Enhancing Dynamic Access Control Based on Device Fingerprints in IoE Networks: Opportunities and Challenges

Samia Oukemeni [1], Karim Zkik [1]

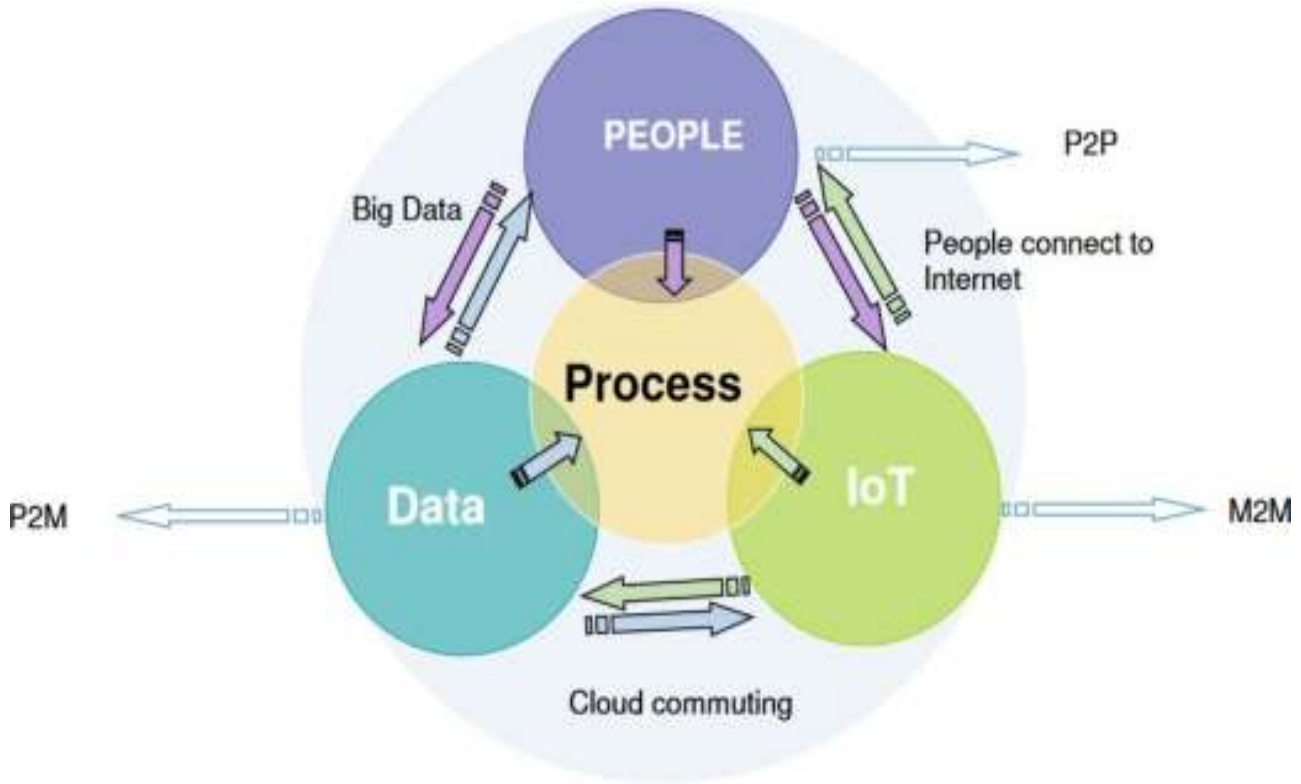
CERADE, ESAIP Ecole d'Ingénieurs
Angers, France

C&ESAR'23

Outline

1. Introduction
2. Access Control Models in IoE Environments
   - AC Challenges in Dynamic Environments
   - Limitations of Traditional AC Models in IoE
   - Dynamic AC Applied to IoE
3. New AC Model Based on Device Fingerprinting
4. Challenges and Trade-offs of DF-based AC Models
5. Conclusion

Internet of Everything



The four pillars of IoE

Challenges of Internet of Everything

- Different devices, processes, and things are connected
- Increased attack surface
- Interoperability
- Issues of increased Cyber-Physical risks
- Difficulties in identifying and responding to threats
- Legacy Systems Vulnerabilities

Challenges of AC in Dynamic Environments

- Navigating access in a network of devices and data
- Adapting to the fast dynamics of IoE ecosystems
- Achieving robust access management with the growing number of connected devices

Answer: Dynamic Access Control:

- ✓ Factor-in user/device identity, situational context, trust levels, and real-time security threat status
- ✓ Adapt and modify access decisions in response to changing conditions
- ✓ Define a granular level of control compared to traditional methods

