IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

Advanced Technologies: Security in IIoT – Part 2

Dr. Sudip Misra

Professor

Department of Computer Science and Engineering

Indian Institute of Technology Kharagpur

Email: smisra@sit.iitkgp.ernet.in

Website: http://cse.iitkgp.ac.in/~smisra/

Research Lab: cse.iitkgp.ac.in/~smisra/swan/

Security requirements for IIoT

- End-to-end security is the primary requirement of IIoT
- Both horizontal and vertical security are important
- Security of the whole system depends:
  - Security of deployed devices
  - Communication security
  - Data protection
  - Security management

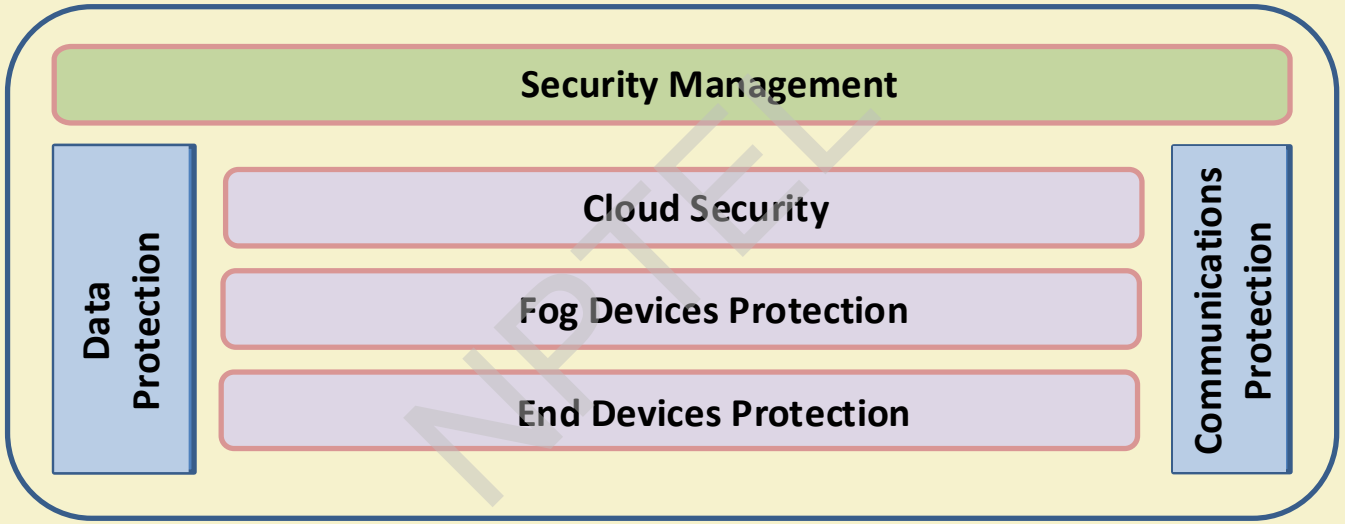
Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

Security Framework for IIoT

- Every industrial application of IoT must have a security framework with its own requirements and solutions
- The framework should address:
  - Different security issues in IIoT
  - Trustworthy IIoT System
  - Major security building blocks of IIoT
  - Techniques for securing each independent block and secure integration

Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

IIoT Security Building Blocks:



