



SafeHaven

IoT Personalized and Secured

Subhash Gutti
Harish Gowda

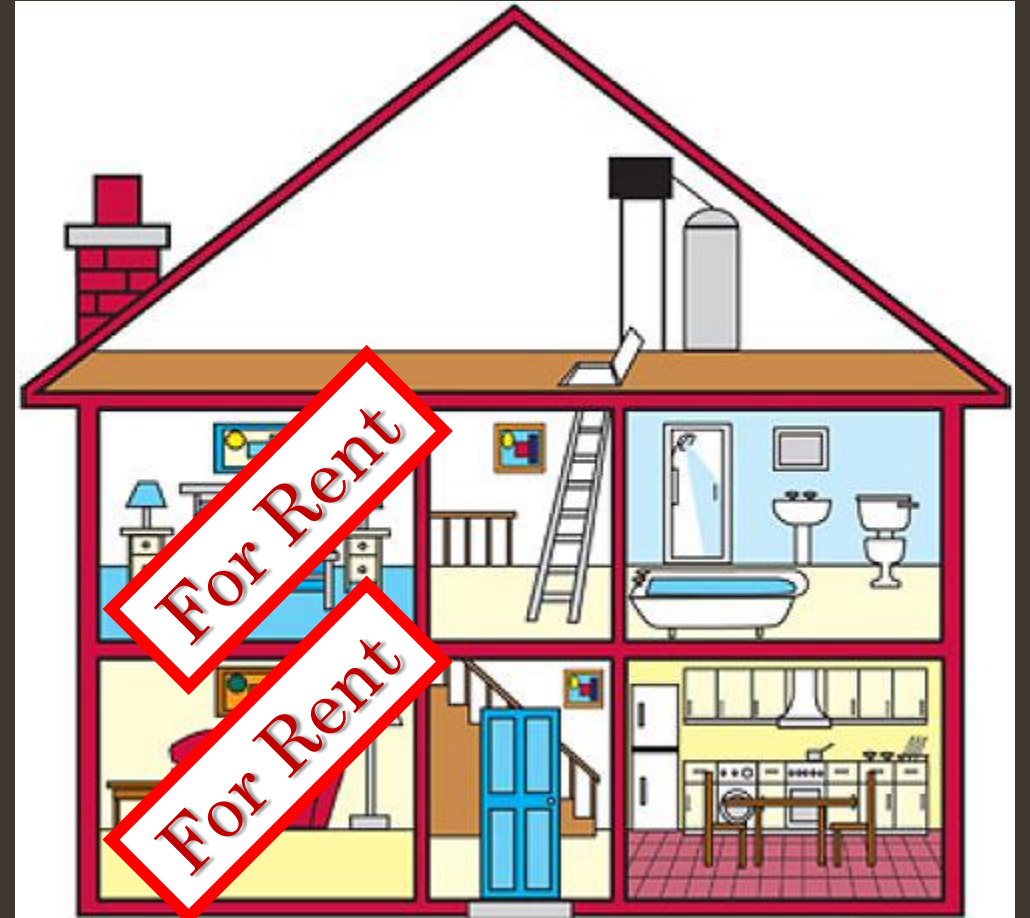


Use Case

Sophie owns a 3 bedroom home. Her contractor convinced her to automate her whole house with IoT devices. Sophie listed 2 bedrooms for rent.

For IoT devices, Sophie used to

- Share her access credentials with new tenants
- All IoT devices in her home were accessible to everyone
- Sometimes devices were accessible even after tenant's departure



ars TECHNICA   [SIGN IN](#)

RISK ASSESSMENT —

“Internet of Things” security broken and getting worse

Hacker News

[new](#) | [comments](#) | [show](#) | [ask](#) | [jobs](#) | [submit](#)

▲ Say Cheese: a snapshot of the massive DDoS attacks coming from IoT cameras (cloudflare.com)

▲ riskable 13 hours ago [-]

I've been warning about this kind of thing for *years* and years. Both professionally and in my personal life. On forums and anywhere people will listen...

IoT is a security disaster

I hate to suggest things like this but we may need *legal* remedies to solve the problem before it becomes an Internet Zombie Armageddon (IZA). It's *that* bad.

There's going to be *tens of billions* of IoT devices installed at businesses and homes in just a few short years. If they're not receiving regular, timely security updates the Internet as we know it may just plain collapse from the sheer weight of all the zombies.

I propose a mandatory "nutrition label" of sorts for IoT device packaging. Something like this:

- * Updates itself regularly
- * Conforms to NIST security standards
- * **Public penetration test results:** <https://ptr>
- * **Shares data with 3rd party:** No
- * **Administration by vendor:** No
- * Requires Internet connection to administer: 1
- * **Requires 3rd party service to function:** No
- * **Notifies of intrusion:** Yes
- * **Logs all access:** Yes
- * **Encrypts all network traffic:** Yes

Something like a publicly-posted penetration test would be incredibly valuable. Especially if it was performed after each update of the device and at regular intervals. Even if it was an automated test (which in theory could be 'gamed') it would still be better than what we have now which is *nothing!*

11 Oct 2016 by [Marek Majkowski](#).

iously ignored, has
issue of high

TE

Additional challenges...

