Internet of Things (IoT) - Demystified

Keynote – ICIT 2017
22nd Dec 2017

Saraju P. Mohanty
University of North Texas, USA.

Email: saraju.mohanty@unt.edu
More Info: http://www.smohanty.org
Talk - Outline

- Motivations for IoT
- Selected Components of IoT
- Selected Applications of IoT
- Driving Technologies of IoT
- Challenges and Research in IoT
- IoT Design Flow
- Tools and Solutions for IoT
- Related Buzzwords of IoT
- Conclusions and Future Directions
Population Trend – Urban Migration

“India is to be found not in its few cities, but in its 700,000 villages.”
- Mahatma Gandhi

- 2025: 60% of world population will be urban
- 2050: 70% of world population will be urban

Source: http://www.urbangateway.org
Human Migration Problem

- Uncontrolled growth of urban population
- Limited natural and man-made resources

Source: https://humanitycollege.org
Smart Cities: For effective management of limited resource to serve largest possible population to improve:

- Livability
- Workability
- Sustainability

“Cities around the world could spend as much as $41 trillion on smart tech over the next 20 years.”

Smart Cities - 3 Is

The 3Is are provided by the Internet of Things (IoT).

Source: Mohanty 2016, EuroSimE 2016 Keynote Presentation
IoT is the Backbone Smart Cities

Source: Mohanty 2016, CE Magazine July 2016
Internet of Things (IoT) - History

1969
The Internet Emerges
The first nodes of what would eventually become known as ARPANET, the precursor to today's Internet, are established at UCLA and Stanford universities.

1982
TCP/IP Takes Shape
Internet Protocol (TCP/IP) becomes a standard, ushering in a worldwide network of fully interconnected networks called the Internet.

1990
A Thing Is Born
John Romkey and Simon Hackett create the world’s first connected device (other than a computer): a toaster powered through the Internet.

1999
The IoT Gets a Name
Kevin Ashton coins the term “Internet of things” and establishes MIT’s Auto-ID Center, a global research network of academic laboratories focused on RFID and the IoT.

2005
Getting Global Attention
The United Nations first mentions IoT in an International Telecommunications Union report. Three years later, the first international IoT conference takes place in Zurich.

2008
Connections Count
The IPSO Alliance is formed to promote IP connections across networks of “smart objects.” The alliance now boasts more than 50 member firms.

2011
IPV6 Launches
The protocol expands the number of objects that can connect to the Internet by introducing 340 undecillion IP addresses (2128).

2013
Google Raises the Glass
Google Glass, controlled through voice recognition software and a touchpad built into the device, is released to developers.

2014
Apple Takes a Bite
Apple announces HealthKit and HomeKit, two health and home automation developments. The firm’s iBeacon advances context and geolocation services.


IoT Keynote by Prof./Dr. Saraju P. Mohanty

22nd Dec 2017
Components
IoT – Definition - IoT European Research Cluster (IERC)

A dynamic global network infrastructure

with self configuring capabilities

based on standard and interoperable communication protocols

where physical and virtual “things”

have identities, physical attributes, and virtual personalities and

use intelligent interfaces,

and are seamlessly integrated

into the information network.


IEEE also provides a formal, comprehensive definition of IoT.

IoT Keynote by Prof./Dr. Saraju P. Mohanty
IoT – Definition - International Telecommunication Union (ITU)

A network that is: “Available anywhere, anytime, by anything and anyone.”

Internet of Things (IoT) – Concept

**Things**
Sensors/actuators with IP address that can be connected to Internet

**Local Network**
Can be wired or wireless: LAN, Body Area Network (BAN), Personal Area Network (PAN), Controller Area Network (CAN)

**Cloud Services**
Data either sent to or received from cloud (e.g. machine activation, workflow, and analytics)

**Global Network**
Connecting bridge between the local network, cloud services and connected consumer devices

**Connected Consumer Electronics**
Smart phones, devices, cars, wearables which are connected to the Things

IoT Keynote by Prof./Dr. Saraju P. Mohanty

22nd Dec 2017
IoT Architecture - 3 & 5 Level Model

Three Level Model

Five Level Model

Source: Nia 2017, IEEE TETC 2017
IoT Architecture - 7 Level Model

Overall architecture:
- A configurable dynamic global network of networks
- Systems-of-Systems

Source: Mohanty 2016, EuroSimE 2016 Keynote Presentation
IoT – Sensors


100s of Sensors

IoT Keynote by Prof./Dr. Saraju P. Mohanty
The “Things” refer to any physical object with a device that has its own IP address and can connect and send/receive data via network.
IoT - Communications

Selected IoT Communications Technology

- Bluetooth Low-Energy (BLE)
- Zigbee
- Z-Wave
- 6LowPAN
- Thread
- WiFi
- Cellular
- NFC
- Sigfox
- Neul
- LoRaWAN

Data rate, log scale

Power consumption, indicative

Range, log scale


Source: https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about
**IoT - Cloud**

- **Software as a Service (SaaS)**
- **Platform as a Service (PaaS)**
- **Infrastructure as a Service (IaaS)**

Source: Gubbi 2013, Elsevier FGCS 2013

Source: https://www.livewireindia.com/cloud_computing_training.php
IoT - Applications
IoT - Markets and Stakeholders

- Consumer Equipment Providers
- Hospitals and Doctors
- ICT Infrastructure Providers
- Insurance Companies
- Logistics Companies
- Appliances Providers
- Regulators
- Facility Management
- Public Transportation Companies
- Retail Stores
- City Authorities
- Application developers
- Manufacturing Industries
- Utilities
- Automation equipment providers


IoT Keynote by Prof./Dr. Saraju P. Mohanty
IoT in Smart Healthcare

Quality and sustainable healthcare with limited resources, anywhere, anytime.

