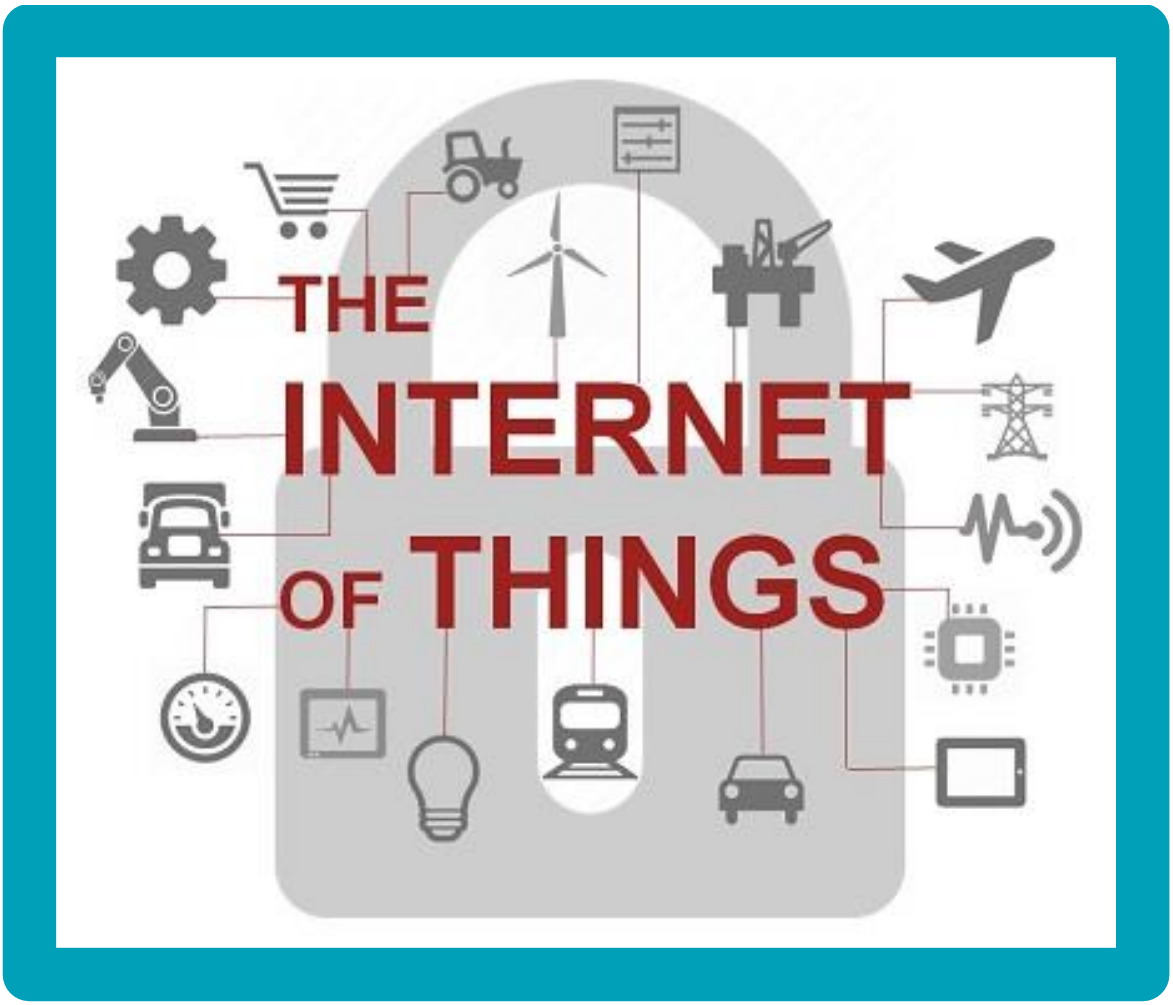
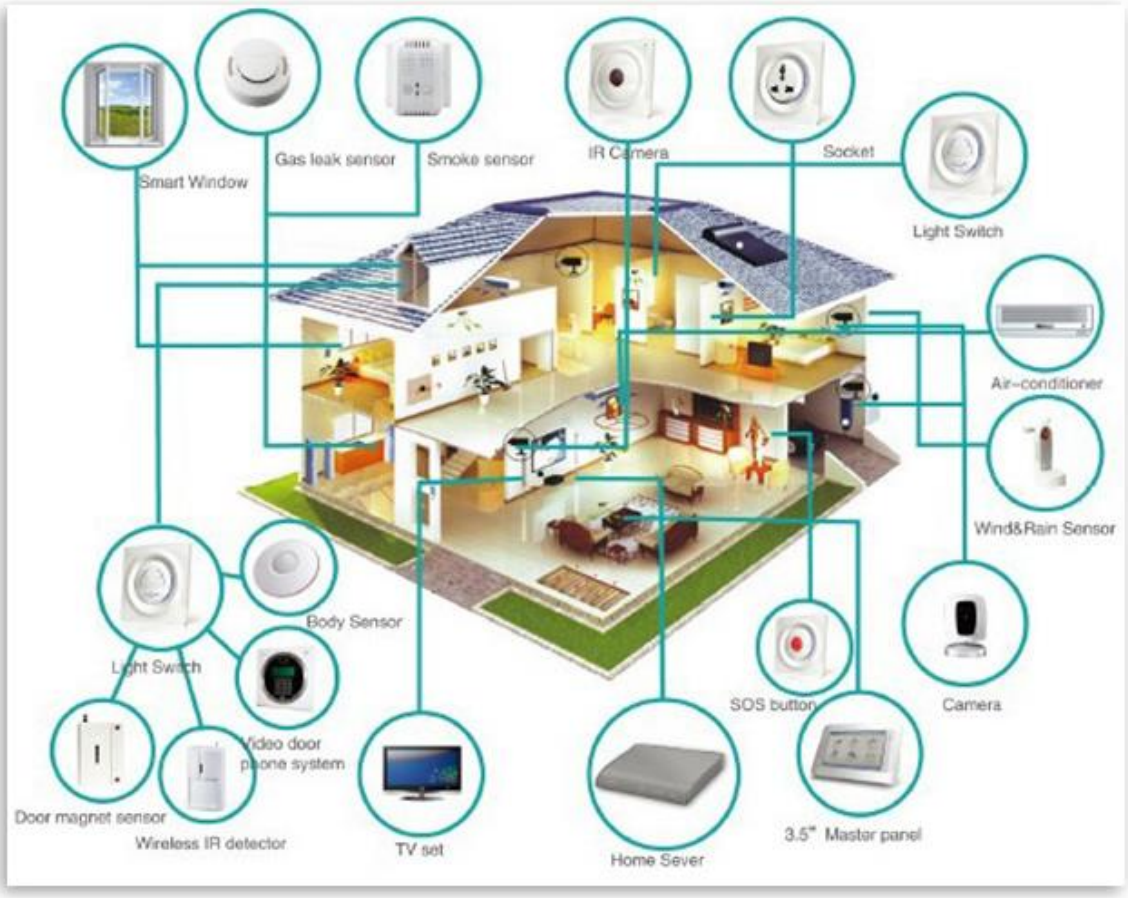


