



TÉCNICO  
LISBOA



inescid  
lisboa

INFOBLENDER

HASLAB/INESC TEC  
& MINHO UNIVERSITY

SureThing:  
device location  
certification for  
the IoT



[Miguel.Pardal@tecnico.ulisboa.pt](mailto:Miguel.Pardal@tecnico.ulisboa.pt)

INESC TEC, December 3<sup>rd</sup>, 2018

The slide features a decorative background of curved lines in shades of gray, some solid and some dashed, sweeping across the top and sides. A blue speech bubble shape is positioned on the left side, containing the word 'Outline'.

## Outline

- **Short career summary**
- **Research context**
- **SureThing project**
  - **for Mobile devices**
  - **Ongoing work**

## Career steps



- LEIC 2000
  - **Personal Information Server**  
(*feeds*)

- MEIC 2006
  - Web Services **Security**  
(*digital notary*)



- DEIC 2014
  - Scalable & Secure RFID Discovery  
(*supply chain traceability, IoT*)



- Post-doc/sabbatical 2017
  - **Private** communication middleware  
(*multi-cipher, multi-path communication*)

Distributed  
Systems Group

- **Security & Privacy**  
in the new *frontiers* of  
**Information Technologies**  
and **Computer Science:**
  - **Internet of Things & Cloud**



Security &  
Privacy

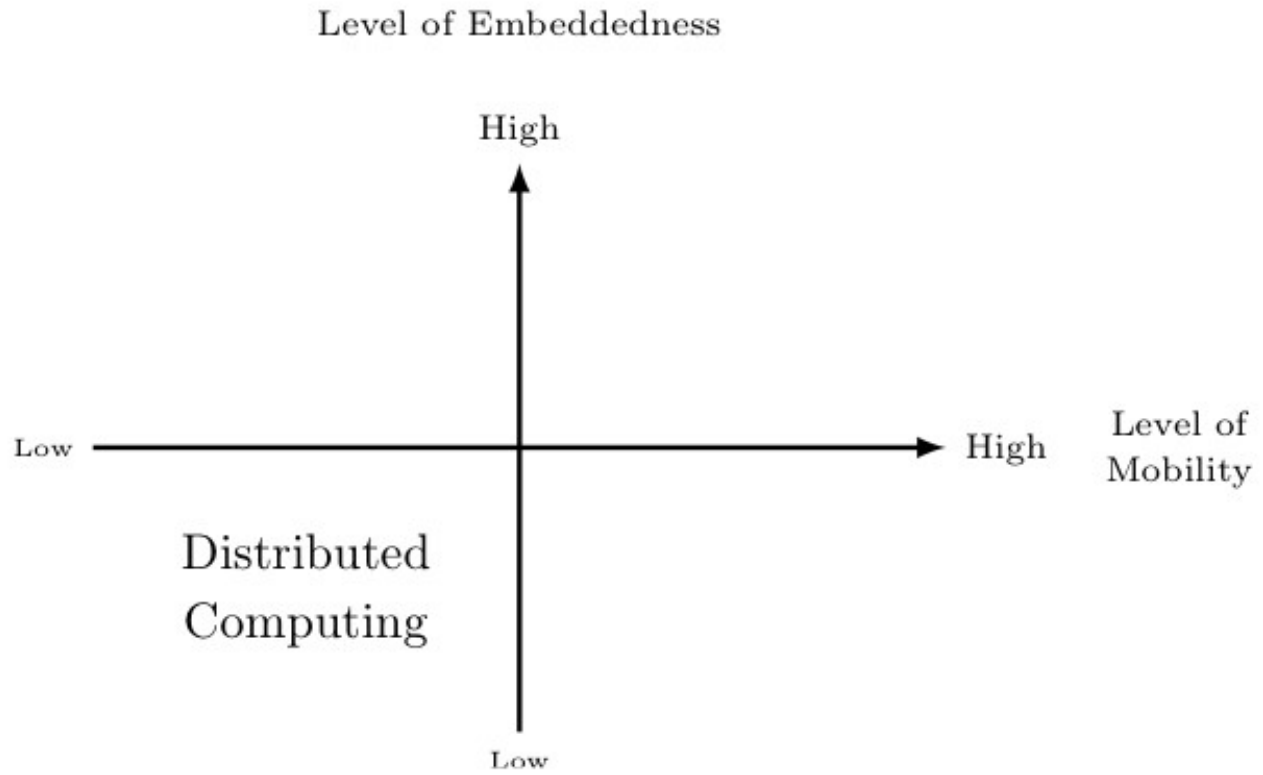
Digital  
Citizenship

- **CIA properties:**
  - Confidentiality
  - Integrity
  - Availability
- **TIU properties:**
  - Transparency
  - Intervenability
  - Unlinkability