IoT Role Includes:
- Real-time monitoring
- Better emergency response
- Easy access of patient data
- Connectivity among stakeholders
- Remote access to healthcare

"$117 Billion Market For IoT in Healthcare By 2020."

Source: Mohanty 2016, CE Magazine July 2016

“The global market of IoT based connected cars is expected to reach $46 Billion by 2020.”

Source: Datta 2017, CE Magazine Oct 2017

IoT Role Includes:
- Traffic management
- Real-time vehicle tracking
- Vehicle-to-Vehicle communication
- Scheduling of train, aircraft
- Automatic payment/ticket system
- Automatic toll collection

**IoT in Smart Energy**

**Internet of Energy**

**IoT Role Includes:**
- Management of energy usage
- Power generation dispatch for solar, wind, etc.
- Better fault-tolerance of the grid
- Services for plug-in electric vehicles (PEV)
- Enhancing consumer relationships

**Market Value by 2025:** $781.66 Billion

Source: Frost & Sullivan

Source: Mohanty 2016, CE Magazine July 2016

Quality, sustainable, uninterrupted energy with minimal carbon footprint.

22nd Dec 2017

IoT Keynote by Prof./Dr. Saraju P. Mohanty
IoT in Smart Agriculture

Climate-Smart Agriculture Objectives:
- Increasing agricultural productivity
- Resilience to climate change
- Reducing greenhouse gas

Smart Agriculture/Farming Market Worth $18.21 Billion By 2025


Source: Maurya 2017, CE Magazine July 2017

Automatic Irrigation System

Source: [http://www.fao.org](http://www.fao.org)
Driving Technologies
Cheap and Compact Sensor Technology


- Biosensor
- Thermal Sensor
- Photo Sensors
- Piezoelectric Sensor
- Image Sensor
- Gas Sensor
- Humidity Sensor
- Motion Sensor

Gas Sensor
Temperature Sensor
Air Quality Sensor
Humidity and Temperature Sensor
Light Sensor
Barometer Sensor
Water Sensor
Dust Sensor

Source: http://wiki.seeed.cc/Sensor/

IoT Keynote by Prof./Dr. Saraju P. Mohanty

22nd Dec 2017
Better Imaging Sensor Technology

Image Sensors

Charged Couple Device (CCD) Sensor

Complementary Metal Oxide Semiconductor (CMOS) Sensors

Passive Pixel Sensor (PPS)

Active Pixel Sensor (APS)

Digital Pixel Sensor (DPS)

Based on Sensing Element

Photodiode-Type APS

Photogate-Type APS

Based on Operation Mode

Linear-Mode APS

Logarithmic-Mode APS

“The global CMOS image sensor market is likely to be worth $10.17 billion by 2020.”


Visible Light Communications (VLC)

- LEDs can switch their light intensity at a rate that is imperceptible to human eye.
- This property can be used for the value added services based on Visible Light Communication (VLC).

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>LiFi</th>
<th>WiFi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>Huge</td>
<td>Limited</td>
</tr>
<tr>
<td>Requires Line of Sight</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>EMI + Hazard Concerns</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Susceptibility to Eavesdropping</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Range</td>
<td>Short</td>
<td>Medium</td>
</tr>
<tr>
<td>Data Density</td>
<td>High</td>
<td>Limited</td>
</tr>
</tbody>
</table>

Source: VLCS-2014

Source: Ribeiro 2017, CE Magazine October 2017
Efficient Media Compression – Better Portable Graphics (BPG)

- BPG compression instead of JPEG?
  - Attributes that differentiate BPG from JPEG and make it an excellent choice include:
    - Meeting modern display requirements: high quality and lower size.
    - BPG compression is based on the High Efficiency Video Coding (HEVC), which is considered a major advance in compression techniques.
    - Supported by most web browsers with a small Javascript decoder.

Variety of Computer Memory

Based on Storage Capability

- Volatile
  - Static RAM (SRAM)
  - Dynamic RAM (DRAM)
  - Twin Transistor RAM (TTRAM)
  - Zero-Capacitor RAM (ZRAM)
  - Thyristor RAM (TRAM)

- Nonvolatile
  - Read-Only Memory (e.g. Programmable ROM (PROM), Erasable PROM (EPROM), Electrically Erasable PROM (EEPROM))
  - Magnetic Storage Hard Disk Drive (HDD)
  - Non-Volatile RAM (NVRAM) (e.g. Flash Memory)
  - Resistive RAM (RRAM or ReRAM)
  - Magnetic or Magnetoresistive RAM (MRAM)
  - Phase-Change RAM (PRAM, PCRAM)
  - Conductive Metal Oxide (CMOX) Memory

Based on Access

- Random-Access Memory (RAM)
- Serial Access Memory (e.g. Shift Registers, Queues)
- Content Addressable Memory (CAM)

The flash memory market is expected to be worth $37.6 worldwide by 2020.


