Challenges for PKI: IoT, Blockchains

शिवकुमार G. Sivakumar சிவகுமார்

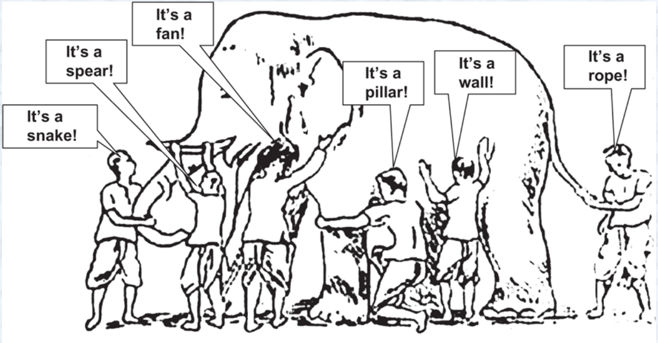
Computer Science and Engineering
भारतीय प्रौद्योगिकी संस्थान मुंबई (IIT Bombay)
siva@iitb.ac.in

June 17, 2016

- The Good (Emerging Technologies, 3rd Platform)
- The Bad (IoT Challenges (Or Opportunities?))
- The Ugly(Why trust CAs? Decentralized Trust)

Expectations, Fear, Risk of Change

Blind men and the Elephant - अन्ध-गज न्यायः



Note: The risks of analytical thinking and fragmentation of knowledge

पूर्व पक्ष (Purva Paksha) for Future of Internet

Web 1.0 may have *democratized access to information*, but it is like drinking water from a fire hose!
Search engines provide partial solutions, but cannot combine, categorize and infer!

Web 2.0 may have allowed *right to assembly/collaboartion*, but

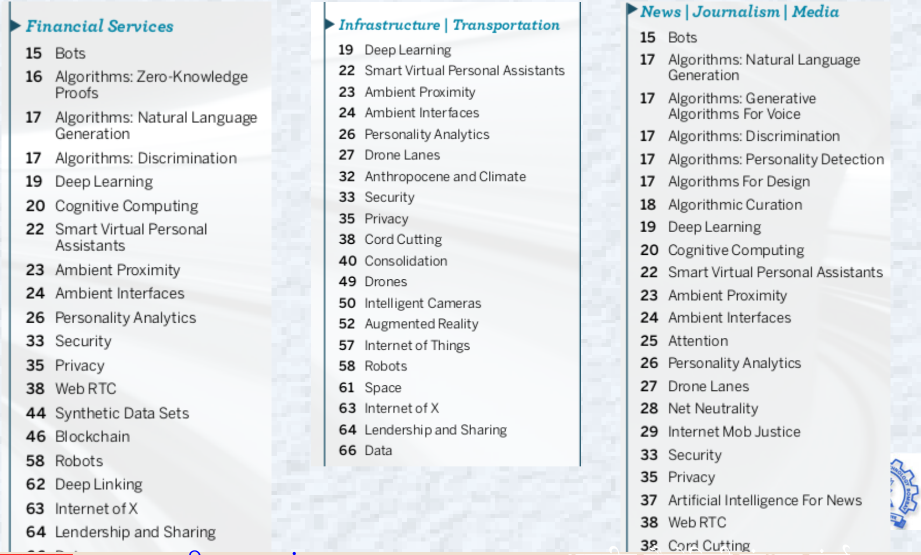
- Proliferated unreliable, contradictory information.
- Facilitated malicious uses including loss of privacy, security.

What do you want from Web 3.0?
What you want to see/hear when you wakeup?
I have a dream ...

How to achieve? AI meets the web of Open Enterprises!

http://webbmediagroup.com/2016-trends

Excellent report explaining 81 notable Technology trends



Financial Services

15	Bots
16	Algorithms: Zero-Knowledge Proofs
17	Algorithms: Natural Language Generation
17	Algorithms: Discrimination
19	Deep Learning
20	Cognitive Computing
22	Smart Virtual Personal Assistants
23	Ambient Proximity
24	Ambient Interfaces
26	Personality Analytics
33	Security
35	Privacy
38	Web RTC
44	Synthetic Data Sets
46	Blockchain
58	Robots
62	Deep Linking
63	Internet of X
64	Lendership and Sharing