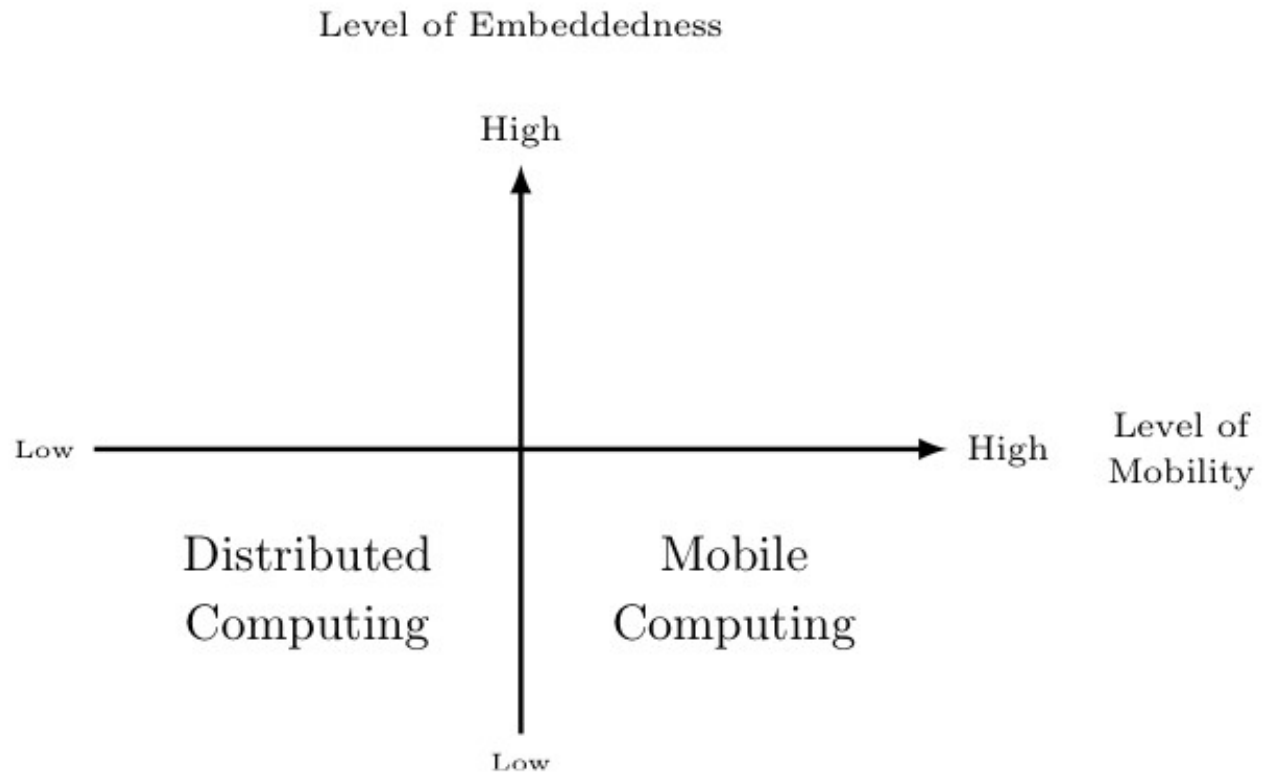


Research context

From *distributed*  
to *ubiquitous*  
computing

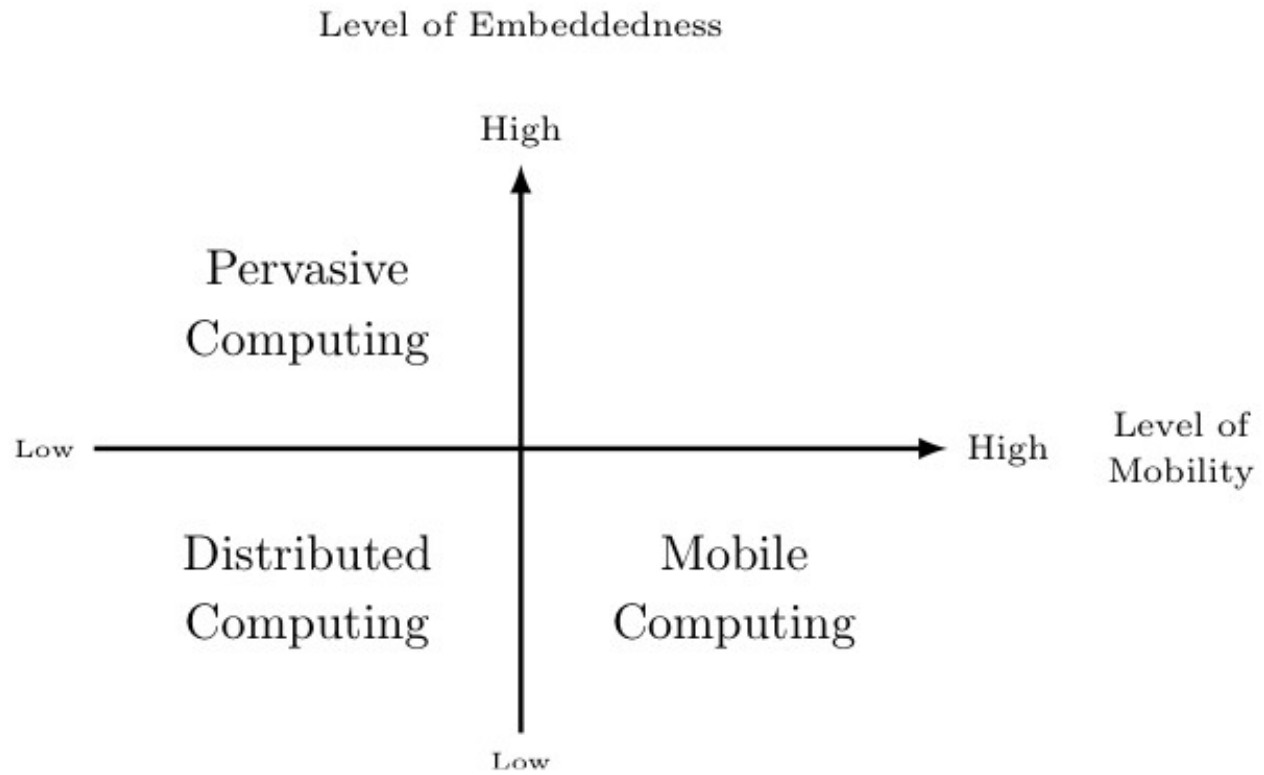


From *distributed*  
to *ubiquitous*  
computing



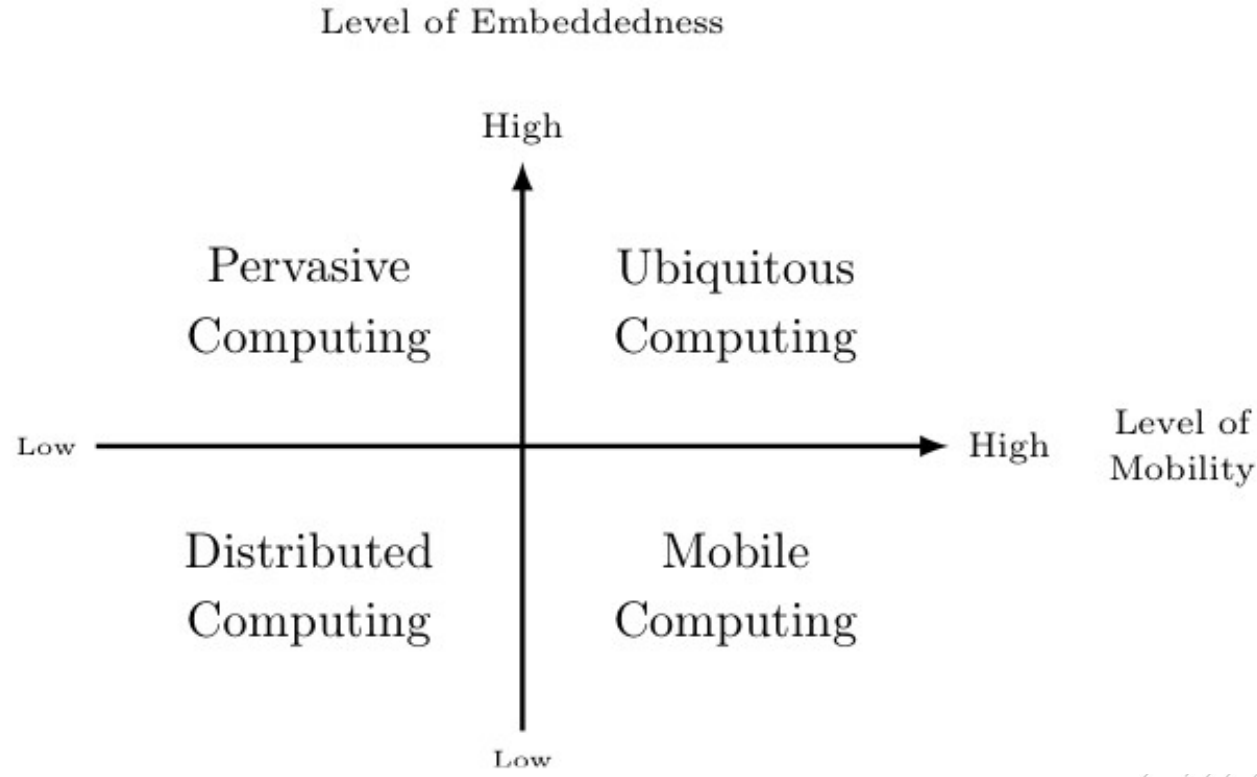


From *distributed*  
to *ubiquitous*  
computing



From *distributed*  
to *ubiquitous*  
computing

Figure credits: Marc-Oliver Pahl



# Smart Spaces

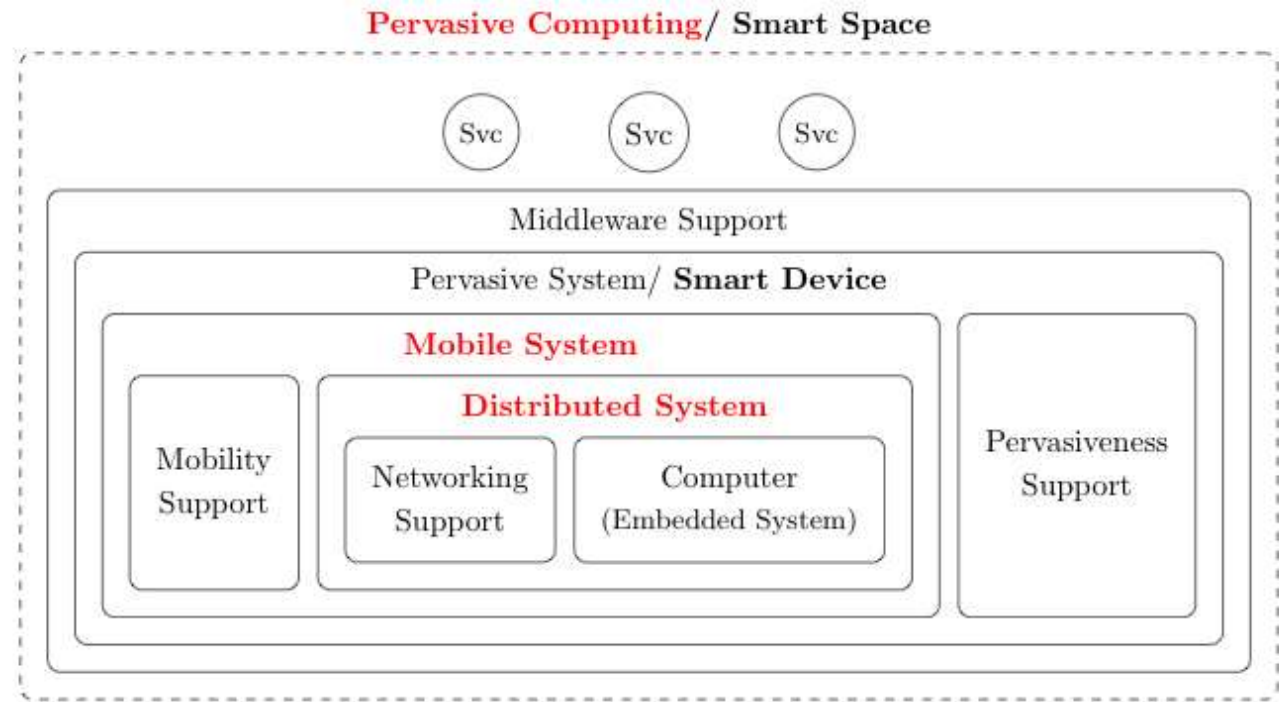
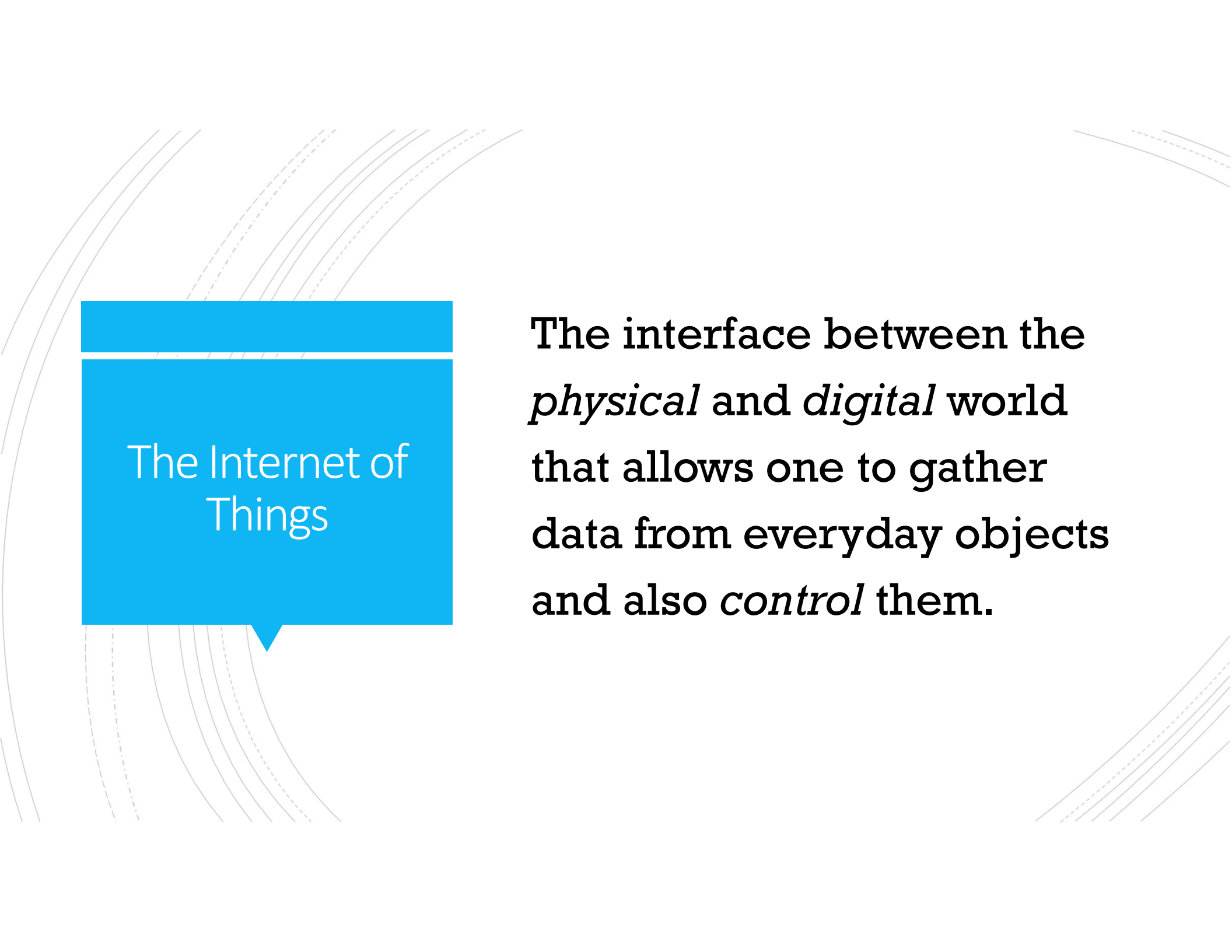


Figure credits: Marc-Oliver Pahl

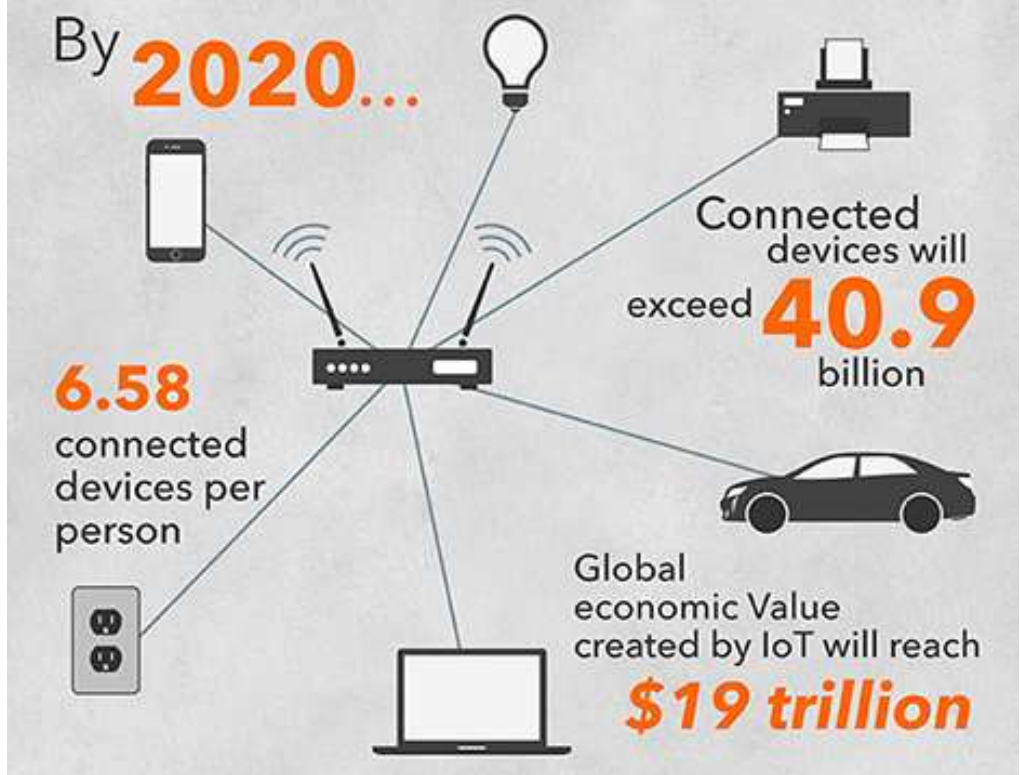
The background features several sets of curved lines in light gray, some solid and some dashed, creating a sense of motion or connectivity. A blue speech bubble shape is positioned on the left side, containing the title text.

## The Internet of Things

The interface between the *physical* and *digital* world that allows one to gather data from everyday objects and also *control* them.

# Device growth

Figure: IBM



Electronic  
business



# Augmented reality



# Hyper-reality

Concept video by Keiichi Matsuda:  
<https://vimeo.com/166807261>





Hyper-reality  
(turned off)

