Internet Of Things

Security in IoT

PRAJANYA GUPTA

Internet Of Things

What is IoT and some popular projects

- The internet of things(IoT) is a concept for an ecosystem of electronics that aren’t traditional computing devices but are web-enabled smart devices that use embedded systems, to collect, send and act on data they acquire.

- Ocean of things

Internet Of Things

Security in IoT

- IoT are web enabled device that makes them prone to hacking.
- There have been many cases of data leaks, breaches, hijacking, flooding and the list just continues.

$14.4 trillion

Market rise

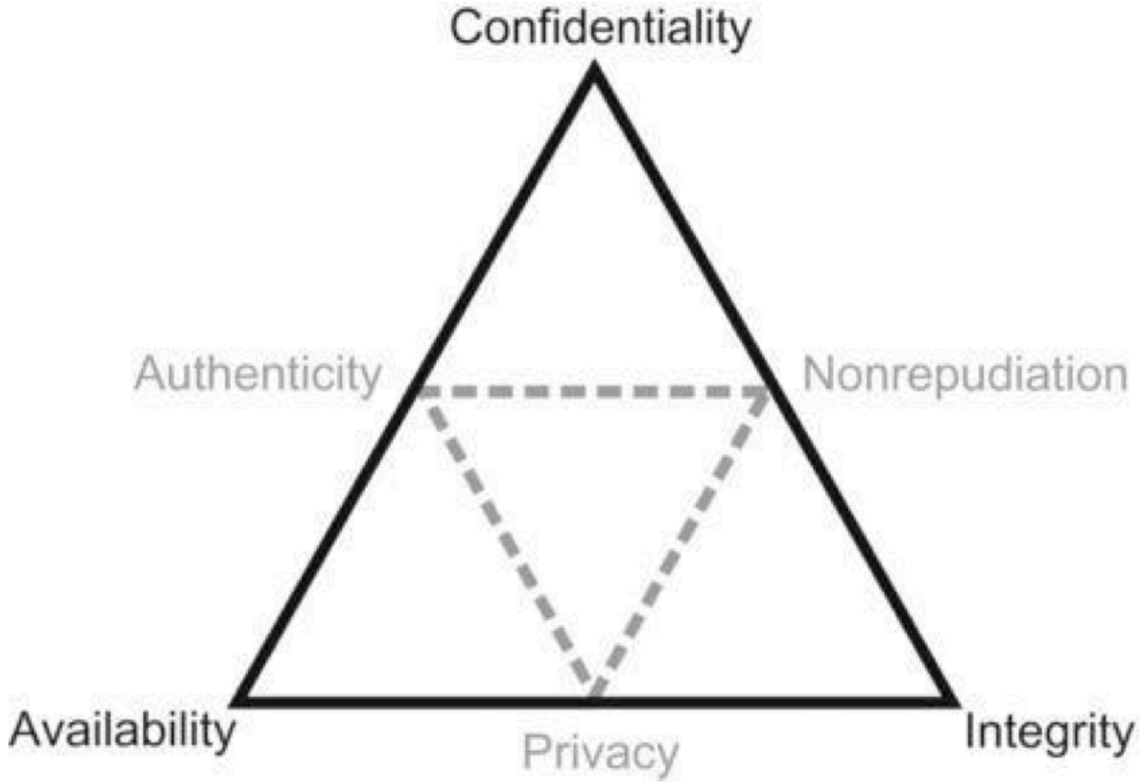
4.4 zettabytes

Data produced in 2020

IOT SECURITY: CHALLENGES, SOLUTIONS & FUTURE PROSPECTS

Mikhail Gloukhovtsev

- Key security requirements
- IoT security based on the three main domains
  1. TRUST
  2. DATA CONFIDENTIALITY
  3. PRIVACY



- **Confidentiality**—data is secured to authorized parties
- **Integrity**—data is trusted
- **Availability**—data is accessible when and where needed
- **Nonrepudiation**—service provides a trusted audit trail
- **Authenticity**—components can prove their identity
- **Privacy**—service does not automatically see customer data

TRUST

- Trusted Platform Modules
- Blockchain to develop trust in transactions
- Identity management