Infrastructure | Transportation

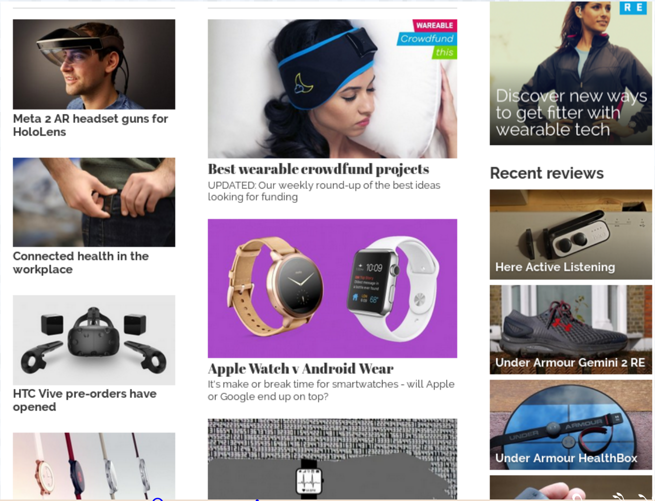
19	Deep Learning
22	Smart Virtual Personal Assistants
23	Ambient Proximity
24	Ambient Interfaces
26	Personality Analytics
27	Drone Lanes
32	Anthropocene and Climate
33	Security
35	Privacy
38	Cord Cutting
40	Consolidation
49	Drones
50	Intelligent Cameras
52	Augmented Reality
57	Internet of Things
58	Robots
61	Space
63	Internet of X
64	Lendership and Sharing
66	Data

News | Journalism | Media

15	Bots
17	Algorithms: Natural Language Generation
17	Algorithms: Generative Algorithms For Voice
17	Algorithms: Discrimination
17	Algorithms: Personality Detection
17	Algorithms For Design
18	Algorithmic Curation
19	Deep Learning
20	Cognitive Computing
22	Smart Virtual Personal Assistants
23	Ambient Proximity
24	Ambient Interfaces
25	Attention
26	Personality Analytics
27	Drone Lanes
28	Net Neutrality
29	Internet Mob Justice
33	Security
35	Privacy
37	Artificial Intelligence For News
38	Web RTC
38	Cord Cutting

Wearables and Pervasive Computing

Will drastically improve the way we interact with systems and data, literally fusing IT with our daily lives and surroundings. From *www.wareable.com*



Meta 2 AR headset guns for HoloLens

Connected health in the workplace

HTC Vive pre-orders have opened

WAREABLE Crowdfund this

Best wearable crowdfund projects

UPDATED: Our weekly round-up of the best ideas looking for funding

Apple Watch v Android Wear

It's make or break time for smartwatches - will Apple or Google end up on top?

R E

Discover new ways to get fitter with wearable tech

Recent reviews

Here Active Listening

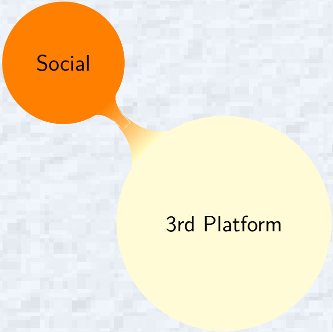
Under Armour Gemini 2 RE

Under Armour HealthBox

3rd platform: SMAC + IoT

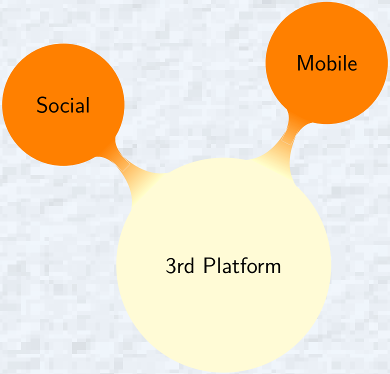
- Main Frame (1960s ...)
- Client Server (1990s ...)
- Today (Handheld, Pervasive Computing)

3rd platform: SMAC + IoT



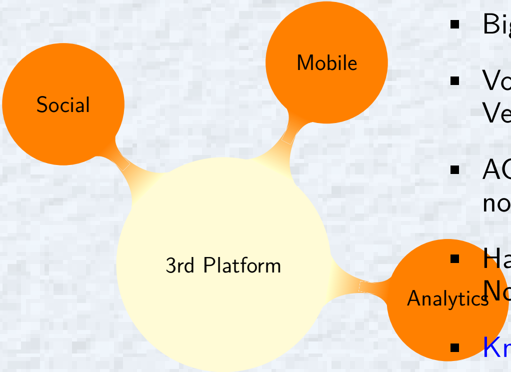
- What's App (how many engineers?)
- Facebook, Twitter, GooglePlus ...
- Web 2.0 (Right to Assembly)
- Crowdsourcing (Wikipedia)
- Crowdfunding (no banks!)