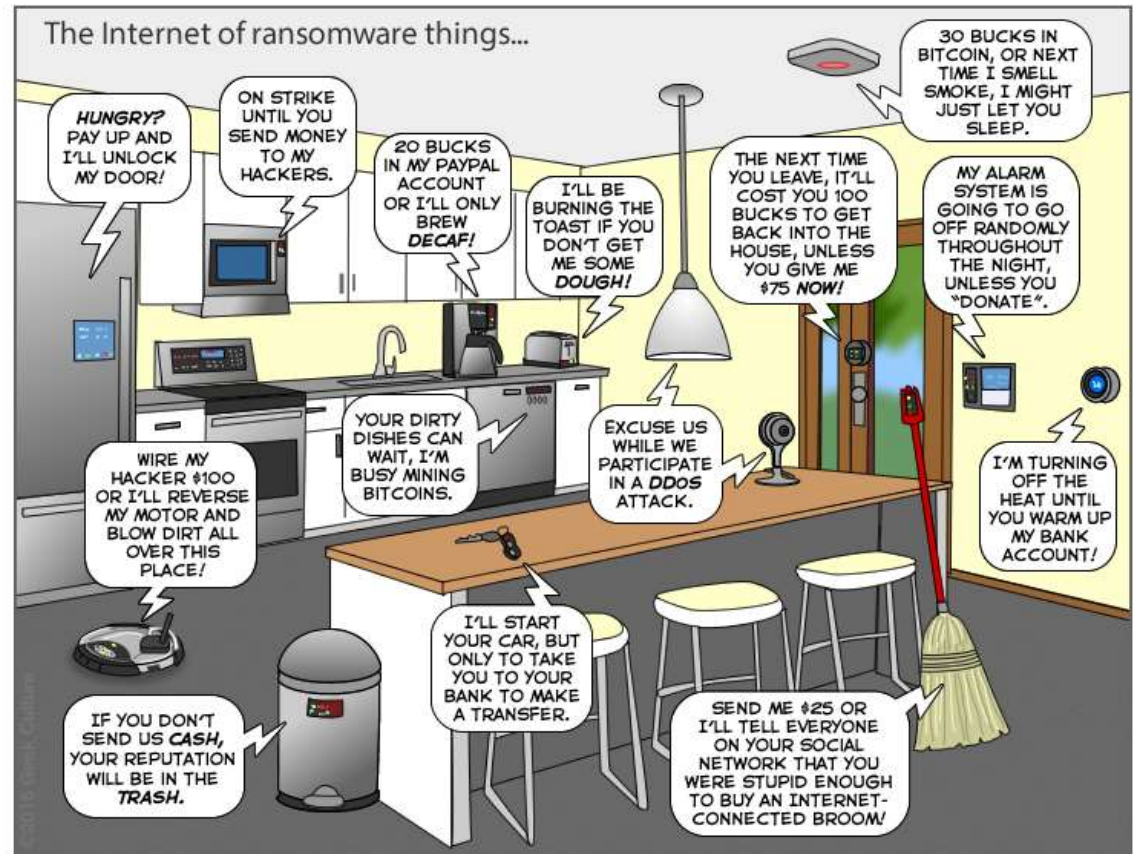


Hyper-reality gone wrong

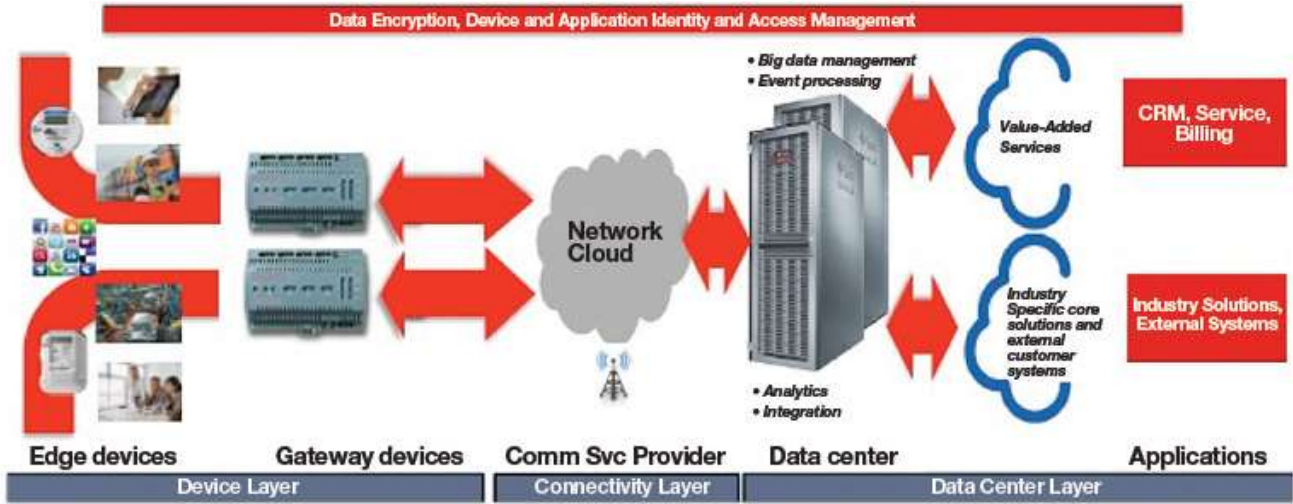


# The Internet of *ransoms*

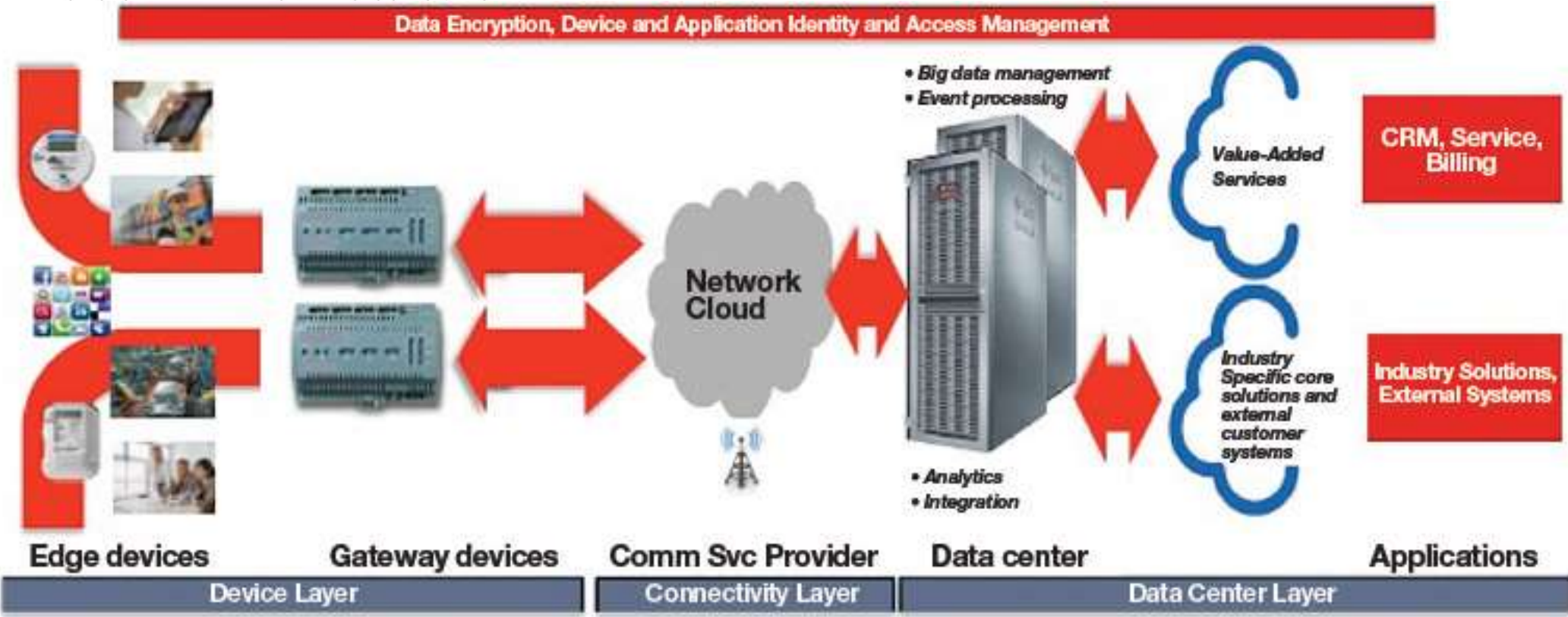
Image credits: Joy of Tech



# IoT: from edge to cloud



Embedded Systems and The Internet of Things –  
What's Under the Hood? | RTC Magazine  
<http://rtomagazine.com/articles/view/103677>



# IoT attack surfaces

Credits: Daniel Miessler

ECOSYSTEM  
ACCESS CONTROL

DEVICE WEB  
INTERFACE

ADMINISTRATIVE  
INTERFACE

ECOSYSTEM  
COMMUNICATION

UPDATE  
MECHANISM

NETWORK TRAFFIC

DEVICE MEMORY

DEVICE FIRMWARE

LOCAL DATA  
STORAGE

VENDOR BACKEND  
APIs

MOBILE  
APPLICATION

DEVICE PHYSICAL  
INTERFACES

DEVICE NETWORK  
SERVICES

CLOUD WEB  
INTERFACE

THIRD-PARTY  
BACKEND APIs

VENDOR BACKEND  
APIs

## Why new research is necessary

Bruce Schneier, The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters | Motherboard Magazine  
[http://motherboard.vice.com/en\\_uk/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster](http://motherboard.vice.com/en_uk/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster)

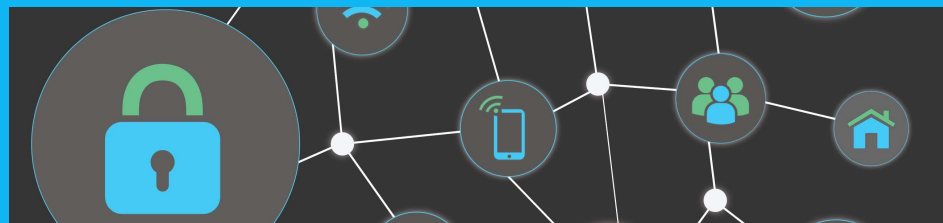
- Internet threats so far have been most about *confidentiality*
  - Bad things happen to our data
  - Most problems today are not solved, only mitigated
- On the Internet of Things, attackers now have “*hands and feet*”
  - The ability to directly affect the physical world
  - Attacks against *flesh, steel, and concrete*

## IoT security challenges

- **Secure Device**
  - How to make sure device code is correct and up-to-date?
  - How to trust data from device?
- **Secure Communication**
  - How to protect confidentiality and integrity when infra-structure has more constraints?
- **Secure Communities**
  - How can people participate and take benefits?
  - How can people trust the system?