IoT Secure

Open architecture to provide security to and from IoT world

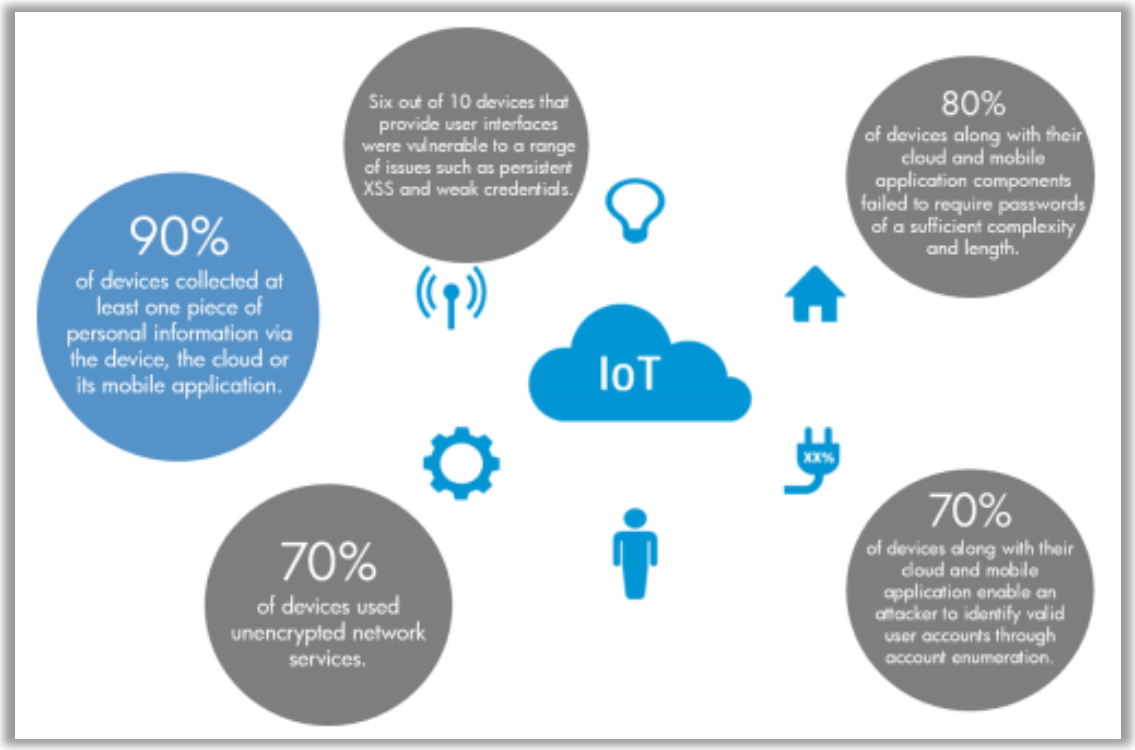
IoT secure | IoT Security | November 8, 2016



Internet of Things

IoT devices are increasing rapidly these days with 10 billion devices currently deployed and expected to reach 50 billion by 2020. We all know why we use them and how awesome these are!!!

Current Vulnerabilities



Most of currently IoT devices have vulnerabilities like Username Enumeration, weak passwords, unencrypted services, weak authentication of network devices. Also, these lack software updates, making these obsolete devices susceptible to newly found vulnerabilities. An average of 19 vulnerabilities per day were reported in 2014, according to the data from the National Vulnerability Database (NVD).

As good IoT devices are, because of these security issues, they are also proving troublemaker for internet. Low computing and power profile make it harder to deploy complex security measures on them.