Multi User Management

Concurrent Controlled User Access

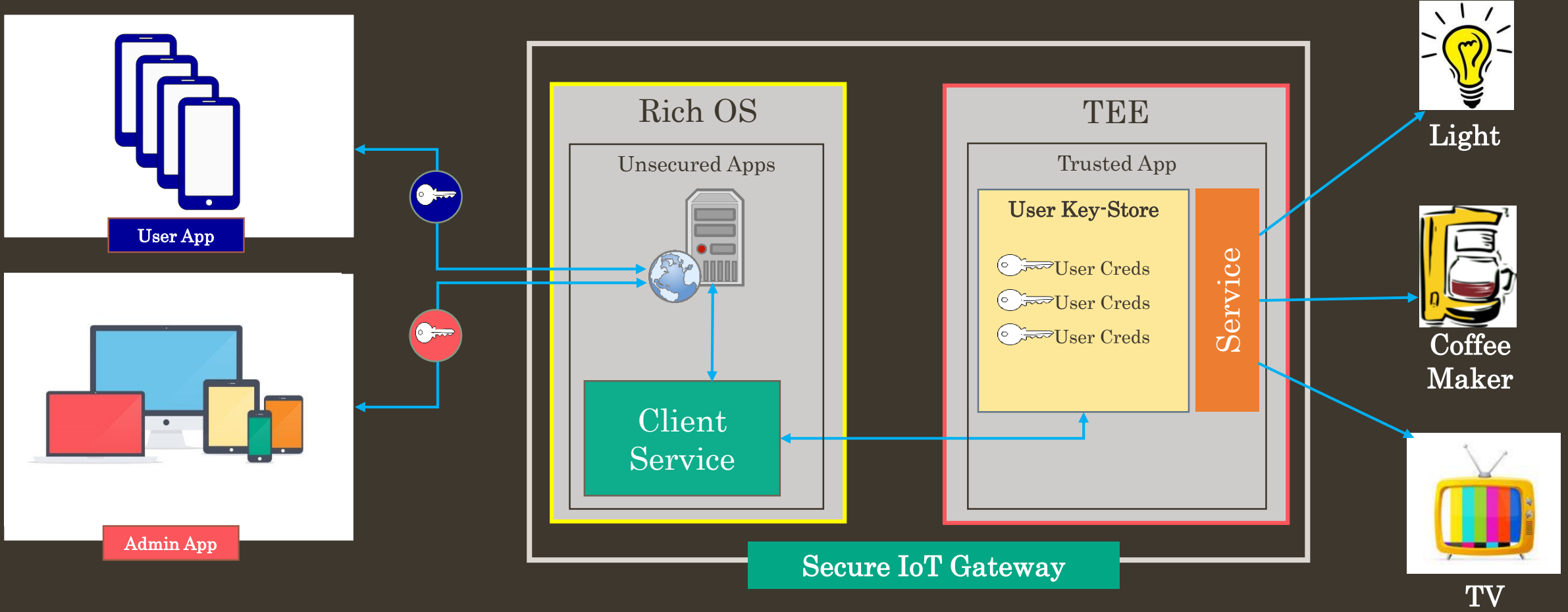
Personalization

The logo for SafeHaven, with 'Safe' in blue and 'Haven' in green, set against a white rectangular background.

Solution


- Easy user management.
- User Profile Information protection via TEE (Trusted Execution Environment).
- Encrypted communication between users and devices.
- Unique and encrypted IoT commands (replay attack safe).
- Secure & dynamic access control to the services exposed (for administration).
- Options to automate access control.

Architecture



User Interface

Administration

SafeHaven 

Registration

Name

Email Id


Phone Number

Password

Password Again

Public Key

Register


SafeHaven 

Login






Name


Password

Login

SafeHaven 

75°

-  Light OFF
-  Coffee maker OFF
-  Television OFF
-  Air Conditioner OFF
-  Bed Massager BUY

Administration 

Sophie	
Light	Admin Access
Coffee Maker	Admin Access
Television	Admin Access
Kevin Revoke All	
Light	Allowed
Coffee Maker	Deny
Television	Deny
Clint Revoke All	
Light	Allowed
Coffee Maker	Deny
Television	Allowed

Market Opportunities

Analysts predict

up to 30 Billion wireless devices

will be connected to the IoT by 2020 *

Gartner Says a Typical Family Home Could Contain More Than

500 Smart Devices

by 2022 +

* https://en.wikipedia.org/wiki/Internet_of_things

+ <http://www.gartner.com/newsroom/id/2839717>

Scalable Solutions

Hospitals

Hotels

Offices

Next Phase

Develop the framework and SDK.

Customize solutions to different industries (hotels, hospitals, homes etc)

Custom solutions for Hub and individual device form factors.

We thank GlobalPlatform & sponsors for providing us the opportunity and helping us in developing this solution

- Harish & Subhash