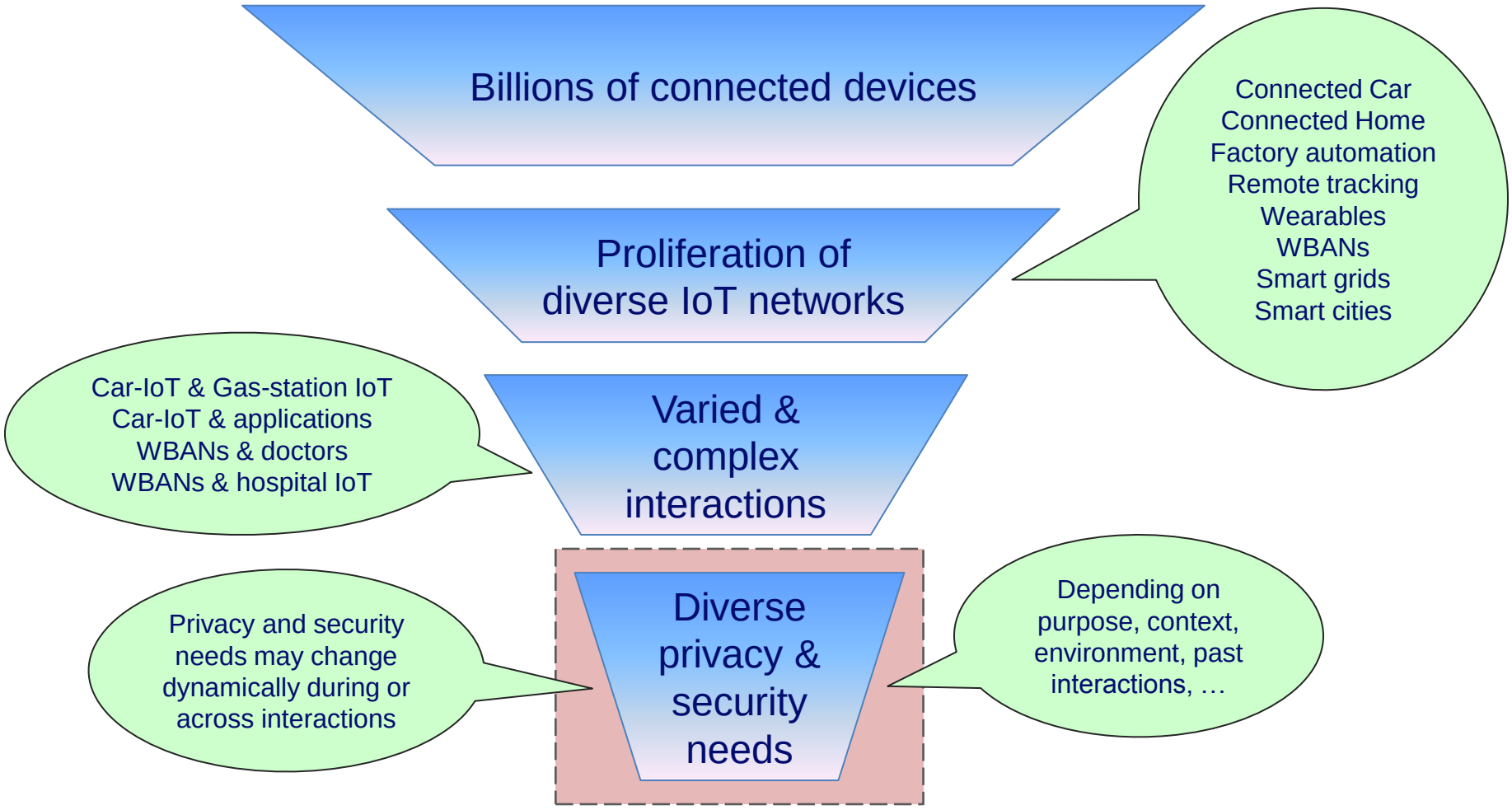
Adaptive and composite privacy and security mechanism for IoT communication