Implications: IoT World

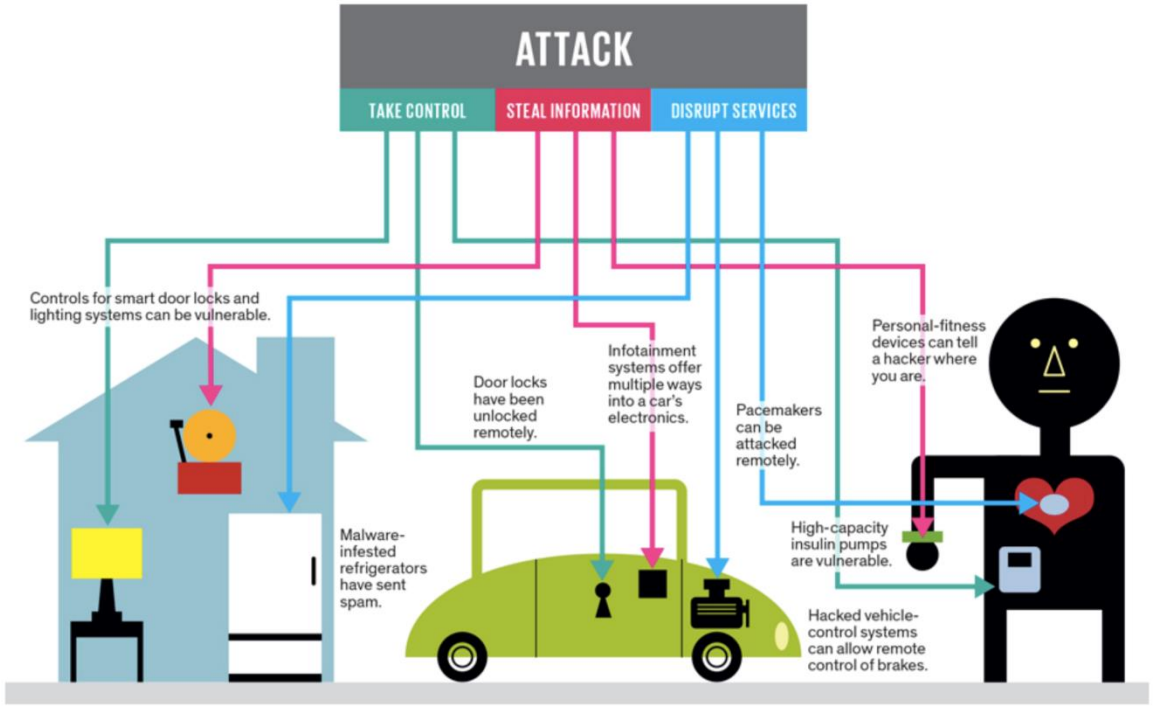
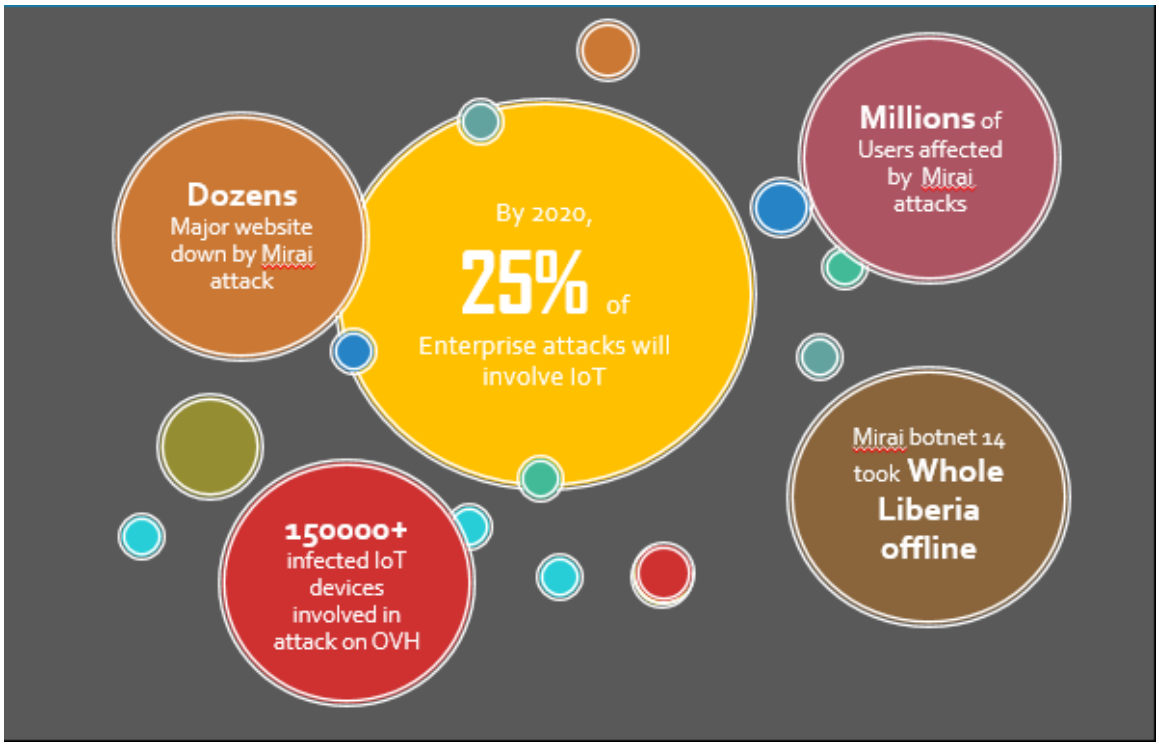


Illustration: J. D. King

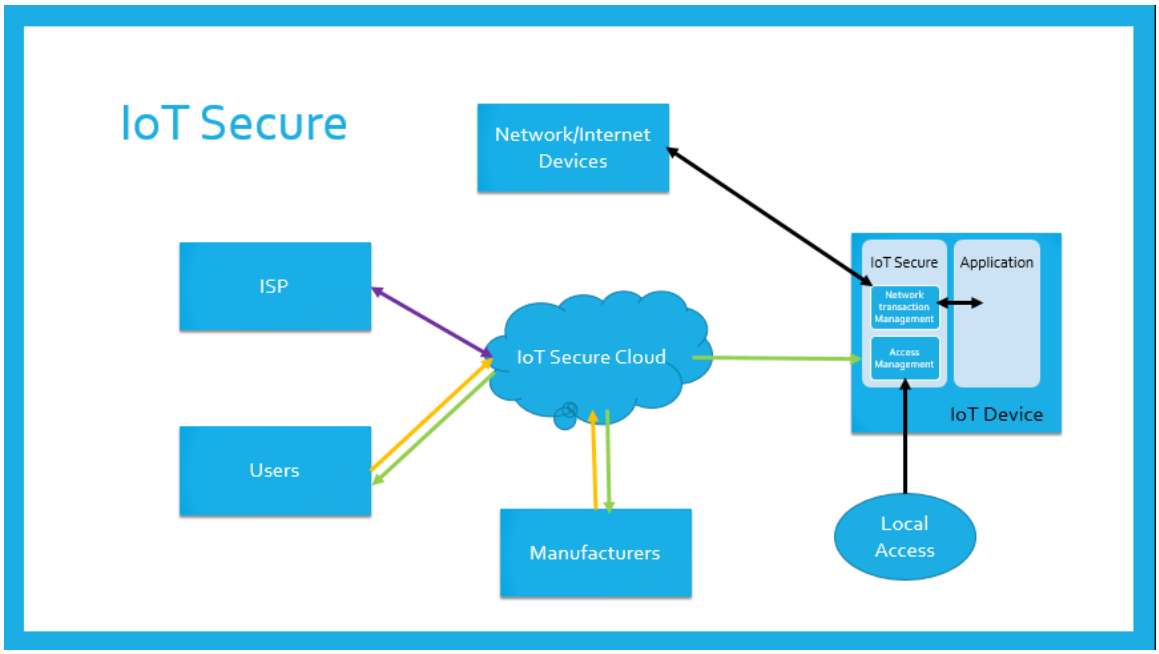
Security vulnerabilities on IoT Device can result in serious harm to IoT Device or device users as depicted above.

Implications: Rest of Internet



Because of these unsecured devices, connectivity of all devices to unified internet has become weakness, debilitating other, albeit secure but compute/bandwidth limited, server and devices. Recently, 1 million devices were hacked and utilized for DDoS attack on security researcher Brian Krebs blog. It has baffled the security experts as this problem will drastically increase over coming years. There are some solutions like Google Project Shield but neither mitigate the security issue of IOT devices nor protect rest of internet, only selected ones. We are presenting an open source solution, IoT Secure, to handle this problem.