Traditional AC Models in IoE

Traditional Access Control Models and their limitations

Model	Description	Limitations
Discretionary Access Control (DAC)	Users determine access rights for owned objects	Lacks granularity and not suitable for complex systems
Mandatory Access Control (MAC)	Assigns labels to users and objects to determine access rights	Lacks flexibility, unsuitable for dynamic systems
Role-Based Access Control (RBAC)	Assigns roles to users; Access is granted based on roles	Can become complex and difficult to manage in larger systems

Dynamic Access Control applied to IoE

- Development of new access control models that are more flexible and context-aware
- Access Control models for IoE, in general, have to:
  - Be scalable
  - Be easily managed due to the pervasive number of IoT devices, processes, and users that are involved in authorization activities
  - Support advanced features (e.g. access rights delegation, auditability)
  - Be flexible to adapt to different contexts and needs

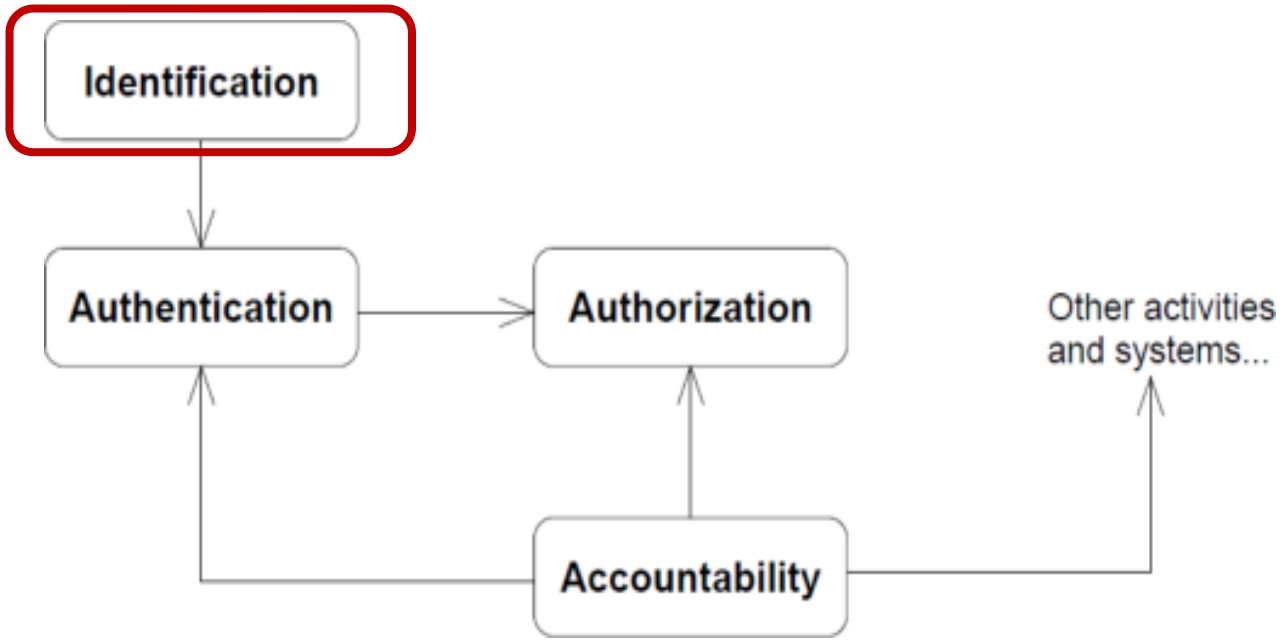
Dynamic Access Control applied to IoE

Access Control Model	Description
Attribute-Based Access Control (ABAC)	Uses attributes for access Suitable for collaborations
Risk-based Access Control	Adjusts privileges based on context and system data Precise access control
Trust-based Access Control	Considers trust levels for user and resource access Based on reputation and behavior
Usage-based Access Control (UCON)	Manages access in distributed environments with obligations conditions, and attribute support
Context-aware Access Control	Gathers and adapts to context changes for a personalized user experience

Dynamic Access Control applied to IoE

Criteria	ABAC	UCON	Context-Aware	Trust-Based	Risk-Based
Fine-grained control	✓	✓	✓	✓	✓
Adaptability and flexibility	✓	✓	✓	✓	✓
Ease of implementation	✓			✓	✓
Complex policy definition	✓	✓			
Predefined levels or thresholds				✓	✓
Additional infrastructure required			✓		