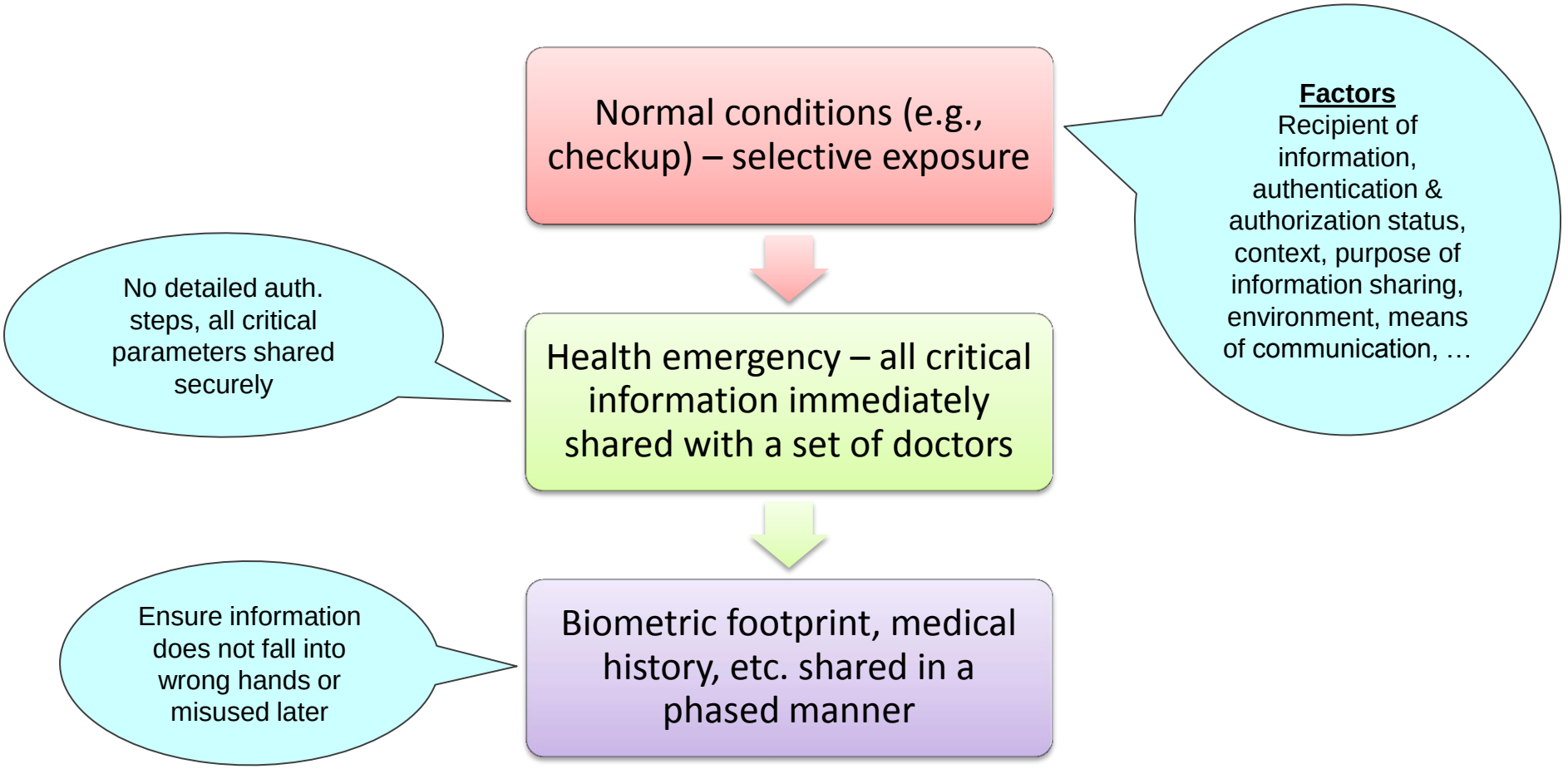
Swaminathan Seetharaman & Sudipta Ghosh

WIPRO
Applying Thought

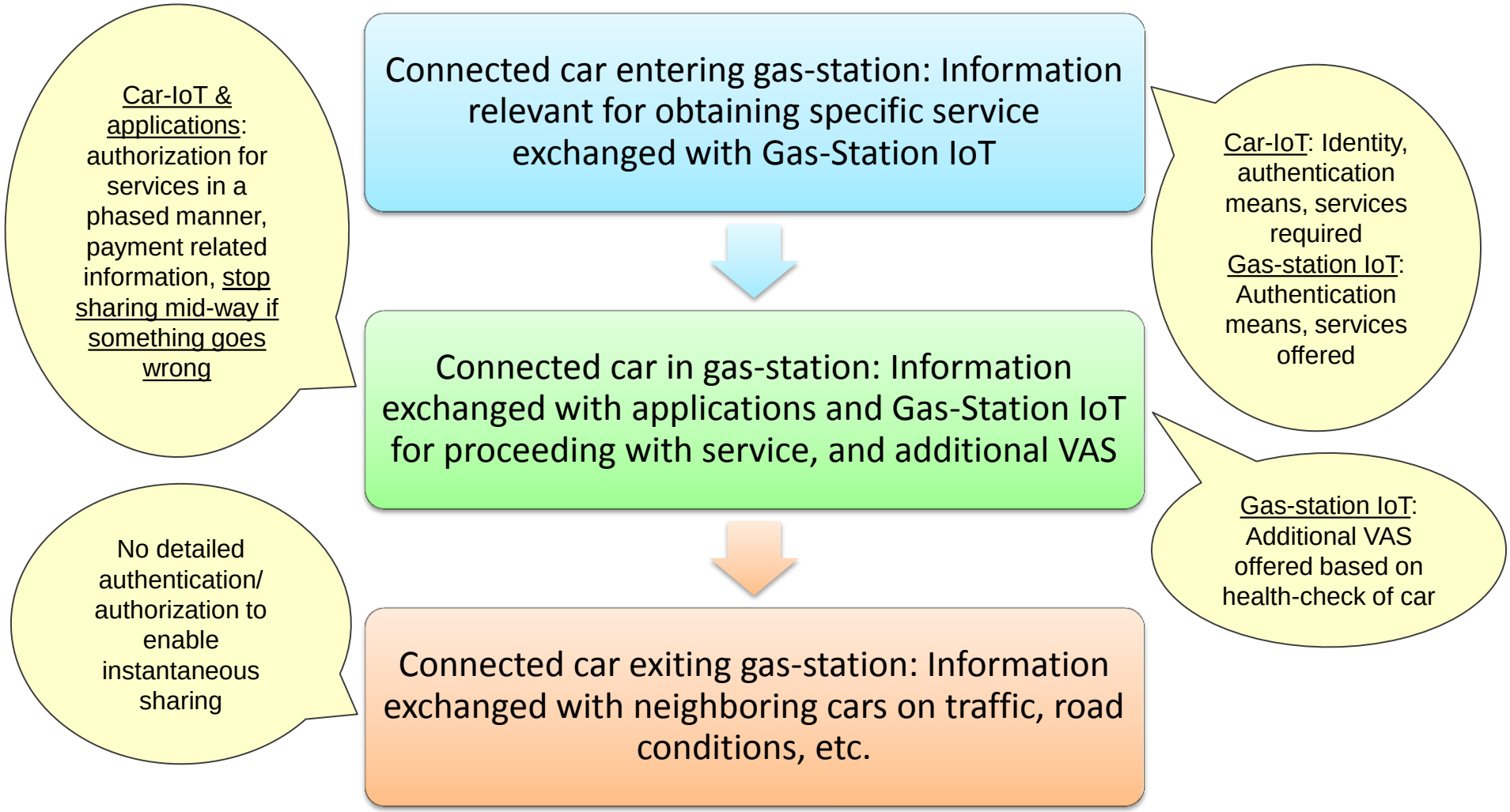
Introduction



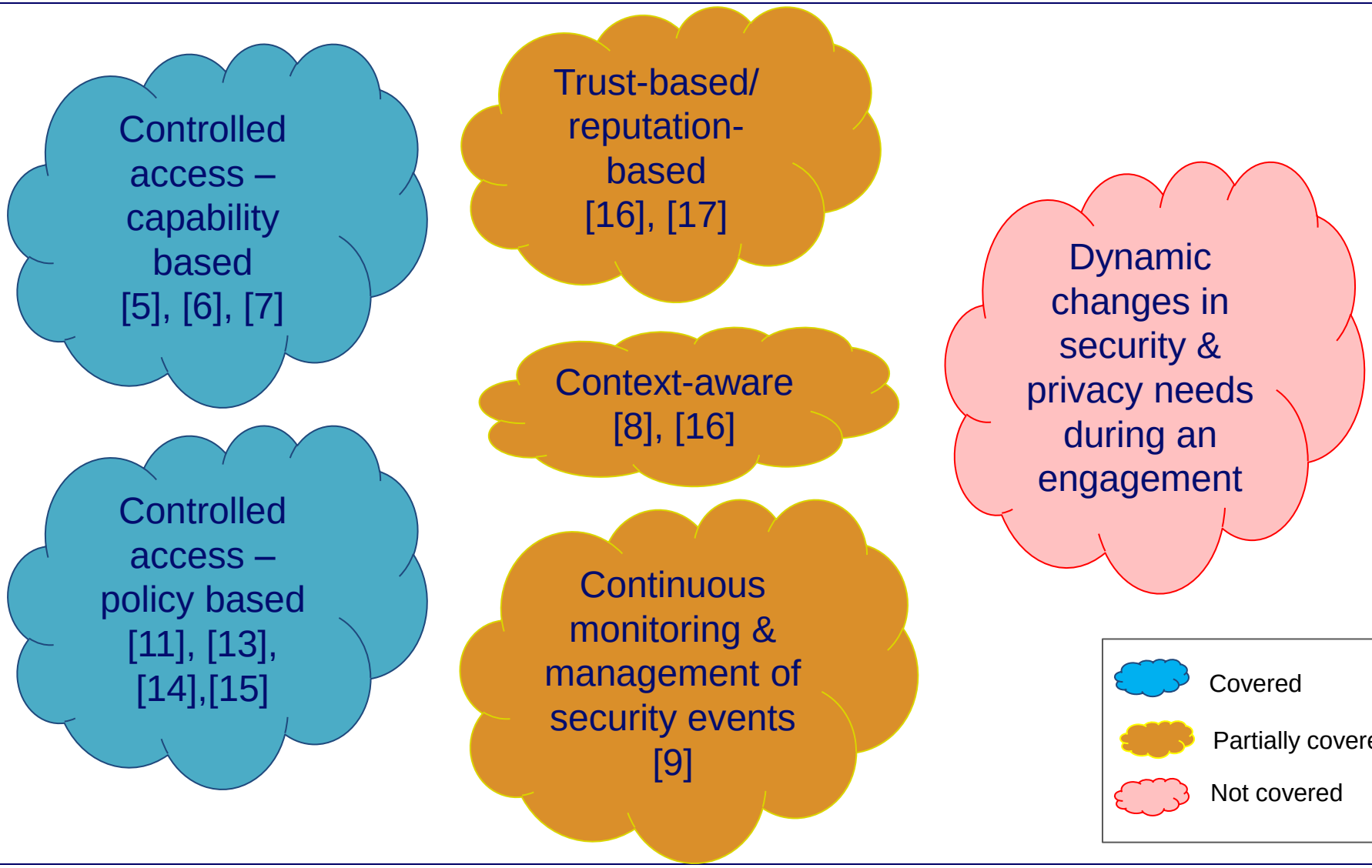
Usecase 1 - WBAN



Usecase 2 - Connected Car



Prior Art


Controlled access – capability based [5], [6], [7]
Trust-based/ reputation-based [16], [17]
Dynamic changes in security & privacy needs during an engagement
Context-aware [8], [16]
Controlled access – policy based [11], [13], [14],[15]
Continuous monitoring & management of security events [9]
Covered
Partially covered
Not covered

Prior Art

Author(s)	Highlights	Limitations
Skarmeta et al [5]	• Distributed capability-based access control mechanism based on digitally signed capability-token	Static and hence unsuitable for changing context and purpose, and for heterogeneous IoT networks with varying capabilities