IoT Secure Architecture



IoT Secure uses multiple levels of security to provide unprecedented security to IoT devices while maintaining very low compute requirement profile to enable it to be adopted at all range of IoT devices. A powerful IoT Secure cloud handles all authentication of users. Using secure channels and random keys, it mitigates default password, dictionary attack problems. Authenticated user is provided one-time usable random key to access the device. Device-end IOT Secure enables device to communicate device with all network devices without cloud intervention and employ several checks to detect aberrational behavior. Still, if any vulnerability of IOT device, because of loophole in IOT device application or even IoT Secure, slips by and hacker is able to use them for initiating DDOS attack, IoT Secure Cloud, monitoring all online DDoS attacks, will be able to identify the pernicious devices, neutralizing them with help of ISP, and apprising both manufacturer and device owner of IOT device. See the "How it will work" for more detailed version.

Features

IoT secure architecture consists IoT device firmware for IoT devices and complementary IoT Secure cloud for monitoring, accessing and controlling IoT devices.

IoT Device Firmware

IOT Device firmware is highly secure and feature rich firmware while maintaining very light footprint which is achieved by shifting some of responsibilities of device to IoT secure cloud. Following are the feature supported by IoT Firmware:

- Device authentication and registration on IoT Secure cloud

- Whitelist based continuous network traffic monitoring to and from IoT device
- User access management system
- Anomalous behavior reporting
- OTA update management (optional)
- Communication establishment mechanism for IoT device behind the NAT (optional)

IoT Secure Cloud

The cloud provide interface for monitoring and controlling all IoT devices. It also monitors web for active DDOS attacks to help mitigate them.

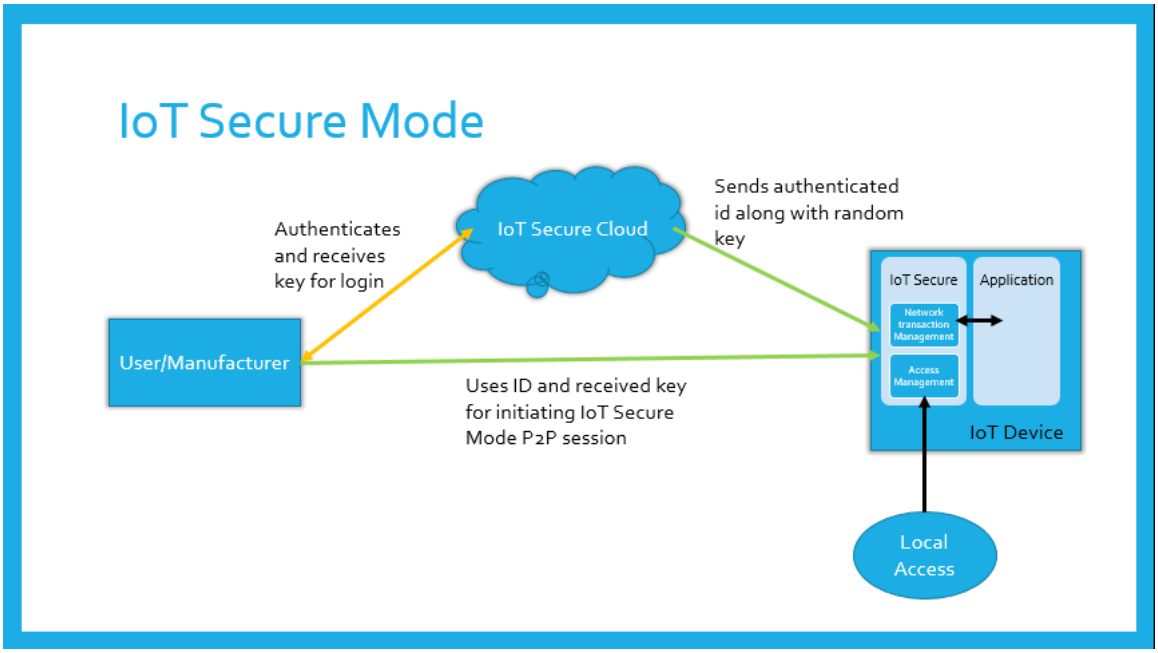
- Interface to monitor and control IoT devices
- User authentication for accessing device
- Secure and Nonintrusive P2P communication establishment between user/third party server and IoT device
- IoT device status reporting to device users/manufacturers.
- Monitor and analyze reported anomalies from IoT devices, notify Users/Manufacturer/IoT Devices.
- Monitoring of active DDoS attack on internet and help ISP mitigate them.

Working

Endpoint Authentication

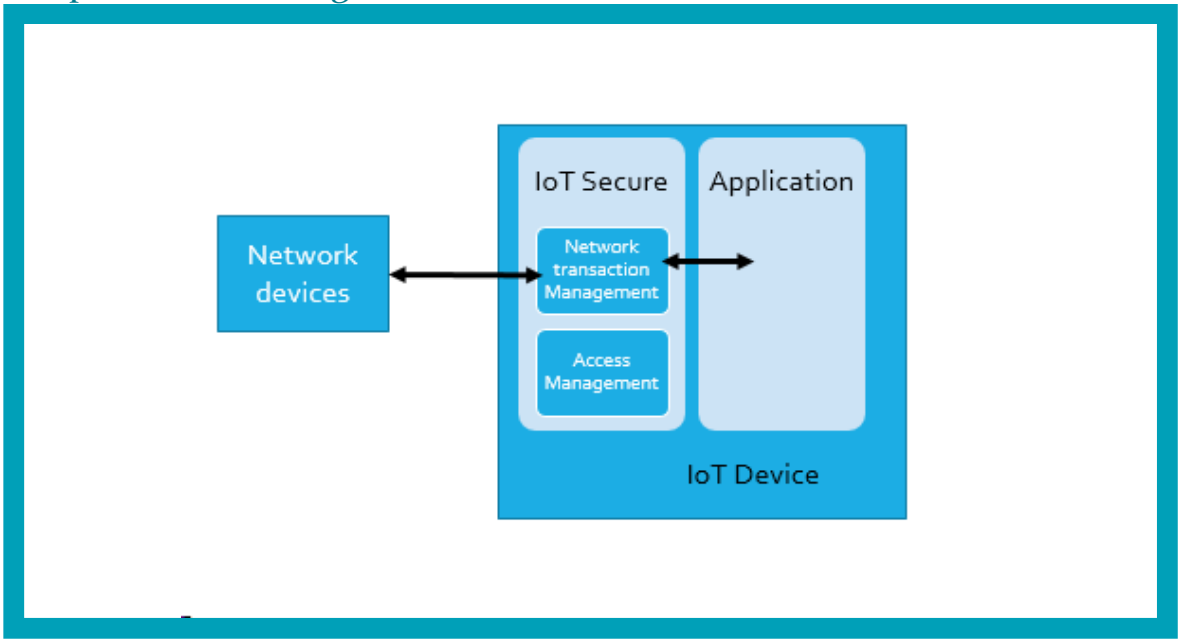
- IoT Device will be registered on IoT Secure Cloud with authentic client IDs (Manufacturers/Users). It will be provided unique id for identification, authentication key for validation of IoT device, random backup key for local only user access to device. Any reconfiguration must be done through IoT secure mode.
- On every boot up, IoT device firmware will establish secure connection with IoT Secure cloud, register itself using its Unique ID and authentication key and then validate application signature against the cloud.
- On any update or configuration change, device will update IoT Secure cloud.