# SureThing project



**FCT**

Fundação para a Ciência e a Tecnologia  
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR



Project goal

- **Create and validate location certificates**
  - Devices can make proof of their location or ask proofs
- **For Internet of Things applications**
  - Smart Spaces

The background features several sets of curved lines in shades of gray, some solid and some dashed, creating a sense of motion and depth. A blue speech bubble shape is positioned on the left side, containing the text 'SureThing framework'.

## SureThing framework

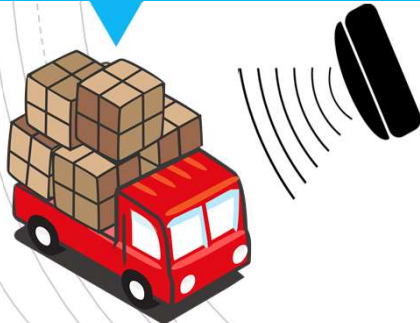
- **Open to diverse technologies**
- **Proof data format**
  - Transport
  - Composition
  - Signature
- **Proof assessment**
  - Weight, rank, compare *strength* of proofs

Use case:  
smart tourism



- **App for tourists**
  - Improve experience
- **Reward visit to locations**
- **Challenges:**
  - Open environment
  - Reuse infrastructure

## Use case: smart taxes



- **Track movements of goods**
  - Mitigate fake shipments
- **Combine location proofs with digital notaries:**
  - Time-stamping
  - Long-term archival
  - Tamper-resistance
- **Extend existing infrastructure with dedicated devices**

## Proximity

Is the device *really* there?



Idea

Let us use the  
*diversity* and *scale*  
of IoT for cyber-defense

Inspiration: PUFs  
Physically Uncloenable  
Functions

## Location sources

- **Raw location**
  - No assurance, can be forged
- **Location metadata**
  - Time, date, identifiers
- **“Unique” measurements**
  - Locality-sensitive network measurements
  - Ambience sensing
  - Environment and social context
    - Witnesses



The background features several sets of curved lines in shades of gray, some solid and some dashed, creating a sense of motion or a circular path. A large blue speech bubble is positioned on the left side of the slide.

## Threats

- **Location spoofing**
- **How to be sure that the device is present?**
  - **Combine location sources for more trusted location claim**
  - **Witness-based location proofs**

The background features several concentric circles, some solid and some dashed, radiating from the center. A blue speech bubble with a white border is positioned in the center, containing the text 'SureThing for mobile devices'.

SureThing for  
mobile devices

## SureThing for mobile devices

- **Issue location proofs for smartphones**
- **Witness-based approach**
- **Different location estimation techniques**

## Location Proof Techniques

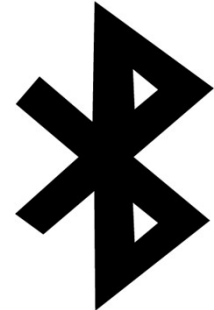
- Based on the used location estimation technique



GPS



Wi-Fi



Bluetooth

## Witness Models

- **Two main models:**
  - **Master** – *trusted* witness
  - **Mobile** – *circumstantial* and *partially trusted* witness

SureThing  
Entities



**Prover**



**Witness**



**Verifier**



**Certification  
Authority**

# Location Proof

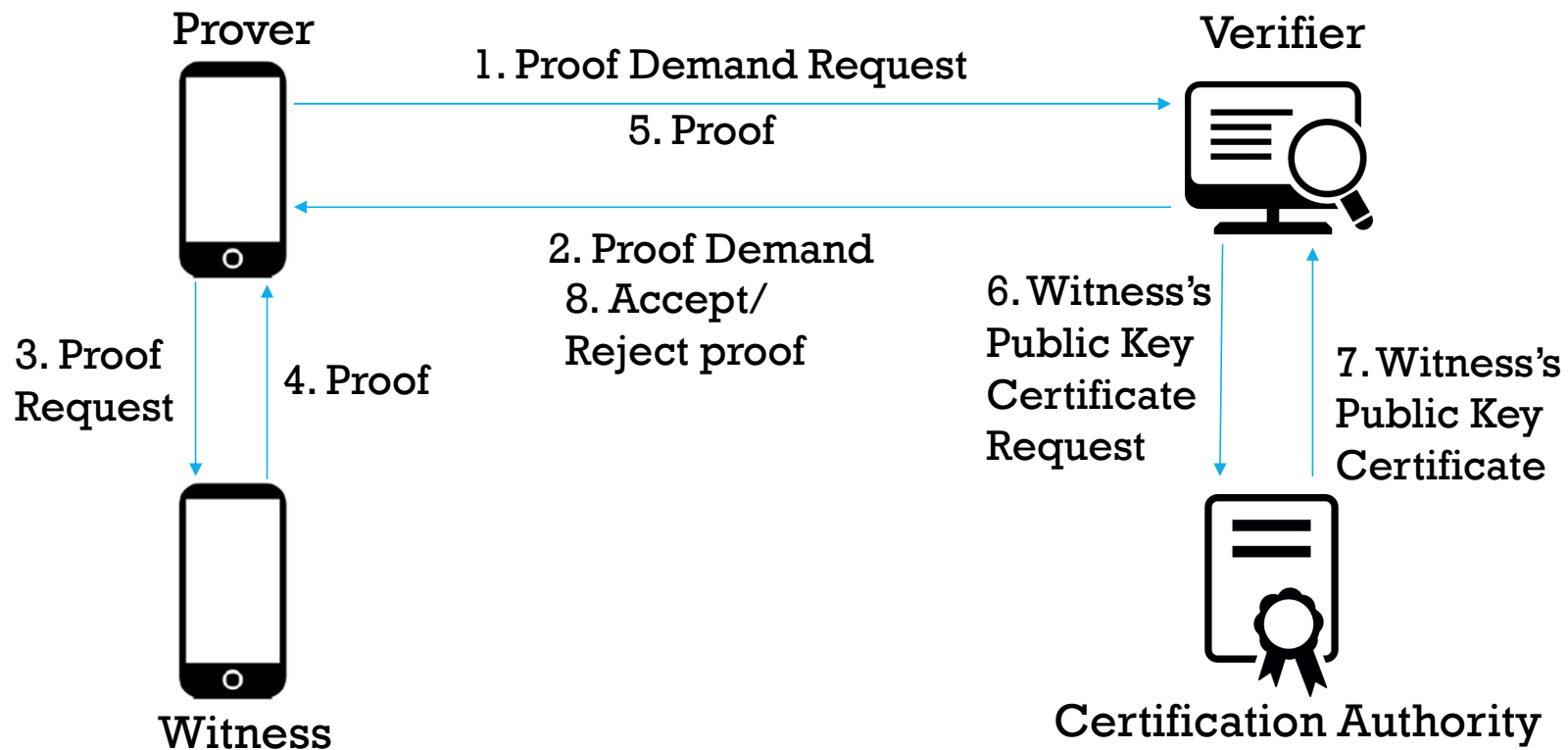
<b>Prover ID</b>	<b>Witness ID</b>	<b>Location of the Prover</b>	<b>Location of the Witness</b>	<b>Nonce</b>	<b>Signature</b>
------------------	-------------------	-----------------------------------	------------------------------------	--------------	------------------

## Location Proof in JSON format

```
{  
  "proverId": "Alice",  
  "witnessId": "Bob",  
  "proverLocation":  
    {  
      "latitude": 38.0123456,  
      "longitude": -9.9876543,  
    },  
  "witnessLocation":  
    {  
      "latitude": 38.0123489,  
      "longitude": -9.9876541,  
    },  
  "nonce": 1234,  
  "signature": "H9xalhdAsHaS..."  
}
```