New AC model based on Device Fingerprint



Access Control Steps

Device Fingerprinting in IoE Environments

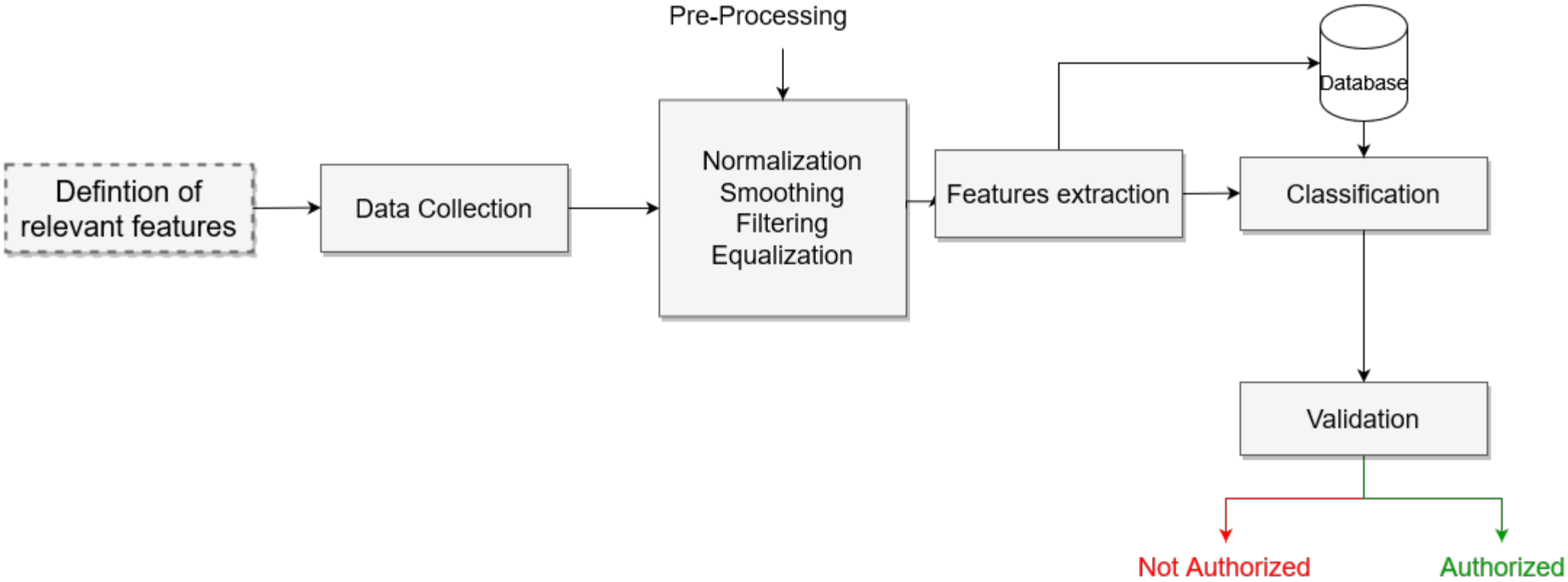
- ***Device fingerprinting is a security mechanism that involves the identification of electronic devices based on unique and distinctive characteristics in their signals or communication patterns***

  - Each IoT device needs a unique identity for authentication
  - Distinctive physical traits serve as unique fingerprints for device identification
  - Establishing trust throughout the device lifecycle

Device Fingerprinting in IoE Environments

- **Unique Identification and Forging Prevention:**
  - Combination of browser data, IP addresses, and hardware details
- **Enhanced Authentication:**
  - Strengthening of user verification & minimizing the risk of unauthorized access
- **Real-time Threat Detection:**
  - Enabling prompt identification of anomalies early intervention against potential threats
- **Safeguarding Against Threats:**
  - Protects against eavesdropping and resource consumption
  - Guards against Sibyl attacks and Masquerade attacks

Device Fingerprint Generation Steps



Device Fingerprinting in IoE

- The features must satisfy certain properties at the physical layer for identification purposes:

1. **Universality**: Every device in the considered device space must have the same features
2. **Uniqueness**: No two devices can have identical fingerprints
3. **Permanence**: The fingerprints must remain consistent over time to uniquely identify a device
4. **Easy to collect**: The identification signals must be easily obtainable with available equipment

Device Fingerprinting in IoE

Study	Methodology	Devices Investigated	Environment	Classification Accuracy
Peng et al	ACTF for feature extraction, 2D-CNN for classification	24 optical fiber Ethernet devices from 4 manufacturers	Indoor	96.29%
Elmaghbub et al	CNN for fingerprint extraction	25 different LoRa devices	Indoor and Outdoor	Indoors: 69-82%, Outdoors: 34-54%
Jian et al	Analysis of 400 GB signal traces from 10,000 radio transmitters	Radio transmitters under different environmental scenarios	Various	Not specified
Ren et al	Use of 12 ZigBee devices and one USRP receiver	Not specified	Not specified	Not specified

Enhancing Access Control using Device Fingerprinting (1)