User Access Authentication



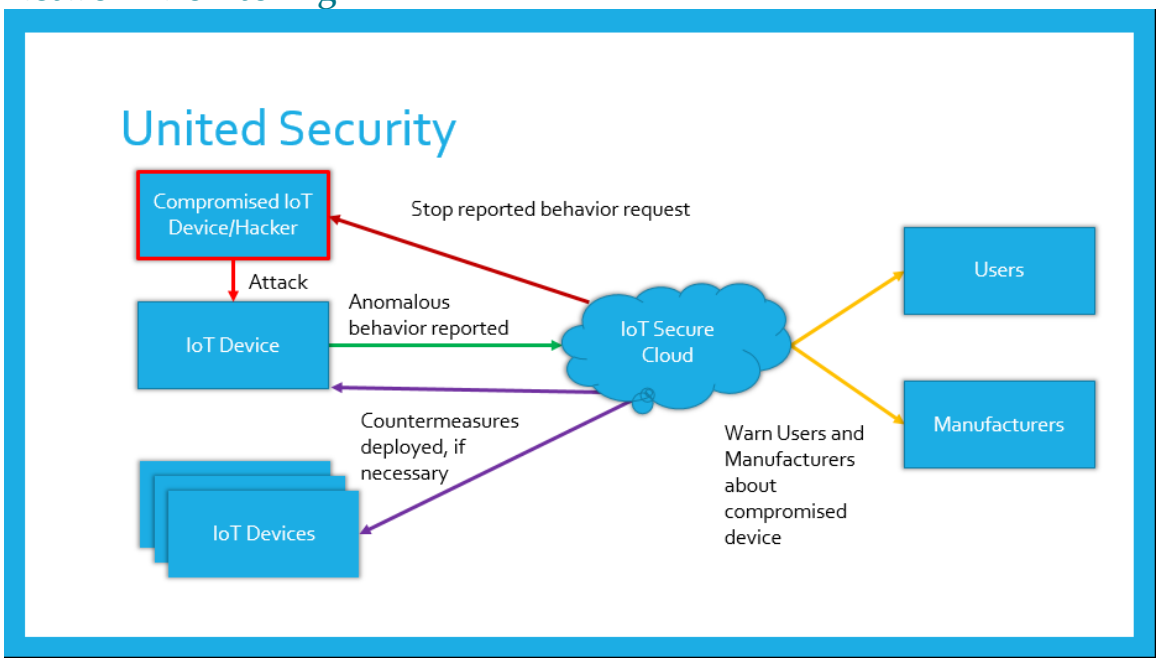
- Manufacturer/User can access the device through internet via authentication from IoT secure cloud. Manufacturer/User will provide unique id of IoT device to IoT Secure cloud and then will be authentication using OTP or email.
- Once authenticated, IoT Secure Cloud will pass user's metadata containing user id, permission level and randomly generated key for user verification to IoT Device. Also it will pass IoT Device metadata, containing IP location and the random key, to user. As key is randomly generated at each login request, it will be one time usable and also time bound.
- User will use IoT device location and one-time usable key to login to device. IOT secure cloud will be bypassed and secure P2P communication will be established. User will now be in IoT secure mode and can do reconfiguration like add/remove other user, renew backup key as well as updating application, based on login permission level.
- Only local device access, for device which is isolated from internet, backup keys can be used to access IoT-Secure mode.

Endpoint Monitoring

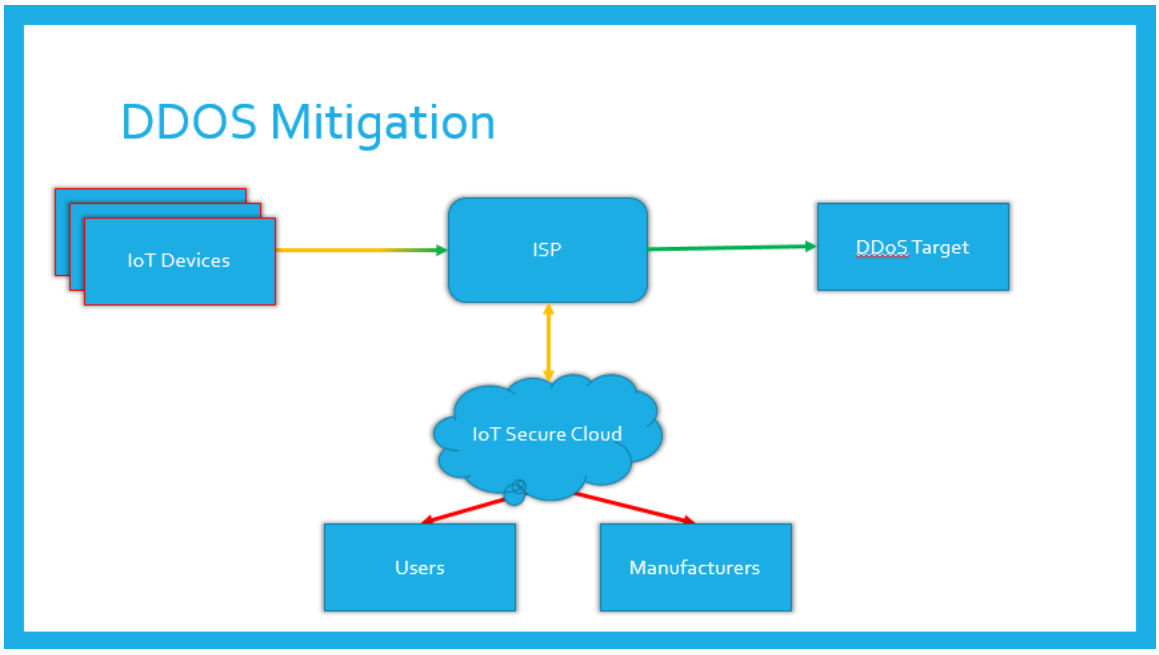


- All application specific transaction, which don't require IoT secure mode access, can be directly established between IoT device and Internet world. These can be restricted via allowed senders and receivers list.
- Allowed senders and receivers list can only be updated via IOT secure mode login to IoT Device. These transactions should not be able to configure or update device.
- Any allowed device can have transaction to or from IoT device application directly without involvement of IoT cloud or Internet.
- Any unwarranted transaction will be reported at IoT Secure cloud, as described in next section, and will be dropped.