# Communication Protocol



# Implementation

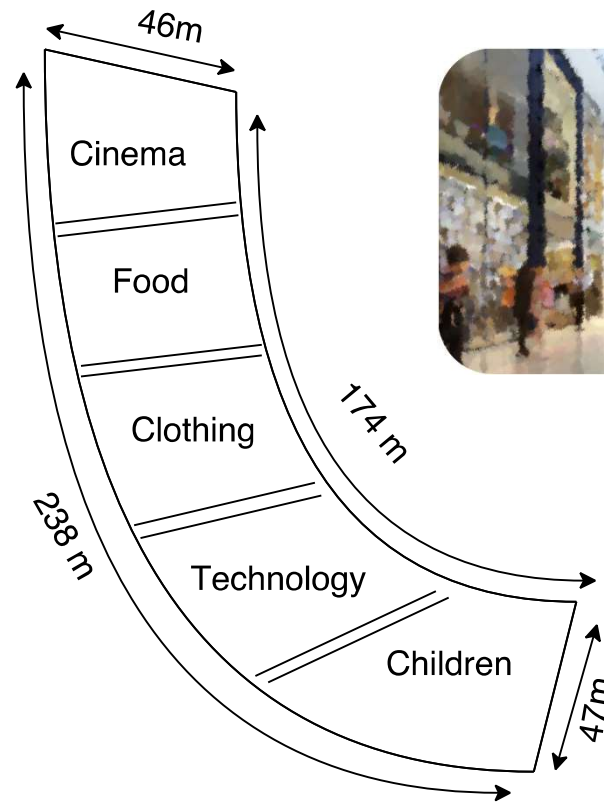
- **Android mobile application for both Prover and Witness**
  - Java programming language
- **Verifier and Certification Authority**
  - RESTful web services
  - JSON messages

## Evaluation

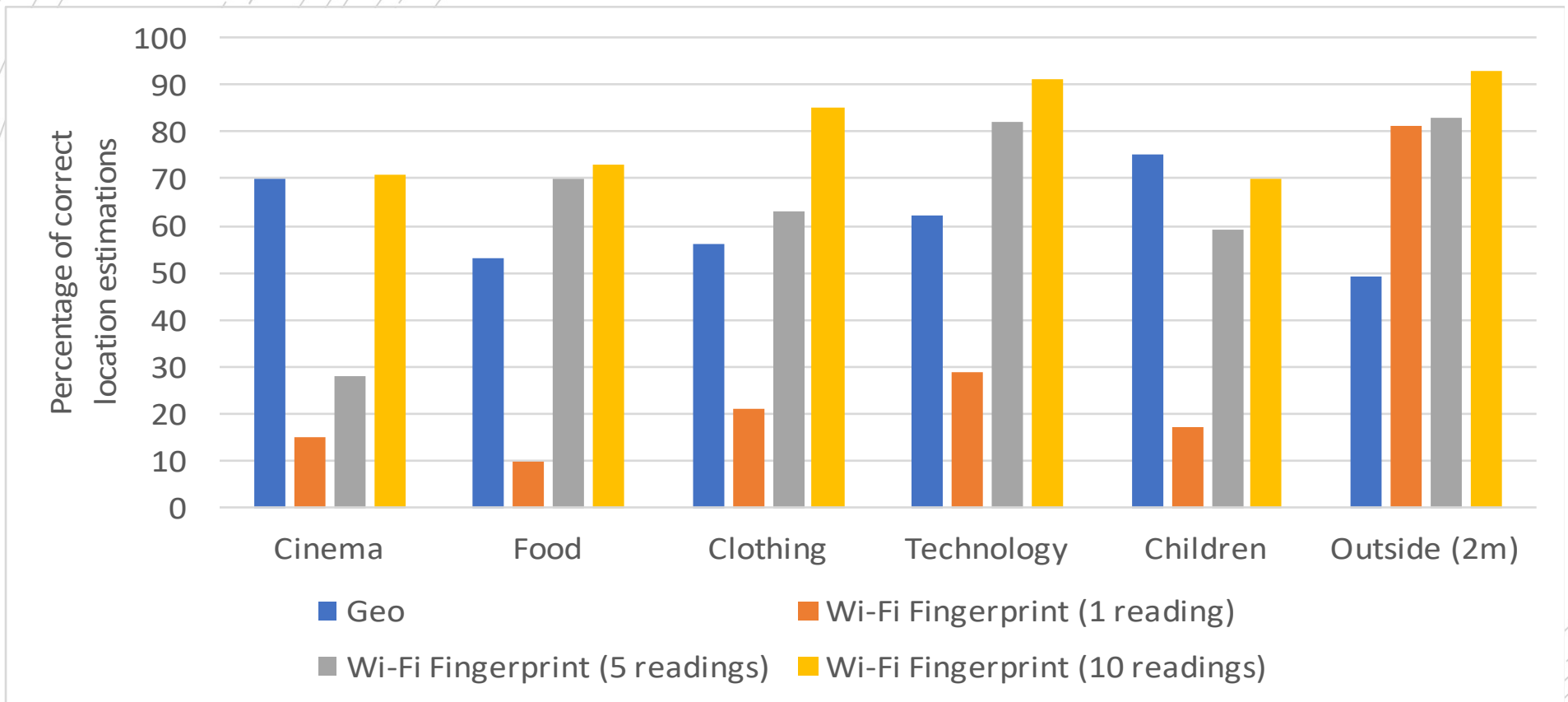
- **How accurate are the location estimation techniques?**
- **How long does it take to issue a location proof?**

## Evaluation Setup

- Building with five different areas
  - Shopping center
  - Testing Geo and Wi-Fi techniques precision

