IDENTITY MANAGEMENT MODELS IN IoT

Identity Management

- Identity management is a combination of processes and technologies to manage and secure access to information and resources.
- IdM is oriented towards identity of either devices or user but in IoT mapping between the device identity and context identity is required.
- The main purpose of the identifier is to uniquely identify things, objects or devices.

Ways to constructidentifiers

1. Using Random Data
2. Hierarchical identifiers
3. encoded identifiers (eg: timestamp)
4. Cryptographic identifiers (eg:Hash)
5. Hybrid identifiers

Identity Management

Current IdM solutions are mainly concerned with identities that are used by end users, and services identify themselves in the networked world (eg: OpenID).

These solutions provide user attributes & authentication as a service to relying parties.

It is complex & dynamically developing area due to its importance in online communities.

Main IdM solution focuses on definition of Idm lifecycle, definition of

Identity Management in IoT

- Describes how users interact with devices as well as devices interact with other
- devices.

- Users interact with their devices and consume services in Iot through verified identity.

- IoT users are able to discover and use devices that are public add things temporarily to their personal space, and share their devices with others and devices that are public can be part of the personal space of multiple users at the same time.

- Secure interaction in and with Iot, secure data management and exchange, authentication, distributed access control and IDM of the devices are the main challenges.

Identifier format for things

- Nomadic devices can join to public or private IoT.
- Need to assign ownership to these devices
- Should provide an easier way to identify whether the thing is RFID tag, sensor node, or PDA.
- This format for devices should have association with different attributes and these attributes are based on namespace in which these devices are used.
- ORI - Object or Resource Identifier

Different Identity Management Models

Need to derive taxonomy of different identity models depending upon scope of an identity as well as the local and global context in which an identity is used and represented.

IoT devices/objects can have knowledge of other IoT devices/objects which can be identified.

The scope and lifetime of these things and identities vary from context to context.

Different Identity Management Models

Identity of an IoT object will be context aware and can be known locally, across the ubiquitous network or globally.

Also IoT objects/devices can also be associated with multiple digital identities (virtual identities).

There is a need that these devices should be uniquely and unambiguously
identified in multi context IoT.

Each object is uniquely identified by a set of attributes.

Different Identity Management Models

1. Local Identity
2. Network Identity
3. Federated Identity
4. Global Identity

Local Identity

- In centralized architecture like smart home or client server paradigm, identity is local in nature.
- In centralized computing, a host system maintains and manages local database of identities.
- In IoT context smart home is an example of centralized computing where all devices in smart home are registered in a local database and if external device or entity wishes to join the system, it is first required to acquire an identity from server and entry is to be made in registry.

Local Identity

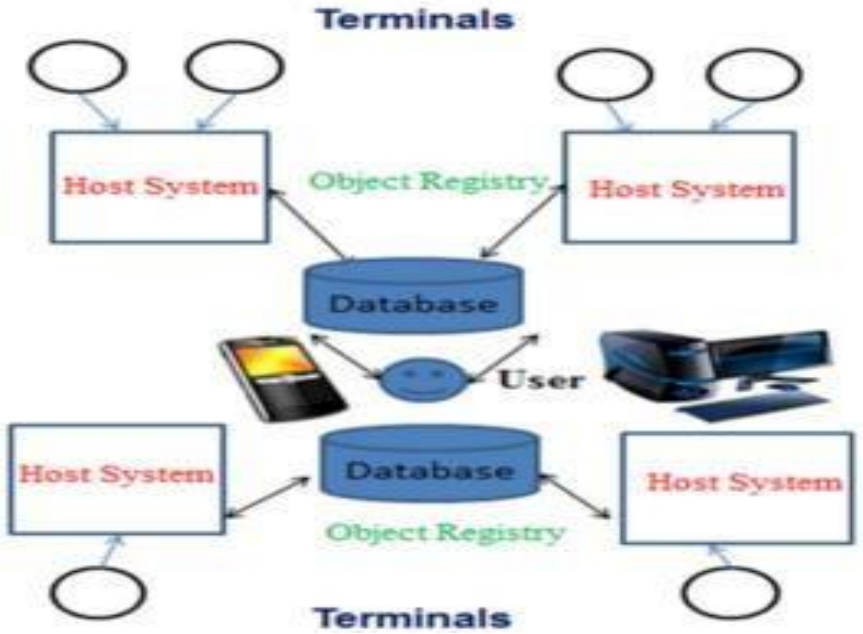
The system also checks for duplication of identity being issued in order to maintain uniqueness.

In centralized computing, addition,deletion of identities is simple and independent of other operations.

As shown in figure, a central object registry is maintained for all the terminals or devices connected to it.