Network Monitoring



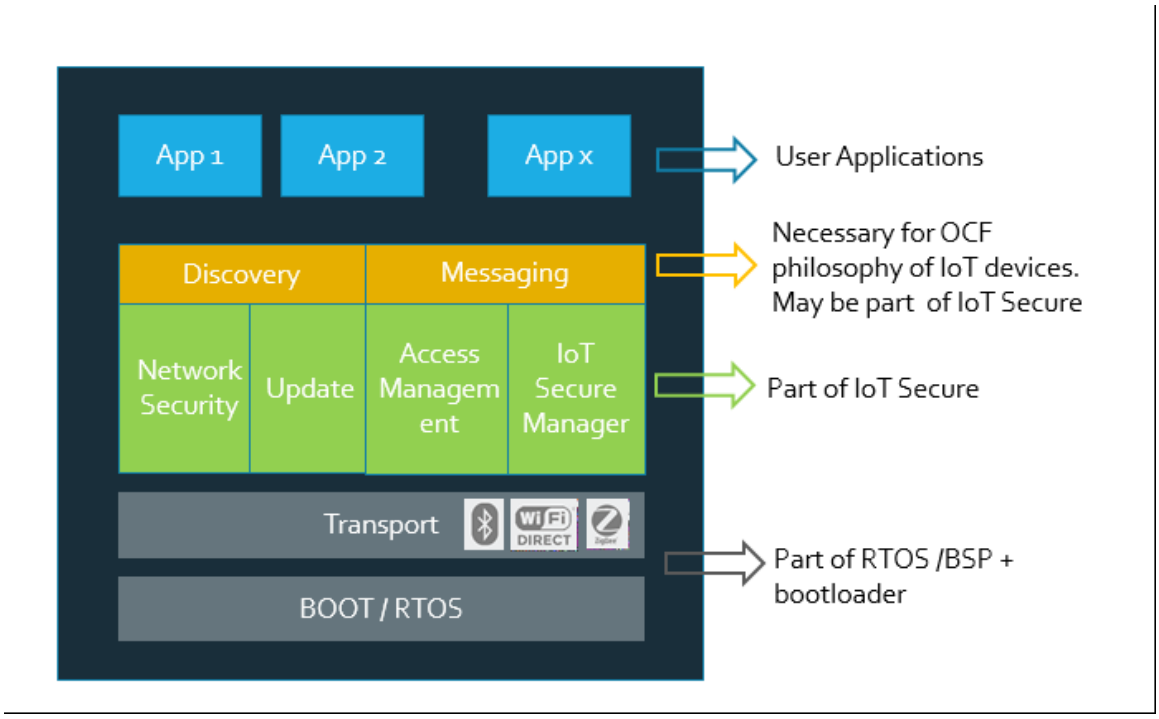
- IoT Device will report anomalous behavior of self or other devices to IoT Secure Cloud. Anomaly can be detected by network transaction monitoring of IoT Secure firmware or reported by App running on IoT secure.
- IoT Secure Cloud will analyze the anomaly report and will determine whether course of action is needed.
- On determining enough confidence on report, IoT Secure can alert the user and manufacturer of both attacker and target devices and even deploy countermeasures on susceptible IoT Devices like adding attacker to blacklist to block at transport layer itself.



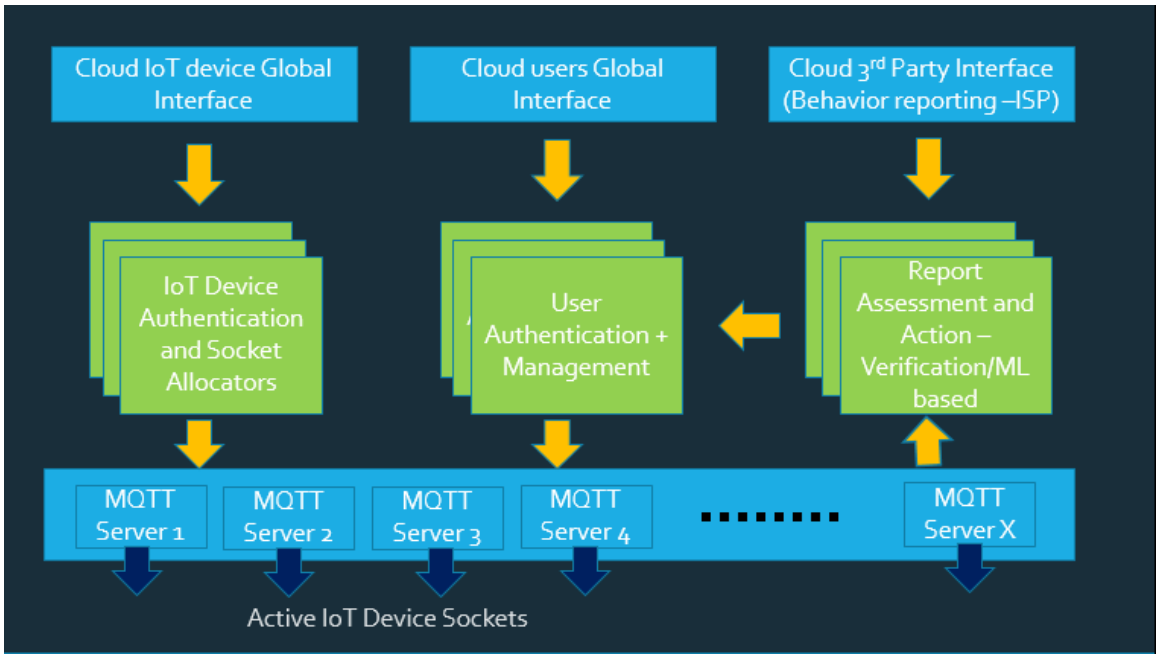
- IoT Secure Cloud will constantly be in sync with ISP for DDoS attack identification and mitigation.
- It will receive list of devices which are engaging with DDoS victim, and will identify compromised devices by analyzing the list with IoT secure database by using machine learning techniques or checking their types and other factors and report back the list of compromised devices to both ISP and IoT device manufacturer/users.
- ISP can drop the packet from devices and will thus will debilitate the DDoS attacks
- IoT device owner/manufacturer be aware of this level 3 vulnerability, which would have otherwise gone unnoticed and will patch them.
- It will help mitigating DDoS attacks as well as exposing compromised IoT devices