Machine Learning Technology

Artificial Intelligence

Tensor Processing Unit (TPU)

IoT Use:
- Better decision
- Faster response

Source: http://transmitter.ieee.org/impact-aimachine-learning-iot-various-industries/

Source: https://fossbytes.com/googles-home-made-ai-processor-is-30x-faster-than-cpus-and-gpus/

April 2017

IoT Keynote by Prof./Dr. Saraju P. Mohanty
Natural Language Processing (NLP)

- NLP is the computer method to analyze, understand, and derive meaning from human language.
- Enables user to address computers as if they are communicating with a person.

Selected NLP Applications

- Machine Translation
- Information Retrieval
- Text Categorization
- Big Data

Source: https://www.linkedin.com/pulse/natural-language-processing-2016-global-market-forecasts-rane

Source: http://blog.algorithmia.com/introduction-natural-language-processing-nlp/
Cognitive Computing: Not just “right” or “wrong” anymore but “probably”.

- Systems that learn at scale, reason with purpose and interact with humans naturally.
- Learn and reason from their interactions with humans and from their experiences with their environment; not programmed.


Usage:
- AI applications
- Expert systems
- Natural language processing
- Robotics
- Virtual reality
Neuromorphic Computing or Brain-Inspired Computing

### Neuromorphic Architecture

- **Dendrites**
- **Soma**
- **Axon**
- **Synapses**

### Processing Powers

<table>
<thead>
<tr>
<th>Types of Chips</th>
<th>Functions</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional Chips (von Neumann Architecture)</td>
<td>Reliably make precision calculations</td>
<td>Any numerical problem, Complex problems require more amount of energy</td>
</tr>
<tr>
<td>Neuromorphic Chips</td>
<td>Detect and Predict Patterns in complex data using minimal energy</td>
<td>Applications with significant visual/auditory data requiring a system to adjust its behavior as it interacts with the world</td>
</tr>
</tbody>
</table>

Neuromorphic Computing or Brain-Inspired Computing


Application 1: Integrate into assistive glasses for visually impaired people for navigating through complex environments, even without the need for a WiFi connection.

Application 2: Neuromorphic-based, solar-powered “sensor leaves” equipped with sensors for sight, smell or sound can help to monitor natural disasters.

Brain Computer Interface (BCI)

“Currently, people interact with their devices by thumb-typing on their phones. A high-bandwidth interface to the brain would help achieve a symbiosis between human and machine intelligence and could make humans more useful in an AI-driven world.”

-- Neuralink - neurotechnology company - Elon Musk.

Think of it as cloud based peer to peer ledger.

A Blockchain is a cloud based database shared by every participant in a system.

The Blockchain contains the complete transaction or other record keeping.

Stay Tuned to: Puthal, Mohanty 2018, CE Magazine March 2018
Challenges and Research
IoT – Selected Challenges

- Massive Scaling
- Design and Operation Cost
- Energy Consumption
- Security, Privacy, and IP Protection
- Creating Knowledge and Big Data
- Architecture and Dependencies
- Robustness

Source: Mohanty 2016, EuroSimE 2016 Keynote Presentation
Eventually Trillions of Things

High Design and Operation Cost

- The design cost is a one-time cost.
- Design cost needs to be small to make a IoT realization possible.
- The operations cost is that required to maintain the IoT.
- A small operations cost will make it easier to operate in the long run with minimal burden on the budget of application in which IoT is deployed.

“Cities around the world could spend as much as $41 trillion on smart tech over the next 20 years.”

Communication Latency and Energy Consumption

- Connected cars require latency of ms to communicate and avoid impending crash.
  - Faster connection
  - Low latency
  - Lower power

- 5G for connected world: This enables all devices to be connected seamlessly.

- How about 5G, WiFi working together more effectively?

Source: https://www.linkedin.com/pulse/key-technologies-connected-world-cloud-computing-ioe-balakrishnan
Energy Consumption of Sensors, Components, and Systems

During GSM Communications

During WiFi Communications

Battery-Less IoT

Battery less operations can lead to reduction of size and weight of the edge devices.


Go Battery-Less

Source: https://www.technologyreview.com/s/529206/a-batteryless-sensor-chip-for-the-internet-of-things/

Batter-Less SoC

Source: http://rlpvlsl.ece.virginia.edu/node/368

Energy Harvesting and Power Management

Source: http://rlpvlsl.ece.virginia.edu/node/368

IoT Keynote by Prof./Dr. Saraju P. Mohanty

22nd Dec 2017
Safety of Electronics

Smartphone Battery

1. Heating starts.
2. Protective layer breaks down.
3. Electrolyte breaks down into flammable gases.
4. Separator melts, possibly causing a short circuit.
5. Cathode breaks down, generating oxygen.