3rd platform: SMAC + IoT



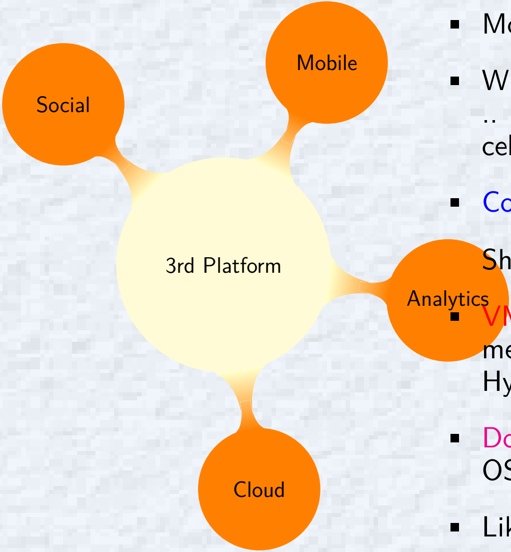
- Phone (Smart, Not-so-smart!)
- Wearables! (Google glass, Haptic)
- Internet of "Me" (highly personalized) Business (no *generic* products!)
- BYOx: Device security, App/content management nightmare.
- Data Loss Prevention (Fortress Approach - Firewall, IDS/IPS - won't work!)

3rd platform: SMAC + IoT



- Big Data
- Volume, Variety, Velocity, Veracity
- ACID properties Database not needed
- Hadoop, Map Reduce, NoSql
- Knowledge is Power!
- Collect, Analyse, Infer, Predict

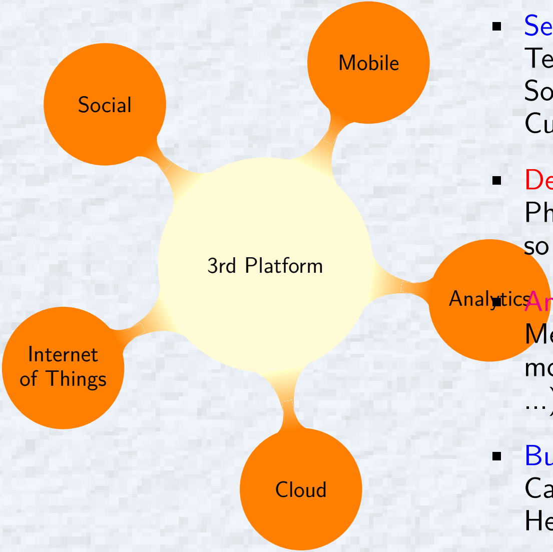
3rd platform: SMAC + IoT



- Moore's law
- What could fit in a building .. room ... pocket ... blood cell!
- Containers Analogy from Shipping

- VMs separate OS from bare metal (at great cost- Hypervisor, OS image)
- Docker- separates apps from OS/infra using containers.
- Like *IaaS*, *PaaS*, *SaaS* Have you heard of *CaaS*?

3rd platform: SMAC + IoT



- Sensors (Location, Temperature, Motion, Sound, Vibration, Pressure, Current, ...)
- Device Eco System (Smart Phones, Communicate with so many servers!)
- Ambient Services (Maps, Messaging, Traffic modelling and prediction, ...)
- Business Use Cases (Ola Cabs, Home Depot, Philips Healthcare, ...)
- Impact on wireless

Open Enterprises of the Future

What the Future Holds?

Modify a Google Calendar to allow a colleague to add a Faaso's roll order to a meeting invite that can be picked up by Ola and delivered by a drone to a client's office five minutes before the scheduled meeting starts.

What this needs?

- Multi-Party Services Orchestration
- Transparent Information Flow
- Transparent Event Flow
- Semantic Consistency
- Network and Protocol Adaptability
- End-to-End Security
- Business Management

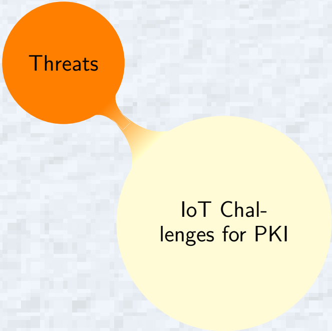
In the Security context, this is securing M2M communications!