As in case of smart home, all devices in one context are registered with one central database and can be shared across the system.

Local Identity



Advantages of Local Identity

Simplicity :

As one central entity is responsible for issuing and registering identity, manageability become
easy.

Generally flat addressing or naming mechanism is adopted in local identity model and identity establishment process depends on the credentials provided by the objects

Theses credentials are then compared with the similar detail stored in object registry/database.

Local scope of identity and flat addressing makes it simple.

Advantages of Local Identity

Manageability

As the central entity is responsible for assigning an identity, object registry can assign and
store identities based on its capacity.

But with increasing number of objects in scalable IoT networks, performance becomes bottleneck.

Flat Addressing:

As the scope of identity in local identity is local, flat addressing is useful for such systems
but it results into name collisions.

Disadvantages of Local IdM

Decision and action are more time consuming

Increased dependency and vulnerability

Greater number of objects that rely on one central registry causes problem of single point of failure.

More delay in response towards identity assignment and establishment as one central system is responsible for it.

Secrecy is hard to maintain as identities are stored at one central location.

Network Identity Management Model

- In distributed IoT networks, the classical and centralized mechanism does not suffice because of distributed nature of the device-to-device communication
- IdM is one of the main issues in IoT because such networks could be both distributed and dynamic in nature.
- In IoT each device will have to assume that arbitrary devices can establish direct, ad-hoc communication with it.

Network Identity Management Model

- This distributed nature of IoT leads to the concept of network identity.
- In network identity model, identity is authenticated to the network of devices rather than an individual host or entity.
- Once the identity establishment is done to the network, this identity will flow across the network providing services or resources without explicit identity establishment again.

Network Identity Management Model

- Thus, identity of an individual object will remain same in the participating network.
- Network identity models also have an ability to establish cross-network identity or in most of the cases network identity is confined to single domain.

Network Identity Management Model

- In IoT network A, identity is confined to one domain, while in IoT network B, identity is used across two IoT sub-networks.

Federated Identity Management Model

Identity federation is known within the web security world and refers to management of a network/web objects identity across different domains.

The main reason of enabling federation in network/web environment is that the work flow of system often requires an object for which identity is established in one domain to be established in other domain as well.

Identity in the web based system refers to a users identity while in IoT, identity refers to a device or "thing". Hence the interaction of identities in IoT is in the form of device to device communication.

Federated Identity Management Model

Federated Identity Management Model

Three IoT domains are considered i.e private user, retail shop and goods producer network and two IoT federated networks are considered.

There are different ways of accomplishing federated identity.

In federated networks, devices undergo single registration process.

If the registration is performed more than once, then redundancy of the profiles is to be avoided.

Different federation topologies

Local Profiling

Distributed profiling

Third party profiling

Local Profiling

All devices are registered with the IdM infrastructure of the local networks.

Profiles of these devices are entirely managed by local network and local identity management model is used for local profiling.

Eg- Smart home scenario.

Distributed Profiling

In this scheme, devices complete the registration process with the home IdM infrastructure and when needed new profiles of the same devices can be created in new network.

These profiles will be specific to new network due to need of new attributes.

Hence the profiles become distributed across multiple networks and attribute synchronization need needs to be taken care.

Third party profiling

In this scheme, the trusted third party within established federation is involved for creating and managing profiles.

This reduces the load from member networks from the registration.

Trust management is an important issue to be taken care in third party
profiling.

Advantage of this scheme is that it is scalable in nature and more and more IoT networks can be connected to trusted third party.

Global Web Identity

With the emergence of WWW and popularity of online social networks, global identity is a need today.

Web identity is uniquely identified throughout WWW and it is identifiable via URI (Universal resource identifier).

Due to increasing number of users on WWW and online social network, it is important to keep unique identity of users as well as services.

In context of IoT networks, web identity is ubiquitous in nature and web identity information should be capable of uniquely resolving various IoT networks

Device centric identitymanagement

Eg: Higgins is a software infrastructure that supports consistent user experience that works with digital identity protocols

Eg: WS-Trust, OpenID.

Main objective of Higgins project is to manage multiple contexts, interoperability, define common interface for an identity system.

The HIggins framework does not provide support for quantitative measure identity strength and lacks the fulfillment of defining strength of identity.\

Issue with security

Hybrid Identity management

- Deals with hybrid identities like user as well as device identities.
- In cloud computing, IdM is a hybrid cloud needed to deal with identities of both user
- and devices/services.
- Eg: the Liberty Alliance project is a federated solution for guaranteeing interoperability,
- Supporting privacy, promoting the adoption of specifications and providing guidelines.
- It is a framework in which domains that belong to a federation may exchange identity information about their users and devices using federated identities