Source: http://spectrum.ieee.org/semiconductors/design/how-to-build-a-safer-more-energydense-lithiumion-battery

Thermal Runaway in a Lithium-Ion Battery

IoT Keynote by Prof./Dr. Saraju P. Mohanty

22nd Dec 2017
Energy Storage - High Capacity and Safer Needed

(Silicon Anode) (Lithium Nickel Cobalt Aluminum Oxide - NCA) Cathode

Source: http://spectrum.ieee.org/semiconductors/design/how-to-build-a-safer-more-energydense-lithium-ion-battery

(Ceramic) Separator


Fuel oxidizing enzymes:
Glucose Oxidase
Glucose Dehydrogenases

Oxygen reducing enzymes:
Laccase
Bilirubin Oxidase
Ascorbate Oxidase

Enzymatic Biofuel Cell

Source: https://www.nytimes.com/2016/12/11/technology/designing-a-safer-battery-for-smartphones-that-wont-catch-fire.html

Solid Polymer Lithium Metal Battery

Source: http://spectrum.ieee.org/semiconductors/design/how-to-build-a-safer-more-energydense-lithium-ion-battery

Microbial Fuel Cell (MFC)

Fuel Cell Car

Source: https://www.nytimes.com/2016/12/11/technology/designing-a-safer-battery-for-smartphones-that-wont-catch-fire.html

22nd Dec 2017

IoT Keynote by Prof./Dr. Saraju P. Mohanty
Huge Amount of Data

What Happens in an Internet Minute?

Estimated Data Generated per Day:
2.5 quintillion bytes

And Future Growth is Staggering

IoT Keynote by Prof./Dr. Saraju P. Mohanty
Security, Privacy, and Copyright

Hardware Trojan

IoT Keynote by Prof./Dr. Saraju P. Mohanty
Cybercrime: Top 20 Countries

- **United States of America**: 23%
- **China**: 9%
- **Germany**: 6%
- **Brazil**: 4%
- **Britain**: 5%
- **Spain**: 4%
- **Italy**: 3%
- **France**: 3%
- **Turkey**: 3%
- **Poland**: 3%
- **India**: 3%
- **Canada**: 2%
- **Japan**: 2%
- **Taiwan**: 2%
- **South Korea**: 2%
- **Mexico**: 2%
- **Argentina**: 1%
- **Australia**: 1%
- **Israel**: 1%
- **All Other Countries**: 19%

Source: [https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/](https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/)

- Cybercrime damage costs to hit $6 trillion annually by 2021
- Cybersecurity spending to exceed $1 trillion from 2017 to 2021


22nd Dec 2017

IoT Keynote by Prof./Dr. Saraju P. Mohanty
Security in Communications Technology

Routing Attacks
Malicious Injection
Denial-of-Service (DoS) Attacks

IoT Keynote by Prof./Dr. Saraju P. Mohanty
Security - Systems ...

Power Grid Attack


Source: http://money.cnn.com/2014/06/01/technology/security/car-hack/

Source: http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/
Selected Attacks on a Typical CE System – Security, Privacy, IP Right

Diverse forms of Attacks, following are not same: System Security, Information Security, Information Privacy, System Trustworthiness, Hardware IP protection, Information Copyright Protection.

Include additional hardware components, but perform DVFS like technology for energy and performance optimization.


Light-Weight Cryptography (LWC)

Secure Digital Camera (SDC)

Better Portable Graphics (BPG)
Malicious Design Modifications Issue

Information may bypass giving a non-watermarked or non-encrypted output.

Hardware Trojans

Input → Watermarking and/or Cryptography Processor → Protected/Secure Information

Unprotected/Unsecure Information → Trojan → Select → Output


Provide backdoor to adversary. Chip fails during critical needs.
Trojan Secure Digital Hardware Synthesis

HLS Library Comprising of Module info from Two Vendors

- Datapath Resource configuration ($R_n$)
- Vendor Allocation Type ($A_v$)
- Unrolling Factor ($U$)

Trojan Detection Block

- DMR Scheduling
- Modified Allocation in DMR based on Distinct Vendor Rule

PSO-Driven Exploration for Optimizing Independent Factors Simultaneously

- Optimizing Datapath Configuration
- Optimizing Vendor Allocation Type
- Optimizing Unrolling Factor

Binding

Cost Evaluation

Low Cost Trojan Secured Datapath

Provide backdoor to adversary. Chip fails during critical needs.

Source: Sengupta, Mohanty 2017: TCAD April 2017

22nd Dec 2017

IoT Keynote by Prof./Dr. Saraju P. Mohanty
Memory Attacks

- **Snooping Attacks**: Read confidential information in memory.
- **Spoofing Attacks**: Replace a block with fake information.
- **Splicing Attacks**: Replace a block with a block from another location.
- **Cold Boot Attacks**: Physical access memory to retrieve encryption keys.
- **Replay Attacks**: The value of a block at a given address at one time is written at exactly the same address at a different times; Hardest attack.

Source: Mohanty 2013, Springer CSSP Dec 2013
Memory Security and Protection

Nonvolatile Storage
Source: http://datalocker.com

On-Chip/On-Board Memory Protection
Source: Mohanty 2013, Springer CSSP Dec 2013
RFID Security - Attacks

Selected RFID Attacks

Physical RFID Threats
- Disabling Tags
- Tag Modification
- Cloning Tags
- Reverse Engineering and Physical Exploration

RFID Channel Threats
- Eavesdropping
- Snooping
- Skimming
- Replay Attack
- Relay Attacks
- Electromagnetic Interference

System Threats
- Counterfeiting and Spoofing Attacks
- Tracing and Tracking
- Password Decoding
- Denial of Service (DoS) Attacks