IoT Security Concerns

IoT Challenges for PKI

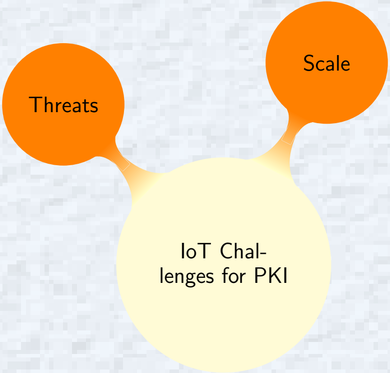
- Personal wearables
- Biomedical implants (pacemaker, insulin control, ...)
- Smart Homes, Smart Grids
  ...
- Transportation industry

IoT Security Concerns



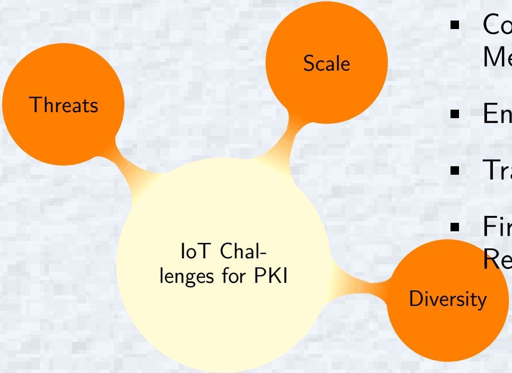
- Fridge ordering junk food.
- Fire in your kitchen!
- Malfunction of pacemaker, insulin injector.
- Driverless car taken over!
- Drone attack.

IoT Security Concerns



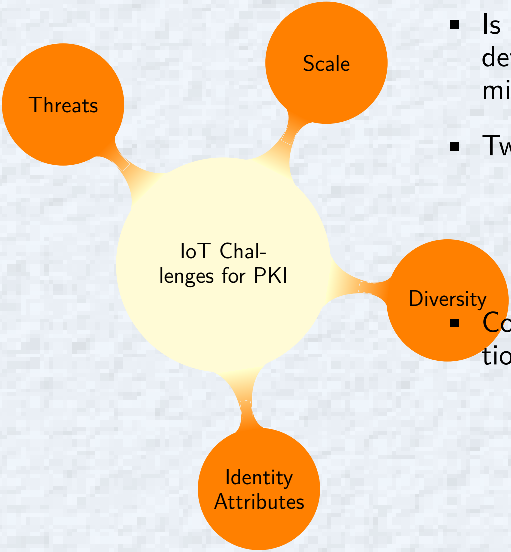
- Firefox has certificates for few hundred CAs.
- Top 3 CAs have over 80% market!
- Let's Encrypt (Free, Automated, Open)
  - Aims to encrypt 100% of web.
  - 1.7 million certificates for more than 3.8 million websites since Sept 2015!
- Gartner: From 4.8 billion connected devices in 2015 to 25 billion in 2020.

IoT Security Concerns



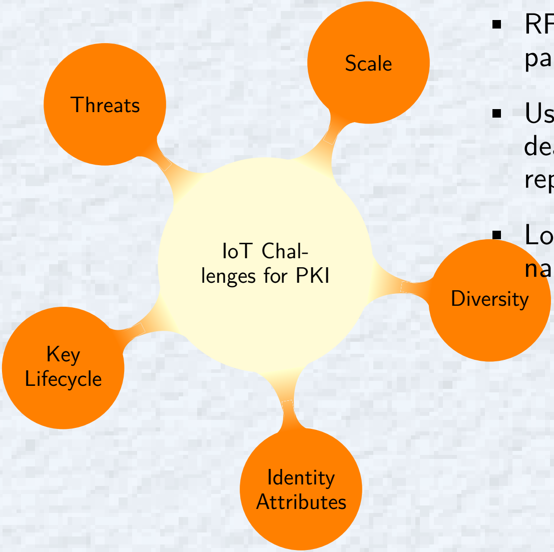
- Computational Power, Low Memory
- Energy constraints
- Transmission Range
- Firmware Upgrades, Reconfiguration

IoT Security Concerns



- Is a *smartphone* a single device? (camera, speaker, microphone, sensors ...)
- Two not feasible
  - Whay you have
  - ~~What you know~~
  - ~~What you are~~
- Context based Authentication/Authorization
  - Location
  - Use case specific
  - Owner
  - Manufacturer
  - Govt.