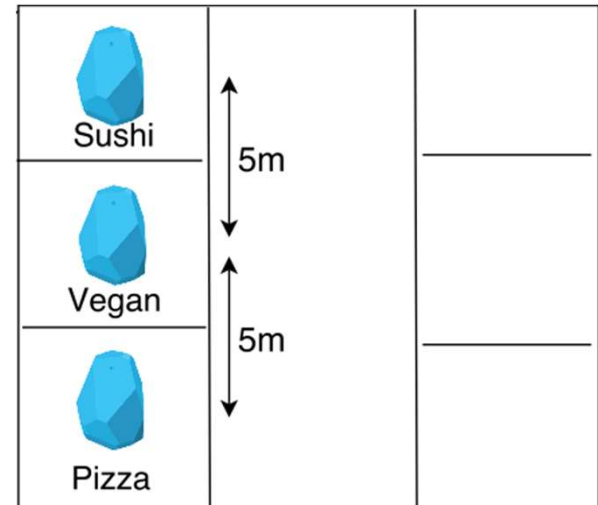


# Comparison of location estimates using GPS and Wi-Fi

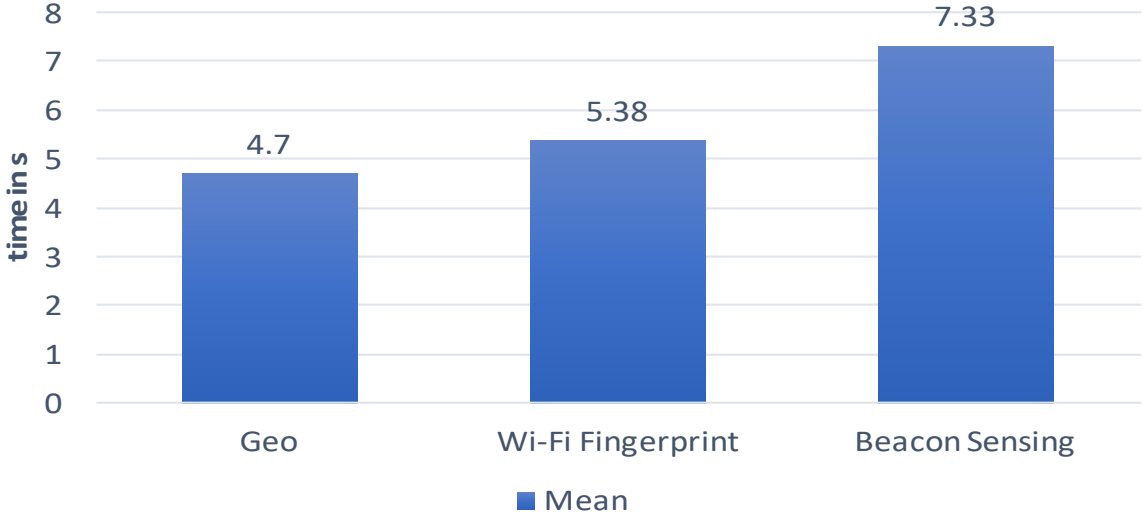


# Bluetooth location estimates

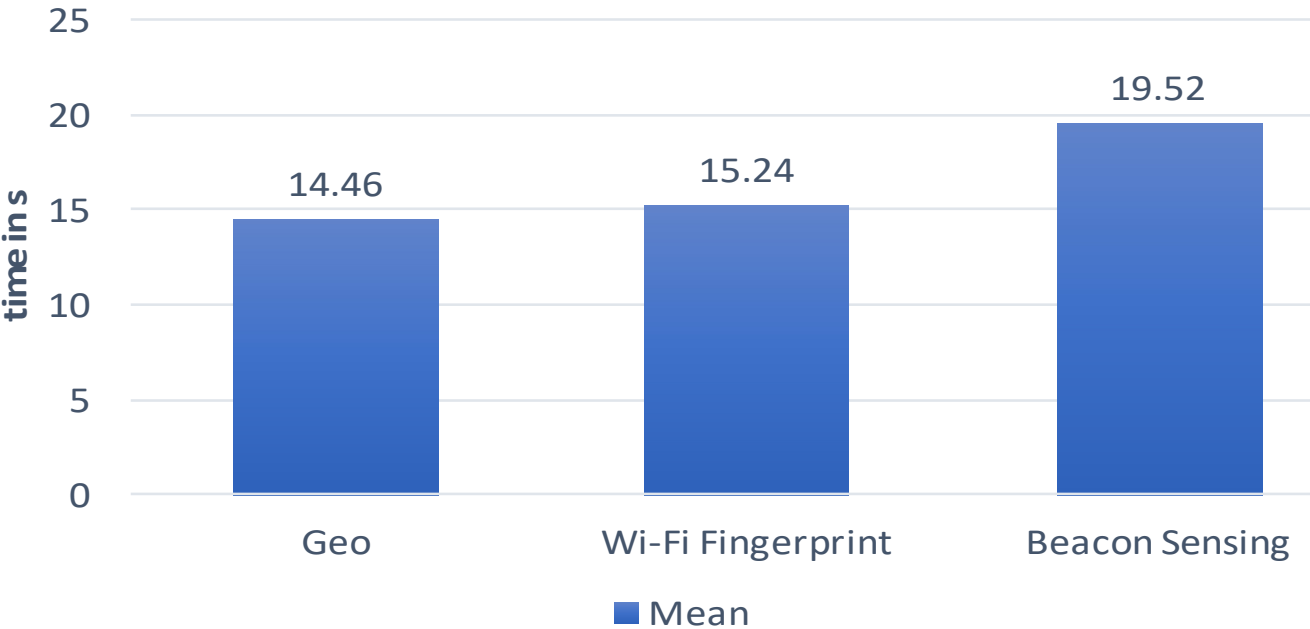
	Correct Claims	Wrong Claims
<b>Sushi Beacon</b>	85%	15%
<b>Vegan Beacon</b>	72%	28%
<b>Pizza Beacon</b>	81%	19%



# Location estimation time



Total proof time



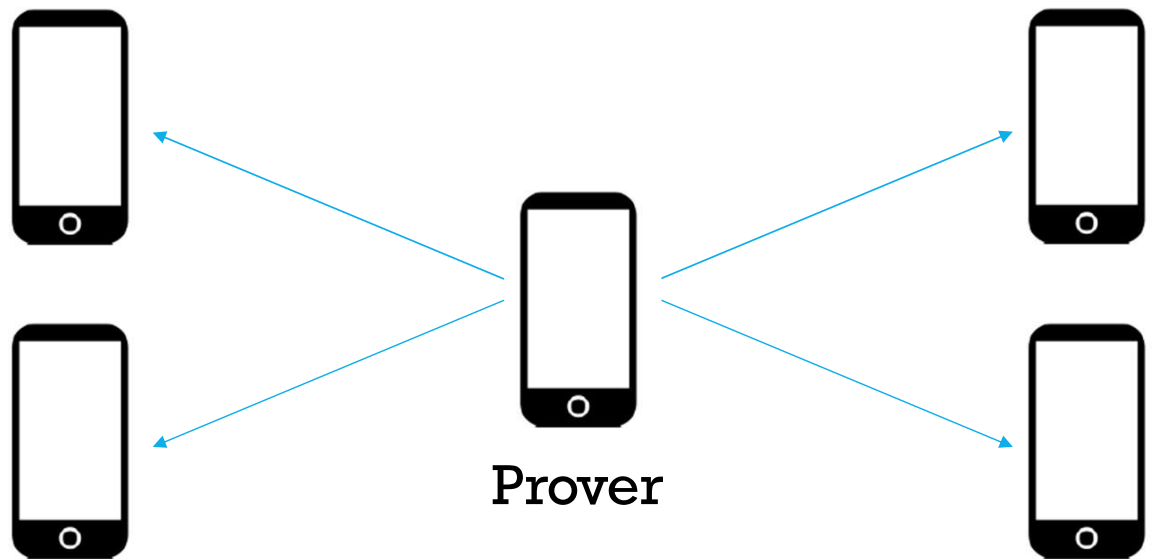


## Collusion avoidance mechanisms

- **Provers can be colluding with false witnesses**
- **Verifier has to use mechanisms to avoid successful collusions**

## Witness redundancy

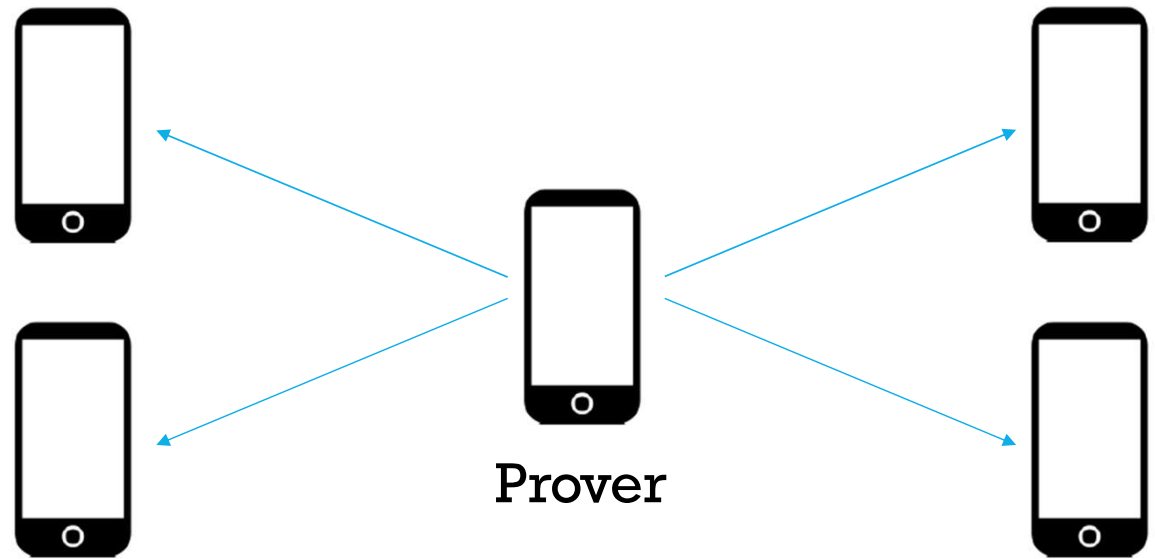
- Prover has to gather proofs from multiple witnesses



## Witness decay

$$V_{xy} = \begin{cases} V & \text{if } N_{xy} = 0 \\ V - \frac{N_{xy}^k}{U} & \text{if } N_{xy} > 1 \end{cases}$$

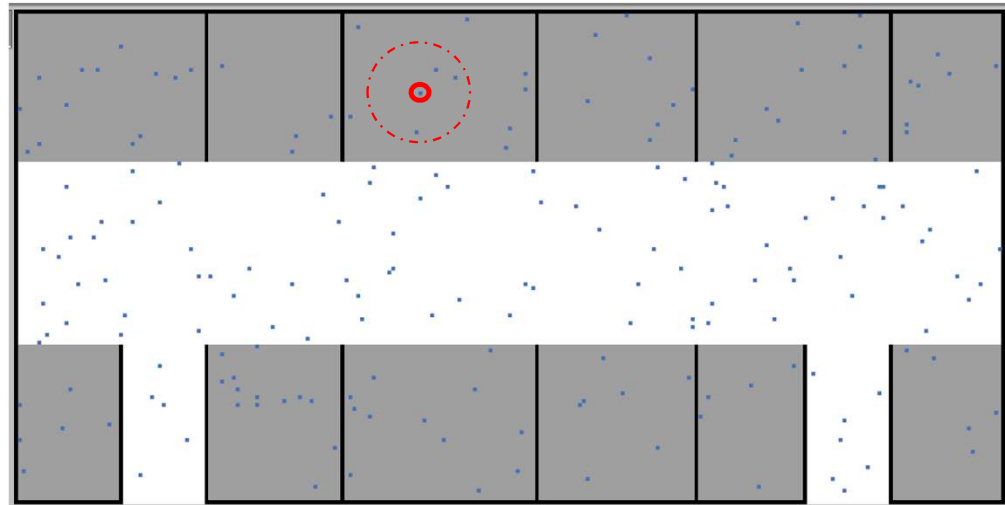
- Proofs given by repeated witnesses become less valuable