Numerous Applications

Source: Khattab 2017: Springer 2017 RFID Security
RFID Security - Solutions

Selected RFID Security Methods

- Killing Tags
- Sleeping Tags
- Faraday Cage
- Blocker Tags
- Tag Relabeling
- Minimalist Cryptography
- Proxy Privacy Devices

Faraday Cage

E = 0

Source: Khattab 2017, Springer 2017 RFID Security

IoT Keynote by Prof./Dr. Saraju P. Mohanty
NFC Security - Attacks

Selected NFC Attacks

- Eavesdropping
- Data Modification
- Relay Attacks
- Data Corruption
- Spoofing
- Interception Attacks
- Theft

Eavesdropping

Relay Attack
Source: https://www.slideshare.net/cgvwzq/on-relaying-nfc-payment-transactions-using-android-devices

Eavesdropping
NFC Security - Solution

Source: Mohanty 2017, CE Magazine Jan 2017

Flowchart:
- Start
- Get ID from NFC Module from Receiver
- Enter Amount
- Verify Fingerprint Data
- Approved?
  - Yes: Send Data over GSM
  - No: Payer Module
- Approved?
  - Yes: Send Data over NFC P2P
  - No: Payee Module
Autonomous Car – Security Vulnerability

Selected Attacks on Autonomous Cars

Replay

Relay

Jamming

Spoofing

Tracking

Light Detection and Ranging (LiDAR)

Camera

Cars can have 100 Electronic Control Units (ECUs) and 100 million lines of code, each from different vendors – Massive security issues.

Source: Petit 2015: IEEE-TITS Apr 2015


IoT Keynote by Prof./Dr. Saraju P. Mohanty

22nd Dec 2017
Autonomous Car Security – Cryptographic Hardware

Cryptographic Services Engine (CSE) Block

Qorivva MPC564xB/C Family from NXP/Freescale

Microcontroller Unit (MCU)

Interrupt Controller (INTC)

CSE Core

ROM

RAM

Host to CSE Interrupt

Debugger Connected

IP SkyBlue-IF

AES

XBAR-IF

RNG

Core

eDMA

FlexRay

Peripheral Bridge

Secure Firewall

FLASH

Secure FLASH

PB-IF

MI

BIU

UTI

ON/OFF

Test Interface Array

Test Interface BIU

• 32-bit secure core; Frequency: 120 MHz
• 128-bit Advanced Encryption Standard (AES)
• Throughput: 100 Mbit/sec
• Latency per operation: 2μs


IoT Keynote by Prof./Dr. Saraju P. Mohanty

22nd Dec 2017
Smart Healthcare - Security and Privacy Issues

Selected Smart Healthcare Security/Privacy Challenges

- Data Eavesdropping
- Data Confidentiality
- Data Privacy
- Location Privacy
- Identity Threats
- Access Control
- Unique Identification
- Data Integrity
**Smart Healthcare Security**

### Insulin Delivery System

- **Glucose Level**
- **Continuous Glucose Sensor**
- **Glucose Meter**
- **Remote Control**
- **Insulin Pump**

**Rolling Code Encoder in Remote Control**

- **Remote Control’s Sequence Counter**
- **Information Bits** (i.e., control command)

**Encryption**

- **Transmitted Data**

- **Key**

**Rolling Code Decoder in Insulin Pump**

- **Received Data**
- **Insulin Pump’s Sequence Counter**
- **Received Counter Value**
- **Received Information** (i.e., control command)

**Decryption**

- **Key**

**Security Attacks**

- **Active Attacks: Impersonation**
- **Universal Software Radio Peripheral**

- **Passive Interception**
- **Remote Control**

**Comparison: Whether within a Range**

- **Y**
- **N**

- **Accept**
- **Drop**

**Source:** Li 2011, e-Health 2011

---

**IoT Keynote by Prof./Dr. Saraju P. Mohanty**

22nd Dec 2017
Side Channel Attacks – Differential and Correlation Power Analysis (DPA/CDA)

Decision on key guess

Cryptographic device (e.g., smart card and reader)

Control, Cryptexts

Input data

Device under attack (DUA)

Abstract model of the DUA

Statistical Analysis

Input, keyguesses

Decision on key guess
DPA Resilience Hardware - Synthesis Flow

Cryptography Algorithm → Hamming code based concurrent error detection and correction in Galois Field → Uniform switching cell Library → Physical-Attack Tolerant Cryptography Hardware

Cryptography Hardware Architecture Description:
- Module DUT
- AND U1 ....
- XOR U2 R ...
- Adder U3 ....
- Reg U4 ....
- endmodule

Uniform SWitching-Activity Logic Cell Library → Gate Level Synthesis

Synthesized Netlist with Error Correction in Sequential Elements with Uniformly Switching Cell Library

Source: Mohanty 2013, Elsevier CEE 2013
Firmware Security

Secure Flash Programming

Secure Off-Line Environment

Private Key

Hash

Sign (RSA)

SW Image + Signature

SW Image

FLASH

Secure Flash Programming

SW Image + Signature

Hash

Signature

Verify (RSA)

Generated Hash

Reference Hash

Public Key

Compare

Run OS

Report Error


IoT Keynote by Prof./Dr. Saraju P. Mohanty
“Film piracy cost the US economy $20.5 billion annually.”