IoT Security Concerns



- RFID tag on International parcel
- User roles (manufacturer, dealer, owner, user, repairshop ...)
- Local versus Global namespace

Blockchains and Distributed PKI

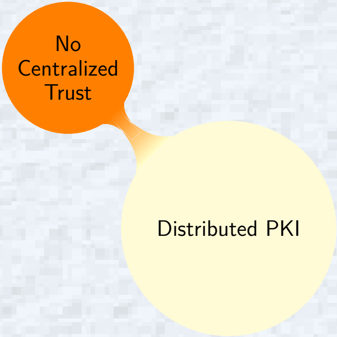
Distributed PKI

- Trust Model
  - Trusted Third Party (TTP)
  - Web of Trust

  - Main Stream Media
  - Social Media

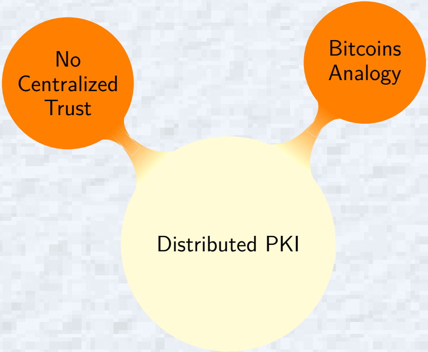
  - iTunes
  - P2P networks

Blockchains and Distributed PKI



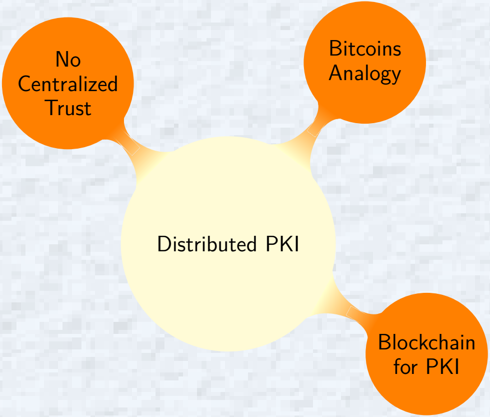
- Ten Risks of PKI by Carl Ellison and Bruce Schneier
- What is the CA an Authority on?
- Corruptible, central points of failure.
- IDs (email, domain) are *borrowed/rented* from 3rd parties.
- Let real owner control identity, others provied auxiliary services only.

Blockchains and Distributed PKI



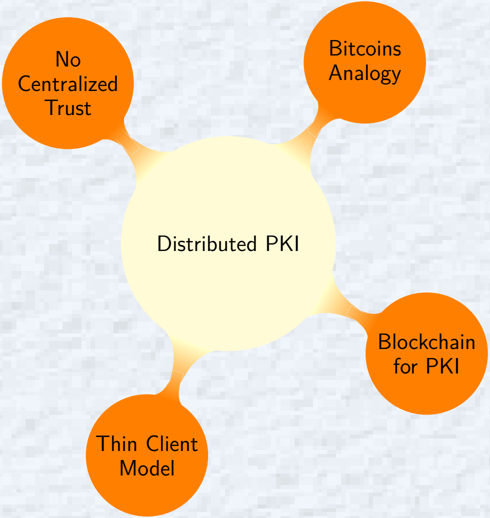
- Bitcoins as peer to peer currency
- No Banks, PayPal, PayTm or 3rd parties
- Chaining blocks of Transactions
- No double spending
- Proof of work establishes legitimacy

Blockchains and Distributed PKI



- Block chain as Distributed Ledger
- Consensus protocol.
- Single version of truth!
- No single party can compromise
- Digitally signed Transactions/Proof of work

Blockchains and Distributed PKI


Distributed PKI

No Centralized Trust

Bitcoins Analogy

Blockchain for PKI

Thin Client Model

- Distributed PKI
- Owners can Register, Update, Lookup, Revoke!
- (Thin) Clients can verify
  - Public Key of any entity (Proof of existence)
  - Revocation of any key (Proof of inexistence)
  - State/Attribute of any key
- Merkle trees make cost low.

Digital India Vision

From India PKI Forum-

The Digital India Vision emphasizes the use of technology to enable connectivity to every Indian citizen for *Education, Healthcare, Financial Inclusion, Other areas of governance*

Aadhar and Digital Signatures can help *Going Green, Reduce Cost and Time, transactions from anywhere, Authenticity, Data Integrity, Traceability*

Long way to go, Glass only half-full.
Excellent program ahead today...