Design

IoT Secure Firmware



IoT Secure Cloud

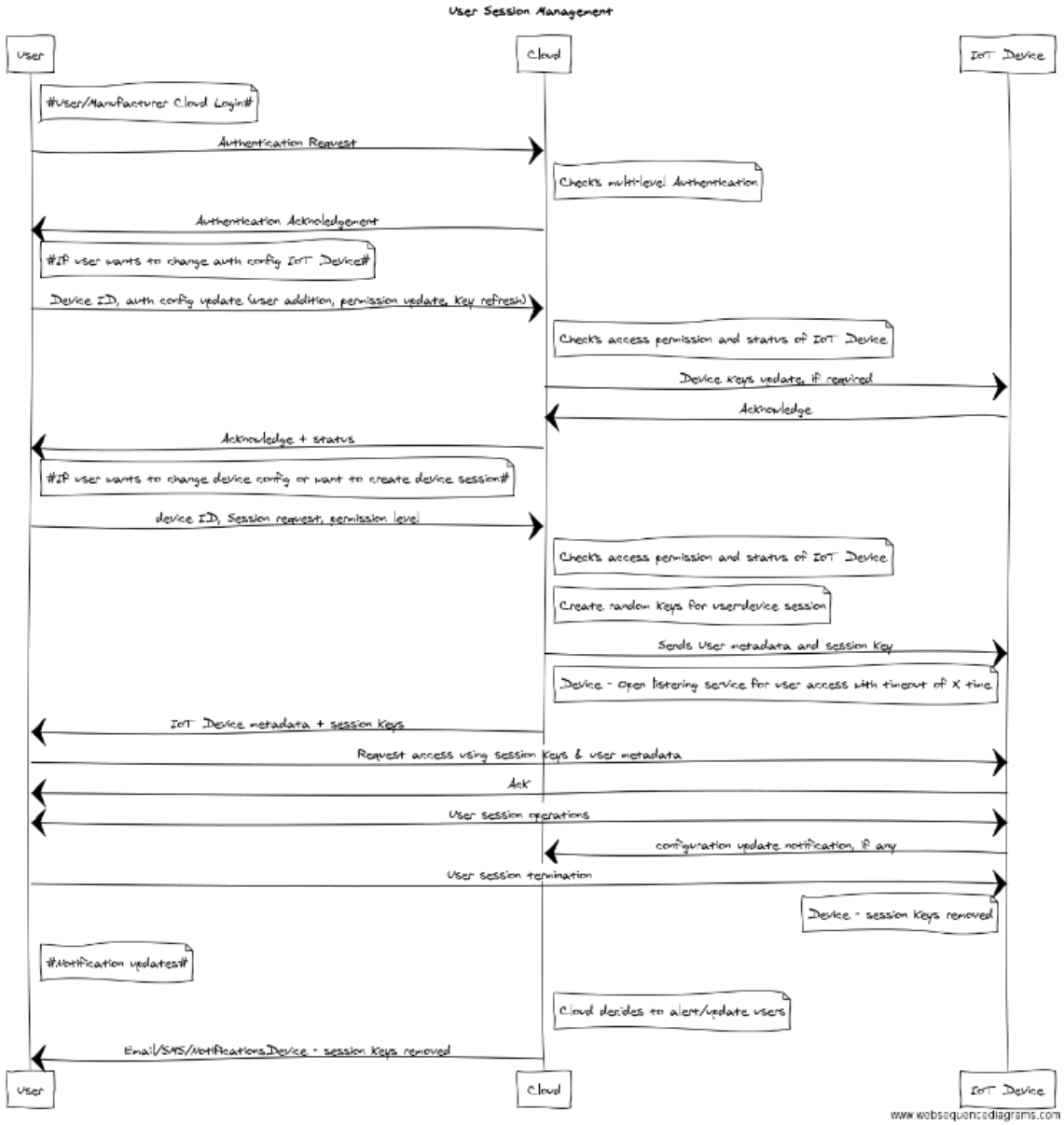


Communication Protocol

Once IoT device is programed by manufacturer, every communication between any of entity, e.g. between IoT Device, Users, Manufacturer and IoT Secure cloud will be secure and encrypted, with both endpoint authenticity confirmation and free from eavesdropping and man in middle attacks.