Source: [http://www.ipi.org/ipi_issues/detail/illegal-streaming-is-dominating-online-piracy](http://www.ipi.org/ipi_issues/detail/illegal-streaming-is-dominating-online-piracy)
Copyright Protection Hardwares – DCT Domain Watermarking

Datapath Architecture

Hardware Layout

Physical Design Data
Total Area: 16.2 sq mm
No. of Transistors: 1.4 million
Power Consumption: 0.3 mW

Source: Mohanty 2006, TCASII May 2006

IoT Keynote by Prof./Dr. Saraju P. Mohanty

22nd Dec 2017
Copyright Protection Hardware – MPEG-4 Video Watermarking

Video Watermarking Architecture: Simulink Model

Video Watermarking Architecture Datapath

FPGA Prototyping
Throughput: 44 frames/sec
Logic Elements in FPGA Prototyping: 28322

Source: Mohanty 2011, JSS May 2011
DRM Hardware - Secure Better Portable Graphics (SBPG)

Idea of Secure BPG (SBPG)

High-Efficiency Video Coding Architecture

Simulink Prototyping
Throughput: 44 frames/sec
Power Dissipation: 8 nW


IoT Keynote by Prof./Dr. Saraju P. Mohanty

22nd Dec 2017
Hardware IP Right Infringement

Chip at Original Design House \(\rightarrow\) Chip at Another Design House \(\rightarrow\) ? Who Owns ?

Company A \(\rightarrow\) Company B


Hardware IPR Infringement

- False Ownership Claim
- Sub-licensing
- Piracy (Reverse Engineering)

IoT Keynote by Prof./Dr. Saraju P. Mohanty

22nd Dec 2017
Hardware Reverse Engineering

CE System disassembly
Subsystem identification, modification

Chip-Level Modification

Source:

Source:
https://www.slideshare.net/SOURCEConference/slicing-into-apple-iphone-reverse-engineering


Source: http://pic-microcontroller.com/counting-bits-hardware-reverse-engineering-silicon-arm1-processor/

22nd Dec 2017

IoT Keynote by Prof./Dr. Saraju P. Mohanty
Counterfeit Hardware

2014 Analog Hardware Market (Total Shipment Revenue US $)

Wireless Market
$18.9 billion (34.8%)

Consumer Electronics
$9.0 billion (16.6%)

Industrial Electronics
$8.9 billion (16.5%)

Automotive
$8.5 billion (15.7%)

Data Processing
$6.0 billion (11%)

Wired Communications
$2.9 billion (5.4%)

Source: https://www.slideshare.net/rorykingihs/ihs-electronics-conference-rory-king-october

Top counterfeit could have impact of $300B on the semiconductor market.

IoT Keynote by Prof./Dr. Saraju P. Mohanty

22nd Dec 2017
Digital Hardware - Watermark

Integration/Transformation → Scheduling → Allocation (Module and Registers) → Binding → Datapath and Controller → RTL Design → FPGA bitstream

Floorplan → Placement → Routing → Layout → Fabrication

Higher abstraction level – Architecture design
Mid abstraction level – RTL
Lower abstraction level – Physical design

Source: Mohanty 2017: CE Magazine October 2017
Digital Hardware Synthesis to Prevent Reverse Engineering

Obfuscation – Intentional modification of the description or the structure of electronic hardware to conceal its functionality for making reverse-engineering difficult.

Source: Sengupta, Mohanty 2017, TCE November 2017

22nd Dec 2017

IoT Keynote by Prof./Dr. Saraju P. Mohanty
PUFs don’t store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.

 Silicon manufacturing process variations are turned into a feature rather than a problem.

Source: Mohanty 2017, Springer ALOG 2017
Design Flow
IoT – Design Flow

1. Concept
2. High Level Design
3. Component Level Design
4. Design Analysis
5. Prototyping


IoT Keynote by Prof./Dr. Saraju P. Mohanty
22nd Dec 2017
IoT – Design Flow

6. Field Testing
7. Release of Beta Version
8. Production
9. Release and Documentation

# Hardware for IoT

## Embedded Systems and Boards
- **Arduino Yun**: ATmega32u4 and Atheros AR9331 (for Linux)
- **Raspberry Pi 3**: Broadcom BCM2837 and ARM Cortex-A53 64-b Quad Core
- **BeagleBone Black**: AM335x ARM Cortex-A8
- **Pinocchio**: ATmega256RF2
- **U DOO**: Freescale i.MX 6 ARM Cortex-A9 and Atmel SAM3X8E ARM Cortex-M3
- **Samsung Artik 10**: ARM A15x4 and A7x4

## Wearable Devices and Gadgets
- **Samsung Gear 2**: Samsung Gear 2
- **FitBit Flex**: FitBit Flex
- **FLORA**: FLORA
- **iWallet**: iWallet