Gusmeroli et al [6]	• Capability-based access control mechanism • Capability directly identifies the resource(s), the subject to which the rights have been granted, the granted rights, and the authorization chain.	• Requires issuing capabilities to all subjects • Not suitable for dynamically changing security and privacy requirements during progressive interactions.
Xin Huang et al [8]	• Context-aware k-anonymity policy • Anonymizes the identifiers of the data record/user so that it is not distinguishable from other users except when required.	• Privacy settings are not dynamically adapted during an interaction with another entity • Security-related aspects are not addressed.
GAMBAS [11]	• Policy-based privacy mechanism that enables secure exchange of information after authentication, key exchange, etc.	• Does not address the dynamic changes in privacy & security requirements during the course of an IoT interaction.

Prior Art

Author(s)	Highlights	Limitations
Pohls et al [9]	• Framework for security, privacy and trust for smart city IoT networks. • Includes continuous monitoring and management of security events, and automated adaptation of deployed security mechanisms to enable reconfigurations due to context change	• Requires explicit reporting of context change, and handles only a limited set of context parameters • Fails to adapt during the course of an interaction.
Neisse et al [16]	Context-aware and trust-based security & privacy framework Security policies are implemented as ECA rules.	• Does not dynamically adapt to changes in context, trust-level, environment, etc. during the interaction. • Limitations in scalability and deployability for new/unknown service-oriented and inter-IoT interaction scenarios
Gessner et al [17]	A security architecture for authorization, authentication, and privacy based on trust and reputation for IoT networks.	• Does not address dynamic adaptations of the privacy & security mechanism as the interaction progresses. • Peer-to-peer information collection and processing for trust and reputation computation may not scalable as the number of parties grow.