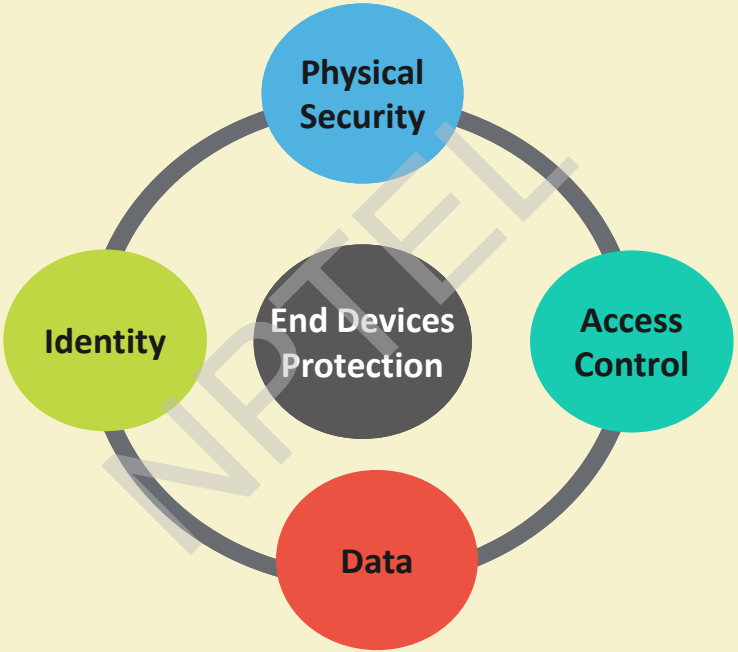
Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium and "Security for the Industrial Internet of Things", Accenture

End Devices Protection - Challenges

- Devices: sensors, actuators, machines and many small embedded devices
- Resource constrained
- Many devices are mobile
- Heterogeneous
- No support for standard cryptographic protocols

Source: “Security for the Industrial Internet of Things”, Accenture

End Devices Protection - Requirement



Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

End Devices Protection - Solutions

- Lightweight cryptographic protocols
  - Energy efficient authentication
  - Lightweight symmetric key cryptography
- IDS and behavior analysis at upper layer devices
  - Malicious behavior detection
  - Abnormal data traffic detection
  - Mitigation using proper actuation unit and signals

Source: Pacheco et al., 2017 and
"Lightweight Cryptography for the Internet of Things", Sony Corporation

Fog Devices Protection

- Devices deployed near to end devices capable of notable computing and storage
- Requirements are same as end devices
- Standard cryptographic protocols for:
  - Authentication between fog devices
  - Authentication between fog devices and cloud
- Lightweight cryptography for security between for authenticating end devices