## Table: Hardware Specifications

<table>
<thead>
<tr>
<th>Features</th>
<th>Processor/Microcontroller</th>
<th>Graphics Processing Unit</th>
<th>Clock Speed</th>
<th>Size</th>
<th>Memory</th>
<th>RAM</th>
<th>Supply Voltage</th>
<th>Listed Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>SparkFun Blynk Board</td>
<td>Tensilica L106 32-b</td>
<td>No</td>
<td>26 MHz</td>
<td>51 mm x 42 mm</td>
<td>4 MB</td>
<td>128 KB</td>
<td>5 V via micro-USB/Li-Po connector and charging circuit</td>
<td>US$29.95</td>
</tr>
<tr>
<td>Arduino Yun</td>
<td>ATmega32u4 and Atheros AR9331 (for Linux)</td>
<td>No</td>
<td>16 MHz and 400 MHz</td>
<td>73 mm x 53 mm</td>
<td>32 KB and 16 MB + micro-SD</td>
<td>64 MB DDR2</td>
<td>5 V via micro-USB</td>
<td>US$58</td>
</tr>
<tr>
<td>Raspberry Pi 3</td>
<td>Broadcom BCM2837 and ARM Cortex-A53 64-b Quad Core</td>
<td>VideoCore IV @ 300/400 MHz</td>
<td>1.2 GHz</td>
<td>85 mm x 56 mm</td>
<td>Micro-SD</td>
<td>1 Gb LPDDR2</td>
<td>5 V via micro-USB</td>
<td>US$35</td>
</tr>
<tr>
<td>cloudBit</td>
<td>Freescale i.MX233 (ARM926EJ-S core)</td>
<td>No</td>
<td>454 MHz</td>
<td>55 mm x 19 mm</td>
<td>Micro-SD slot with 4-GB micro-SD</td>
<td>64 MB</td>
<td>5 V via micro-USB</td>
<td>US$59.95</td>
</tr>
<tr>
<td>Photon</td>
<td>STM32F205 120MHz ARM Cortex M3</td>
<td>No</td>
<td>120 MHz</td>
<td>36.5 mm x 20.3 mm</td>
<td>1 MB</td>
<td>128 KB</td>
<td>5 V via micro-USB</td>
<td>US$19</td>
</tr>
<tr>
<td>BeagleBone Black</td>
<td>AM335x ARM Cortex-A8</td>
<td>PowerVR SGX530</td>
<td>1 GHz</td>
<td>86 mm x 56 mm</td>
<td>4 GB 8-b eMMC, micro-SD</td>
<td>512 MB DDR3</td>
<td>5 V via mini-USB</td>
<td>US$49</td>
</tr>
<tr>
<td>Pinocchio</td>
<td>ATmega256RF2</td>
<td>No</td>
<td>16 MHz</td>
<td>70 mm x 25 mm</td>
<td>256 KB</td>
<td>32 KB</td>
<td>5 V via micro-USB/Li-Po connector and charging circuit</td>
<td>US$109</td>
</tr>
<tr>
<td>UDOO</td>
<td>Freescale i.MX 6 ARM Cortex-A9 and Atmel SAM3X8E ARM Cortex-M3</td>
<td>Vivante GC 2000 for 3-D + GC 355 for 2-D (vector graphics) + GC 320 for 2-D</td>
<td>1 GHz</td>
<td>110 mm x 85 mm</td>
<td>Micro-SD</td>
<td>1 Gb DDR3</td>
<td>12 V</td>
<td>US$135</td>
</tr>
<tr>
<td>Samsung Artik 10</td>
<td>ARM A15x4 and A7x4</td>
<td>Mali-T628 MP6 core</td>
<td>1.3 GHz and 1.0 GHz</td>
<td>39 mm x 29 mm</td>
<td>16 GB</td>
<td>2 Gb LPDDR3</td>
<td>3.4–5 V</td>
<td>US$100</td>
</tr>
</tbody>
</table>

Source: Singh 2017, CE Magazine, April 2017

---

**IoT Keynote by Prof./Dr. Saraju P. Mohanty**

22nd Dec 2017
Software for IoT

- Platforms
  - Temboo
  - Kaa
  - Carriots
  - Ubidots
  - ThingSpeak
  - Artik Cloud
  - Pinoccio
  - Smartliving
  - Samsung ARTIK

- Languages
  - C/C++
  - Java
  - HTML5
  - Javascript
  - Python

Source: Singh 2017, CE Magazine, April 2017
Tools and Solutions
Traditional controllers and processors do not meet IoT requirements, such as multiple sensor, communication protocol, and security requirements.

Existing tools are not enough to meet challenges such as time-to-market, complexity, cost of IoT.

Can a framework be developed for simulation, verification, and optimization:

- of individual (multidiscipline) “Things”
- of IoT Components
- of IoT Architecture
IoT Simulators

Selected IoT Simulators

- Bevywise IoT Simulator
- CUPCARBON
- IoTIFY
- Meshify
- Node-RED
- NetSim
- SimpleIoT Simulator
About
- CUPCARBON is a smart city and Internet of Things Wireless sensor network simulator (SCI-WSN)

Objective
- Design, Visualize, Debug
- Validate distributed algorithms
- Create environmental scenarios

Environments
- Design of mobility scenarios and the generation of natural events such as fires and gas as well as the simulation of mobiles such as vehicles and flying objects (e.g. UAVs, insects, etc.).
- A discrete event simulation of WSNs which takes into account the scenario designed on the basis of the first environment.

Source: http://www.cupcarbon.com/
About:
- Node-RED is a flow-based IoT Simulator.
- It is a programming tool for wiring together hardware devices, APIs and online services in new ways.
- The light-weight runtime is built on Node.js, taking full advantage of its event-driven, non-blocking model.

Editor:
- Browser-based editor.
- The flows created in Node-RED are stored using JSON which can be easily imported and exported for sharing with others.