DATA CONFIDENTIALITY

- Homomorphic encryption

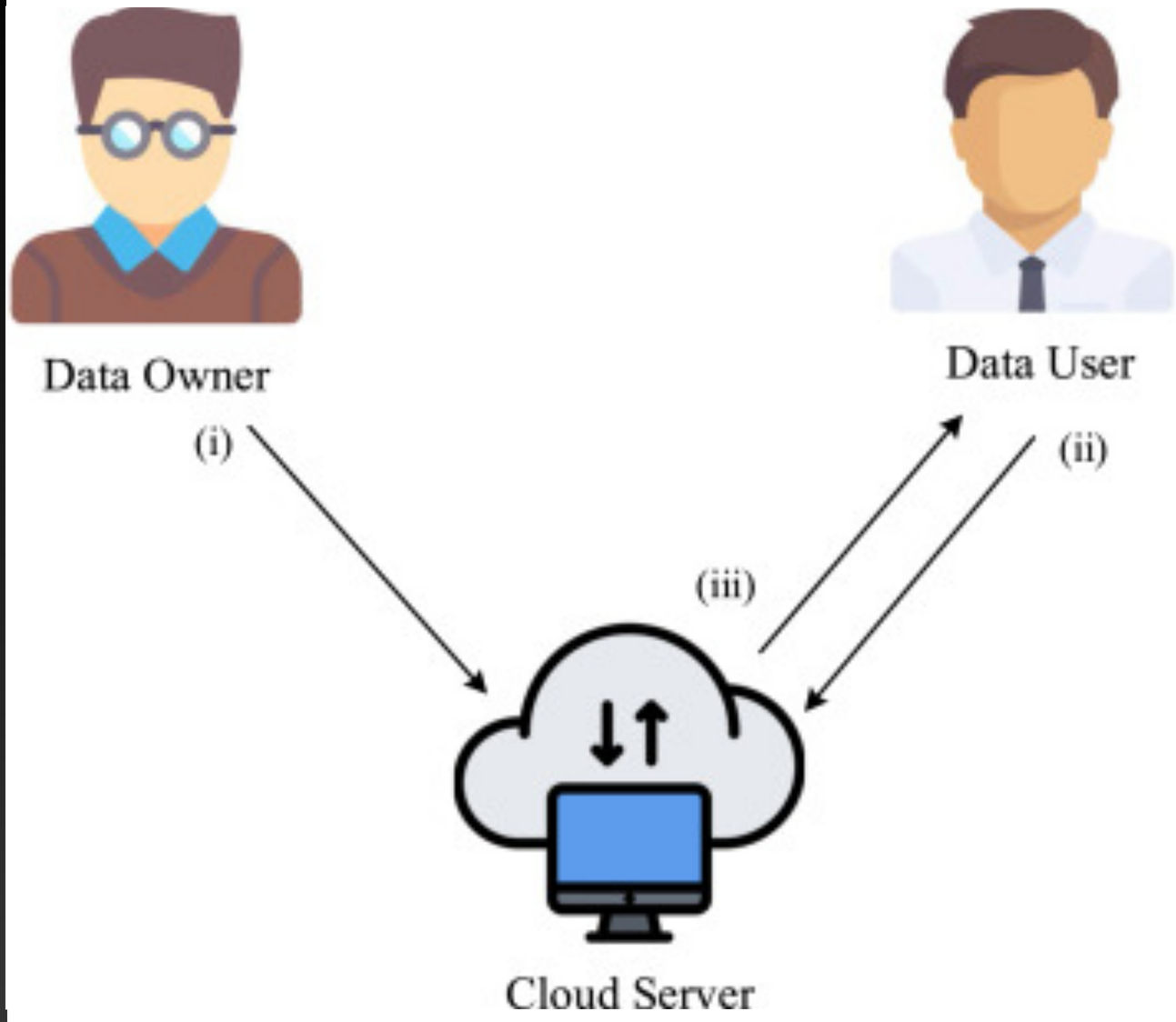
PRIVACY

- Data usage control

Substring-searchable attribute-based encryption and its application for IoT devices

XiSun

- System model
- Three entities in this system
  1. cloud server
  2. data owner
  3. data user
- Application in IoT - out sourcing decryption of data
- Performance testing



Searchable Encryption

Uploading Phase

Queuing Phase

Matching Phase

Having A Local Server

Reduced **COST** of Devices

Easier To **USE**

Easy To Implement The **Current Solutions**

Can Carry Out **Heavy Computation**

Managing **Updates**

Trustworthy Firmware

DATA CONFIDENTIALITY

Privacy

Easy To **Monitor** And **Detect**