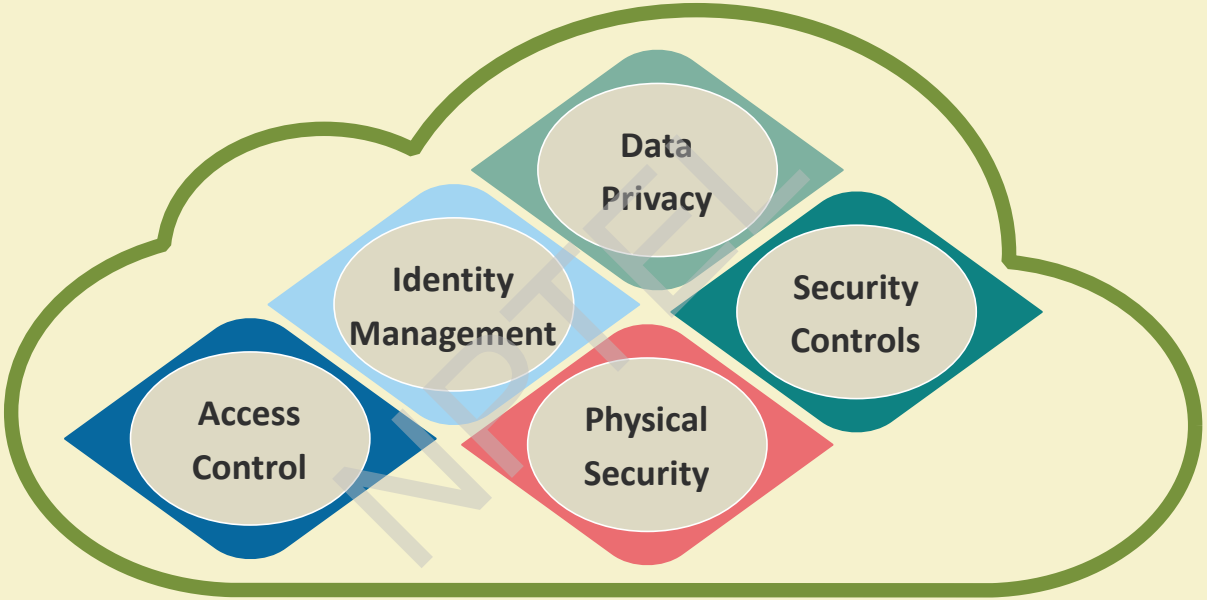
Source: Pacheco et al., 2017

Cloud Security

- Cloud is the data and control hub of the IIoT system
- Security requirement for :
  - Data protection
  - Applications
  - Cloud infrastructure
  - Limiting the service provider access
  - Access control for cloud resources

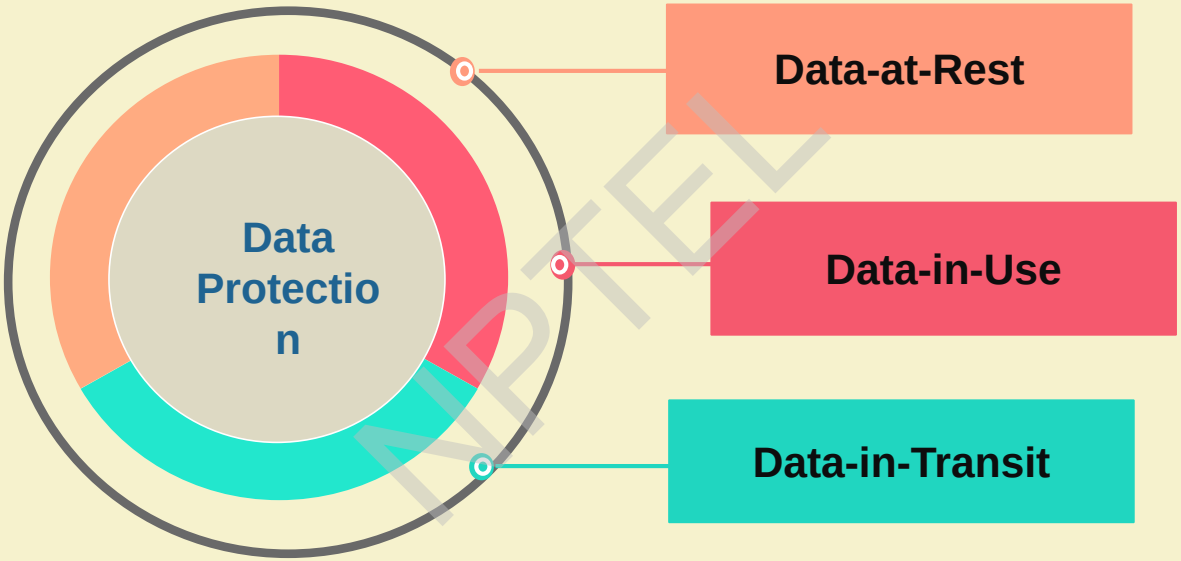
Source: “Cloud computing security”, Wikipedia

Cloud Security



Source: "Cloud computing security", Wikipedia,

Data Protection



Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

Data Protection

- The most sensitive part of IIoT is data
- Different data sources and types with their own lifecycle, risks and security challenges
- Data protection includes:
  - Confidentiality
  - Integrity
  - Availability

Source: “An Introduction to Information Security”, NIST

Communications Protection

- Secure exchange of information between IIoT devices
- Different security risk: sensor data, commands, actuation signals, log reports, configuration messages, etc.
- IIoT traffic and data formats are different from core network
- Protection involves:
  - Communication with devices at the same layer
  - Communication with devices at upper or lower layer

Source: Pacheco et al., 2017

Communications Protection Techniques

- Network access control
- Security gateways
- Network firewalls
- Cryptographic protocols with:
  - Strong mutual authentication
  - Authorization mechanism
  - Data ciphering