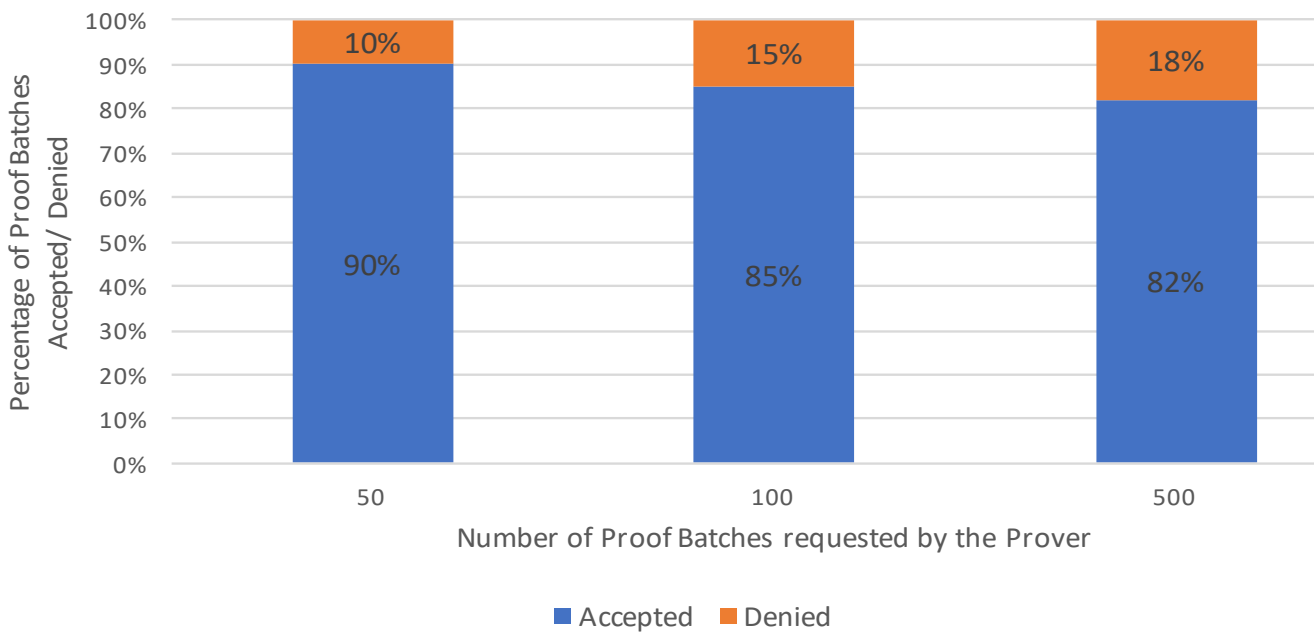
# Collusion avoidance simulation

Netlogo simulation

- Simulated shopping center
- 250 users that behave as *Provers* and *Witnesses*



# Collusion avoidance simulation



# Summary

Witness model	Trusted by the Verifier?	Bottleneck Potential?	Needs Collusion Avoidance?	Best scenarios
Master	Yes	High	No	Low attendance
Mobile	No	Low	Yes	High attendance

## Conclusion

- **Users must provide location proofs to access valuable services**
- **SureThing for mobile devices is a flexible solution**
  - **Different location estimation techniques**
  - **Different witness models**
- **Implementation of a prototype including all the entities**

The background features a series of concentric, overlapping curved lines in shades of gray, some solid and some dashed, creating a sense of motion and depth. A large, bright blue speech bubble shape is centered on the page, containing the main text.

# Future/ongoing work

Started in October 2018



## Neighborhood watch



Pedro Carmo

- **Smart Spaces locality**
  - Neighborhood
- **Keep track of limited devices**
  - How they behave
- **Detect presence of other devices (intrusions)**
  - Detect changes in communication

Use case:  
Smart Tourism



Gabriel Maia

- **App for tourists**
  - Rewards for visit to locations
  - Fast proofs
- **Challenges**
  - Open environment
  - Reuse infrastructure

Use case:  
smart taxes



Henrique Santos

- App to track shipments
  - Mitigate *fake* goods shipments
- Combine location proofs with digital notaries
  - Time-stamping
  - Tamper-resistance
  - Long-term archival
- May add dedicated infrastructure

## Privacy-preserving location proofs



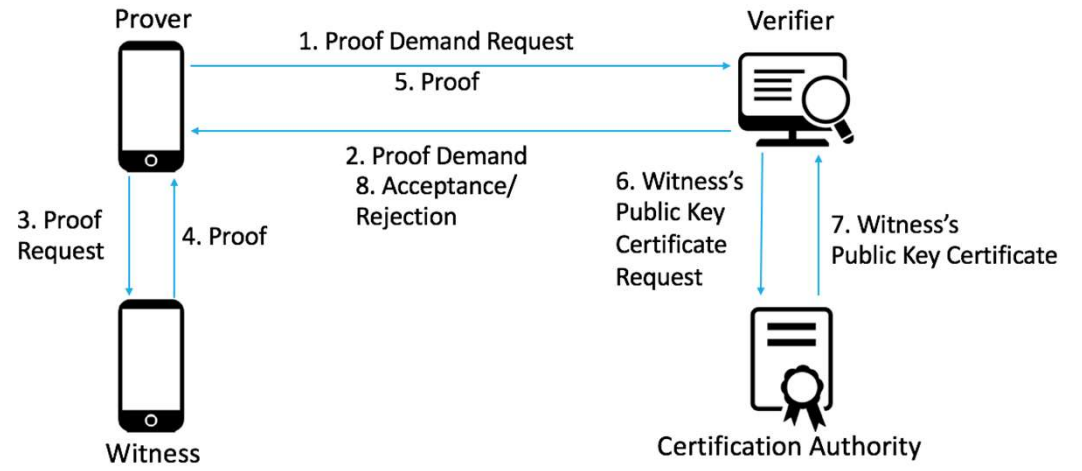
Rui Claro

- **Location data can easily be personal data**
  - **User privacy needs to be protected**
  - **Address TUI properties**
    - *Transparent, Unlink, Intervene*

# SureThing: Device location certification for IoT



Thank you!



<http://surething-project.eu>

miguel.pardal@tecnico.ulisboa.pt



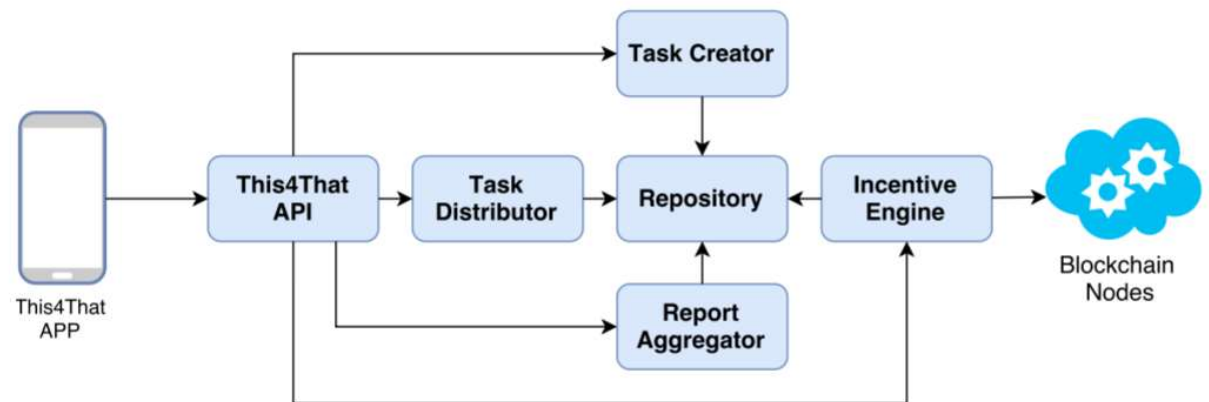
HASLAB/INESC TEC  
& MINHO UNIVERSITY

## SureThing publications

- Diogo Calado, Miguel L. Pardal. *Tamper-proof incentive scheme for mobile crowdsensing systems*. IEEE International Symposium on Network Computing and Applications (NCA), 2018.
- João Ferreira, Miguel L. Pardal. *Witness-based location proofs for mobile devices (short)*. IEEE International Symposium on Network Computing and Applications (NCA), 2018.

This4That -  
Incentives for  
data capture and  
data sharing

- Reward participants that share data
  - E.g. SureThing witness
- Build a distributed, tamper-proof incentive ledger



# This4That architecture