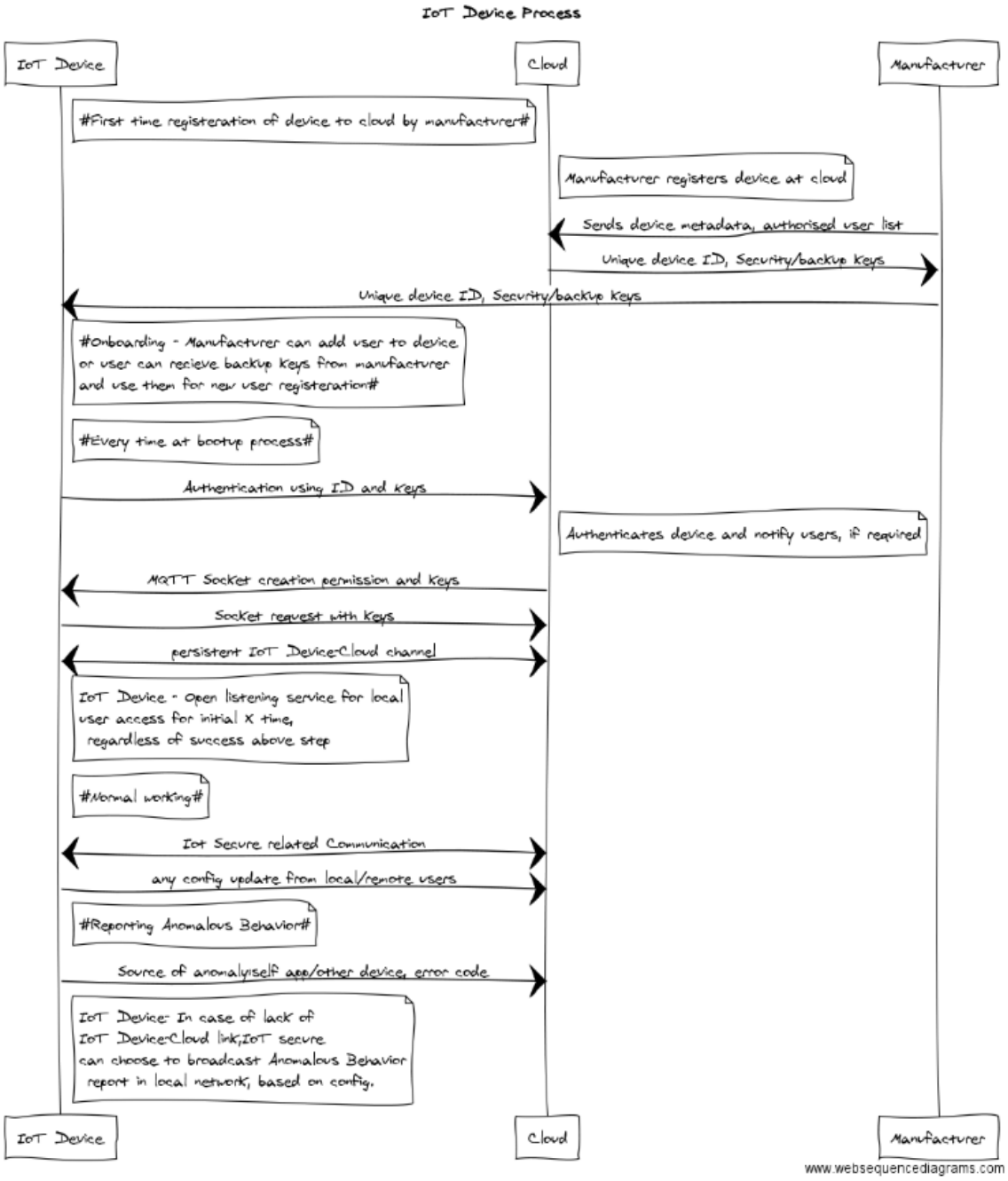
User and IoT secure Cloud Communication

Source	Target	Purpose/Content	Encryption	Source Authenticity
User	Cloud	Authentication, Device access, Device config updates	Cloud public keys	Multiple level authentication (oauth, email, OTP)
Cloud	User	User request reponse, Device notifications via Emails, SMS etc	User Session keys(user public key for email)	IoT Secure Cloud certificate



IoT Device and IoT secure Cloud Communication

Source	Target	Purpose/Content	Encryption	Source Authenticity
IoT Device	Cloud	Authentication, IoT Secure Socket, Device config updates, status, Report anomaly	Cloud public keys	Device authentication keys (preprogrammed)
Cloud	IoT Device	IoT secure commands, queries	Device authentication keys (preprogrammed)	IoT Secure Cloud certificate



IoT Device and User Communication Protocol

On the request from user, IoT secure cloud will help to establish P2P based or relay based secure communication link between device and user. It will also pass device the authentication keys and permission level of user so that user can only do what he is intended to be.

Channel

- P2P (for direct as well as hole punching)
- Bridge – For devices which are behind NAT and P2P communication can't be established, using 3rd party bridge service, secured channel can be established. As only

endpoint have encryption keys, bridge can't decode messages between them. User can specify through which bridge he wants to connect. Cloud will relay bridge location to IoT device for user session.

Permission

User	Firmware update	Application Update	User Addition	IoT Secure device Network configure	Application port 1	Application port n
User 1 (Manufacturer)	x	x	x	x	x	
User2 (IoT owner)			x	x		x
User n						x

Communication

Source	**Target**	**Purpose/Content**	**Encryption**	**Source Authenticity**
User	IoT Device	Device updates, Device application access	One Time Session Key(Provided by Cloud)	User Metadata, Session Authentication Key
IoT Device	User	User request reponse, Application responses etc	One Time Session Key(Provided by Cloud)	Device Metadata, Session Authentication Key

IoT Device to IoT device Communication Protocol

Iotivity, Alljoyn??

Sample Applications

Few application trying to demonstrate how flexibly IoT secure can be used:

1. **Few user controlling IoT Device, no cloud processing necessity**–

   Register user's mobile/web app as user on IoT Secure Cloud with application level access only, so that user's app can only talk to device, not modify. Now, on application request, IoT Secure will establish secure link between IoT device and user app and user app can gather or send data to IoT device application. No need to setup additional server by manufacturer to provide remote access.

2. **Many users / cloud logging or processing required**-
   Manufacturer will register the application server, which he is using for data logging /processing/user management, as user on IoT Secure Cloud for IoT Device with

application level access only. Application server can now connect with IoT devices securely, process data and serve its users.

3. **Independent IoT Secure Cloud –**
   If manufacturer desires, It can setup own IoT Secure Cloud as Implementation open source. Its devices will still be able to operate with other devices locally as discovery and message layers, above IoT Secure, will be same for all devices as in compliance to Open Connectivity Foundation. However, this is not encouraged as usage of single cloud strengthen security as it will have bigger database for device reported/DDOS threat assessment and help user to maintain all device from same location.
4. **Private network operation, No internet connectivity–**
   IoT Secure Cloud is necessary for two task – Better authentication of user and managing network based security. If connection to cloud/Internet is not present, IoT Device can be configured to work normally. Authentication must be carried out using backup keys, which can be downloaded by user from IoT Secure cloud portal, and Network security is compensated by broadcasted anomaly report on IoT Secure local network.
5. **Device Factory Reset functionality-**
   Manufacturer can opt to only retains IoT Secure Firmware and Authentication Keys. On factory reset, when device will establish connection with IoT Secure Cloud and send configuration to cloud, cloud can alert manufacturer on configuration change and manufacturer can automatically upload latest firmware and application set as determined by device id.
6. **Very Small Footprint Device-**
   IoT Secure Firmware should be very lightweight as user authentication and management is shifted on cloud side and security is simplified as devices already have keys before session instead of TLS based handshaking. But, leveraging modular approach, image can still be stripped by stripping some modules and disabling these functionalities from user. For example, one implementation might support only one application and merging both application update and firmware update under firmware update, to reduce IoT firmware size and disabling these functionalities from user account. As per IoT Secure cloud, user can never perform these operations due to lack of permission, so lack of implementation wont effect it.

Availability

Platforms

Not much sure, my thoughts-

Linux, Zypher, Arduino, Hardware based??

If we will be able to develop very lean image based on Zypher and extended it to feature rich IoT Secure module implementation on linux, people can should be able to use for high variety of application. Zypher based implementation on small chip with serial lines for application communication to can even make hardware implementation with network connectivity and IoT Secure.

Brillo, windows based and others can follow??
If we take precaution of modularity and platform independence in above, corresponding teams might be able to provide modifications and updates for them.

Users

It might provide security to few IOT devices, to effectively strengthen IoT world and thus internet, this must be adopted by all IOT manufacturer, from small to large. To encourage it, IoT secure is open architecture and will be developed open source. All small scale manufacturer and users will be provided free cloud services. But, large manufacture can be charged minimally to sustain cloud and development cost.