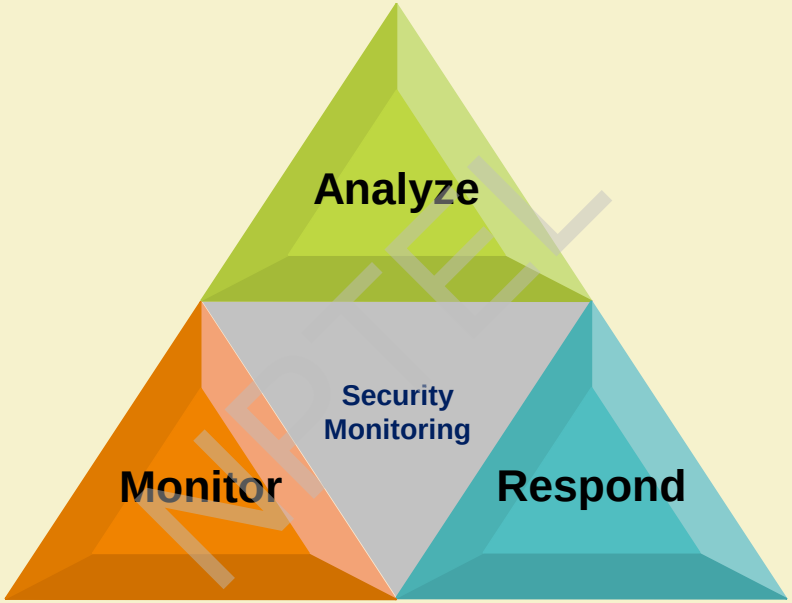
Source: Pacheco et al., 2017

Security Management

- Deals with configurations, periodic updates and managing the security controls
- An active unit, functions from establishment to end of entire IIoT system
- Prevention, detection, analysis and mitigation of security risks
- Performs security monitoring, policy management and updates over time as per standards

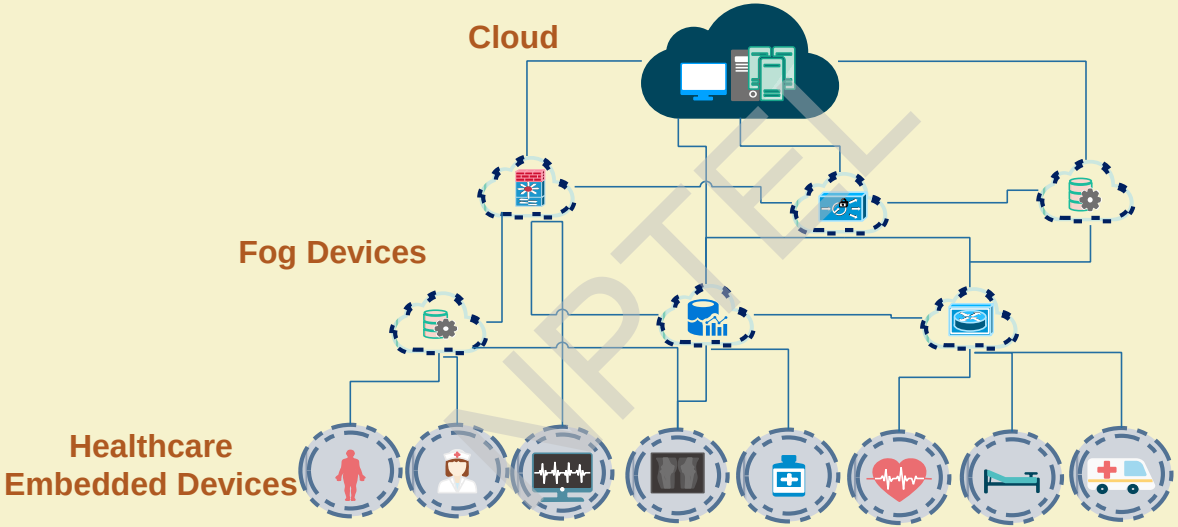
Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

