch" IoT device onboarding.

A high-level solution view of the proposal is provided in Figure 1 below:

Figure 1



In this solution, the Wi-Fi enabled IoT device will have a Passpoint client agent integrated in it. The device will have a manufacturer installed identity, which will be used for the initial Wi-Fi network connection. The Passpoint profile will be tied to the

manufacturer identity credentials and the IoT consortium ID. Various stages of the onboarding process are described below.

Initial Network Connectivity:

Wireless access network will be enabled with Passpoint and it will be configured to support IoT consortium id. As soon as the IoT device is connected to the Wi-Fi network, it will look for HS 2.0 capable SSIDs. Since Enterprise SSID will carry the HS 2.0 indicator on the Wi-Fi Beacon and Probe Response messages. IoT device will then use ANQP GAS messages to collect the supported HS2.0 parameters. Once it finds that Consortium id is included a supported realm by the Wi-Fi network it will attempt to associate with the SSID. IoT device will present manufacturer installed device certificate as part of the initial authentication process. Enterprise AAA server can query the consortium blockchain fabric to verify the device certificate. Since the vendor installed identity credentials are registered on the blockchain fabric, blockchain fabric will confirm the identity. Once the identity is confirmed, the Enterprise AAA server can do another query to download the Network Usage profile corresponding to the device ID. The IoT device will be successfully associated to the Enterprise Wi-Fi and "restricted network access" will be granted. At this time, the IoT device will not be allowed to communicate with any external entities.

Installation of Enterprise Identity

In order to fully onboard the device into the Enterprise network, Enterprise identity credentials need to be installed on the IoT device. This identity installation can be automated by using Passpoint Access Network Query Protocol (ANQP) messages over Generic Advertisement Service (GAS). Some of the Vendor specific information fields, which are part of the IEEE 802.11u specification, are used to push the enterprise credentials over the Passpoint networks dynamically to the IoT device. The primary intention of the IEEE 802.11u specification is to support automated network discovery and selection of the Passpoint enabled networks by compatible handsets as part of generic advertisement service. However, the IEEE 802.11u specification does not limit the exchange of GAS messages even after a device has been successfully associated with a Wi-Fi network. Once the Enterprise credentials have been established, the IoT device will be forced to disconnect

and re-connect on the Wi-Fi network. During the re-association time, the device will use newly installed Enterprise credentials.

Installation of QoS and Firewall Permission Rules: The device network profile which was collected by the Authentication, Authorization, and Accounting (AAA) / Policy server from the blockchain fabric provides enough information to build Access Control Lists (ACLs) and Quality of Service (QoS) rules on the wireless access switch and the permission rules on the firewalls. On the access side this can be installed on the access points/wireless LAN controller (APs/WLC) via RADIUS Change of Authorization (CoA). On the firewall, a Software-Defined Networking (SDN) interface can be used to install the permission rules.

In summary, a consortium blockchain fabric provided as a DNAC APP stack running in a Cloud Neutral Facility. This consortium blockchain fabric achieves two important functions: Verification of IoT vendor installed Identity and IoT Device Network Usage Profile.

Verification of IoT Vendor Installed Identity. IoT device vendors will be part of the IoT consortium that maintains the blockchain fabric. The manufacturer installed identity credentials of the devices are registered on the blockchain. This allows the enterprises to verify the manufacturer installed identity of the device at the time of onboarding.

IoT Device Network Usage Profile. These are the traffic flow characteristics of the IoT application. The IoT service provider is responsible for registering the network usage profile on the blockchain fabric. IoT service providers will be consortium members. In many cases, IoT vendor and IoT service provider will be the same entity.