- **Unique User and Device Identification:**
  - Device-specific fingerprints prevent replication
  - Multi-point verification system makes spoofing difficult

- **Intrinsic Device Properties and Communication Behavior:**
  - Fingerprints based on intrinsic properties
  - Harder to forge or manipulate
  - Only trusted devices access the network
  - Significantly reduces the risk of unauthorized access and security breaches

Enhancing Access Control using Device Fingerprinting (2)

- **Granular Access Control Policies:**
  - Allows granular access control policies
  - Implementation based on user identity and device characteristics
  - Ensures that only authorized devices access sensitive resources

- **Enhanced Security Posture:**
  - Robust defense against MITM attacks and unauthorized intrusions
  - Strong protection against object emulation attacks
  - Combines fingerprinting with encryption and intrusion detection

Integrating Device Fingerprints in AC Systems

- **Key Considerations:**

  - **Usability**: Balance complexity for effective use
  - **Performance**: Ensure speed without compromising security
  - **Accuracy**: Mitigate false positives/negatives for reliability
  - **Heterogeneity**: Adapt to diverse devices in real-time

Integrating Device Fingerprints in AC Systems

- **Trade-offs in DF Integration: Balancing Act**

  - **Cost**: Manage expenses for sustainable implementation at scale
  - **Privacy**: Safeguard sensitive data with encryption and user consent

  Strive for a secure AC system without sacrificing usability and privacy

Conclusion: Comprehensive Insights on DF-based AC

- Comprehensive overview of device fingerprint identification in IoE environments
- **Relevance:** Highlighting its potential to enhance security of AC systems in IoE
- **Limitations:** Factors affecting accuracy like environment, device population, and identification method
- **Recommendations**: Addressing limitations in design and implementation
- **Future Research**: Effectively tackling the six challenges identified in this study and investigate new implementation and architectural approaches of fingerprint identification in Access Control systems, ensuring heightened security and reliability in IoE environments

Merci pour votre attention !

esaip La Salle
ÉCOLE D'INGÉNIEURS

References

- M. Selinger, A. Sepulveda, J. Buchan, Education and the internet of everything (2013). URL: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/education_internet.pdf.
- S. Gusmeroli, S. Piccione, D. Rotondi, A capability-based security approach to manage access control in the internet of things, Mathematical and Computer Modelling 58 (2013) 1189–1205.
- Ouaddah, H. Mousannif, A. A. Elkalam, A. A. Ouahman, Access control in the internetof things: Big challenges and new opportunities, Computer Networks 112 (2017) 237–262.doi:10.1016/j.comnet.2016.11.007.
- R. A. Shaikh, K. Adi, L. Logrippo, S. Mankovski, Risk-based decision method for access control systems, in: 2011 Ninth Annual International Conference on Privacy, Security and trust, IEEE, 2011, pp. 189–192.
- K. Brauer, Authentication and security aspects in an international multi-user network (2011).
- Q. Xu, R. Zheng, W. Saad, Z. Han, Device fingerprinting in wireless networks: Challenges and opportunities, IEEE Communications Surveys & Tutorials 18 (2015) 94–104.
- B. Mahesh, Machine learning algorithms-a review, International Journal of Science and Research (IJSR).[Internet] 9 (2020) 381–386.
- L. Peng, A. Hu, A design of deep learning based optical fiber ethernet device fingerprint identification system, in: ICC 2019-2019 IEEE International Conference on Communications (ICC), IEEE, 2019, pp. 1–6.
- S. Verma, Understanding 1d and 3d convolution neural network: Keras, 2023. URL: https://towardsdatascience.com/understanding-1d-and-3d-convolution-neural-network-keras-9d8f76e29610.
- A. Elmaghbub, B. Hamdaoui, Lora device fingerprinting in the wild: Disclosing rf data-driven fingerprint sensitivity to deployment variability, IEEE Access 9 (2021) 142893–142909.
- T. Jian, B. C. Rendon, E. Ojuba, N. Soltani, Z. Wang, K. Sankhe, A. Gritsenko, J. Dy, K. Chowdhury, S. Ioannidis, Deep learning for rf fingerprinting: A massive experimental study, IEEE Internet of Things Magazine 3 (2020) 50–57.
- Y. Ren, L. Peng, W. Bai, J. Yu, A practical study of channel influence on radio frequency fingerprint features, in: 2018 IEEE International Conference on Electronics and Communication Engineering (ICECE), IEEE, 2018, pp. 1–7.

Enhancing Dynamic Access Control Based on Device Fingerprints for IoE Networks: Opportunities and Challenges

Samia Oukemeni [1], Karim Zkik [1]

CERADE, ESAIP Ecole d'Ingénieurs
Angers, France

C&ESAR'23