Security Monitoring



Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

Use Case – Healthcare Industry



Source: Al-Joboury et al., 2017

Security in Healthcare IoT

- Devices security:
  - Protection of healthcare embedded devices
  - Protection of fog devices - gateways, processing units, data hubs
  - Cloud security
- Communications Security:
  - Healthcare devices - Fog devices (Lightweight cryptography)
  - Fog devices - Fog devices (Cryptography, Firewalls, Security gateways)
  - Fog devices - cloud (Cryptography, Security applications)

Source: Pacheco et al., 2017

Security in Healthcare IoT (Contd.)

- Data Protection:
  - Device data protection (Password, Signatures, Digital certificates)
  - Communication data (data ciphering and hashing)
  - Data at cloud (Access control lists, Signatures, Digital certificates)
- Security Management:
  - Global security handling at cloud
  - SDN-based security management and monitoring

Source: Pacheco et al., 2017 and Flauzac et al., 2017

Regulatory Standards for IIoT Security

- A security standard helps in achieving a common level of security in industries
- Standards help for manufacturers and vendors to offer services at different level of security
- For IIoT, security standards should include requirements of IT and OT
- Till date, there is no security standards specific to IIoT

Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

Standards Related to IIoT Security

IT Security

- ISO/IEC 154083: Common Criteria for Information Technology Security Evaluation
- ISO series of standards for privacy, framework and regulations
- ISO 27017, NIST SP 800-144, ENISA standard: Cloud security standards
- Common criteria and Federal Information Processing Standard (FIPS)

OT Security

- IEC 62443: Industrial automation and control systems security
- NIST SP 800-82: Security in Industrial Control Systems
- NERC-CIP: Critical infrastructure protection
- IEEE 1686: Standard for Intelligent Electronic Devices Cyber Security Capabilities
- NISTIR 7628: Guidelines for Smart Grid Cyber Security

Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

References

[1] M. Katagi and S. Moriai, "Lightweight Cryptography for the Internet of Things", Sony Corporation, Available Online: https://iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf, Accessed on 23 Aug, 2018.

[2] J. Pacheco, D. Ibarra, A. Vijay, and S. Hariri, "IoT Security Framework for Smart Water Systems", *In proc. Of IEEE/ACS 14th International Conference on Computer Systems and Applications*, 2017.

[3] S. khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions", *Journal of Cloud Computing: Advances, Systems, and Applications,* vol. 6, no. 19, 2017.

[4] I. M. Al-Joboury and E. H. Al-Hemiary, "F2CDM: Internet of Things for Healthcare Network Based Fog-to-Cloud and Data-in-Motion Using MQTT Protocol", *In proc. of International Symposium on Ubiquitous Networking*, 2017.

[5] Z. Bakhshi, A. Balador, and J. Mustafa, "Industrial IoT Security Threats and Concerns by Considering Cisco and Microsoft IoT reference Models", *In proc. WCNC Workshop-2018*, Spain, 15-18 April, 2018.

References

[6] "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium, Available Online: www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf, Accessed on Aug 20, 2018.

[7] "Security for the Industrial Internet of Things", Accenture, Available Online: https://www.accenture.com/in-en/insight-security-industrial-internet-things, Accessed on Aug 20, 2018.

[8] "Securing the Internet of Things: A Proposed Framework", Cicso, Available Online: https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html, Accessed on Aug 20, 2018.

[9] O. Flauzac, C. González, A. Hachani, and F. Nolot, "SDN Based Architecture for IoT and Improvement of the Security", *In proc. of 29th IEEE International Conference on Advanced Information Networking and Applications Workshops*, 2017.

[10] "Cloud computing security", Wikipedia, Available Online: https://en.wikipedia.org/wiki/Cloud_computing_security, Accessed on Aug 20, 2018.

[11] "An Introduction to Information Security", NIST, Available Online: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf, Accessed on Aug 20, 2018.

Thank You!!