Advantages:
- Available for smaller computing devices such as Raspberry Pi.
- It takes moments to create cloud applications that combine services from across the platform.
Related Buzzwords
Some related Buzzwords

- Internet of Things (IoT)
- Internet of Everything (IoE)
- Smarter Planet
- Machine to Machine (M2M)
- The Fog
- Trillion Sensors (Tsensors)
- Industry 4.0 (Automation and Data Exchange in Manufacturing Technology)
- Cyber Physical Systems (CPS)
- Industrial Internet of Things (IIoT)

Source: Sangiovanni-Vincentelli 2016, ISC2 2016
IoT Vs Sensor Networks

**Wireless Sensor Networks (WSN)**

- WSN is like the eyes and ears of the IoT.
- A network of small wireless electronic nodes which consists of different sensors.
- The purpose is to collect data from the environment.

**IoT**

- IoT in a broad sense is like a brain.
- Store both real world data and can also be used to monitor the real world parameters and give meaningful interpretation.

IoT adds value to data!

Source: Nia 2017, IEEE TETC 2017
Fog and edge computing involve pushing intelligence and processing capabilities closer to where the data originates from "Things" to reduce communication traffic and improve IoT response.

**Edge Computing**
- Dedicated App Hosting
- Embedded OS
- Device management
- Data Service
- Communication

**Cloud Computing**
- Scalability
- Big Data Analytics
- Software as a Service (SaaS)
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Resource Pooling
- Elastic Compute
- Secure Access

**Fog Computing**
- Real-Time Control
- Real-Time Analysis
- Data Ownership Protection
- Secure Multi-Cloud interworking

**Fog**
- Intelligence - LAN, Processing - fog node or IoT gateway.

**Edge**
- Intelligence, Processing, and Communication - Devices like Programmable Automation Controllers (PACs)

Source: https://www.automationworld.com/fog-computing-vs-edge-computing-whats-difference
IoT Vs Cyber Physical Systems (CPS)

Cyber Physical System (CPS)

Source: Mohanty 2016, CE Magazine July 2016
Internet of Every Things (IoE)

People
Connecting people in more relevant, valuable ways

Data
Converting data into intelligence to make better decisions

IoE

Process
Delivering the right information to the right person (or machine) at the right time

Things
Physical devices and objects connected to the Internet and each other for intelligent decision making; often called Internet of Things (IoT)

Conclusions
Conclusions

- IoT has following components: Things, LAN, Cloud, Internet.
- IoT is backbone of smart cities.
- Scalability, Cost, Energy-consumption, Security are some important challenges of IoT.
- Security, Privacy, and Ownership Rights are critical for trustworthy IoT design.
- Physical Unclonable Functions (PUF) emerging as a good security solution.
- Coordination among the various researchers and design engineers is a challenge as IoT is multidisciplinary.
Future Directions

- Energy-Efficient “Thing” design is needed.
- Security and Privacy of Information need more research.
- Security of the CE systems (e.g. UAV, Smart Cars) needs research.
- Safer and efficient battery need research.
- IoT automatic design tool needs research.
- Some IoT simulators exist, but more needed for efficient, accurate, scalable, multi-discipline simulations.
Membership Fee: $20
Student Membership Fee: $10

Benefits Include:
1) A nice color magazine shipped to your doorstep to update you on latest CE
2) Discount in conference registration
3) Networking opportunity with global peers

Society Website: https://cesoc.ieee.org/

Online at: https://cesoc.ieee.org/membership.html
What is TC-VLSI?

A technical committee of IEEE-CS serves as the focal point of the various technical activities within a technical discipline.

TCVLSI is a constituency of the IEEE-CS that oversees various technical activities related to VLSI.

Key People
Chair
Saraju P. Mohanty, University of North Texas

Vice Chair for Conferences –
Jia Di, University of Arkansas

Treasurer –
Hai (Helen) Li, Duke University

Vice Chair for Membership –
Dhruka Ghati, Oriental University Indore, India

Vice Chair for Liaison –
Nagi Naganathan, Avago Technologies

Vice Chair Outreach and Webmaster –
Mike Borowczak, University of Wyoming

Newsletter EiCs –
Saraju P. Mohanty, University of North Texas

Anirban Sengupta, Indian Institute of Technology Indore

Past Chair –
Joseph Cavallaro, Rice University

TCVLSI Sister Conferences

Sponsored

ARITH: www.arithsymposium.org

ASAP: http://www.asapconference.org/

ASYNC: http://asyncsymposium.org/

iNIS: http://www.ieee-inis.org

ISVLSI: http://www.isvlsi.org

IWLS: http://www.iwls.org

MSE: http://www.mseconference.org

SLIP: http://www.sliponline.org

ECMSM: http://ecmsm2017.mondragon.edu/en

Technically Co-Sponsored

ACSD: http://pn2017.unizar.es/

VLSID: http://vlsidesignconference.org

Technical Scope
Various aspects of VLSI design including design of system-level, logic-level, and circuit-level, and semiconductor processes

TCVLSI Offers
- Student travel grants
- Best paper awards
- Timely CFP info
- Free membership
- Venue to contribute to VLSI
- Circuits & Systems

Join TCVLSI
It’s free to join @ bit.ly/join-tcvlsi
Hardwares are the drivers of the civilization, even softwares need them.

Thank You !!!

Slides Available at: http://www.smohanty.org