Need for this Paper

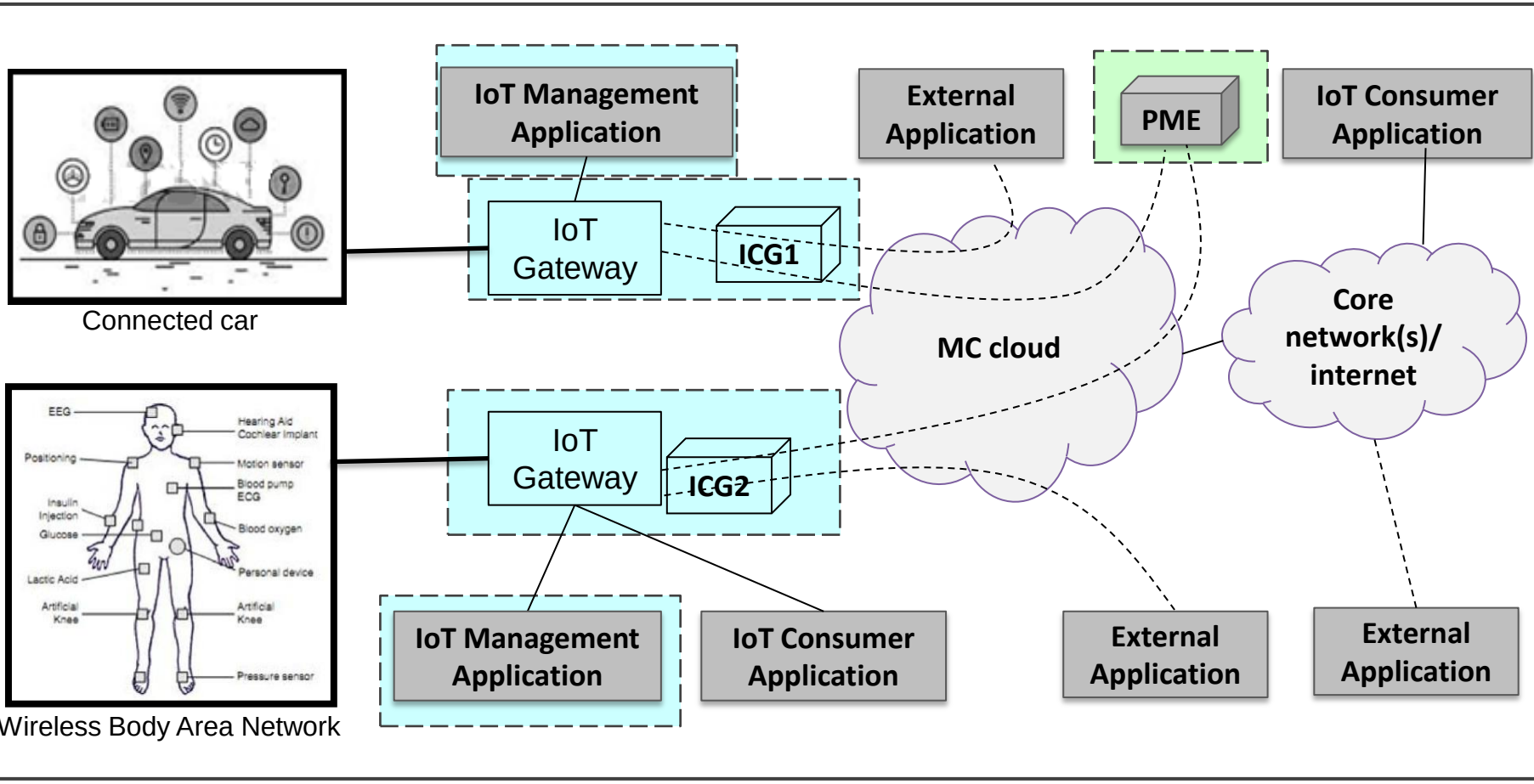
Need for a dynamic, adaptive privacy and security settings taking into consideration the context, purpose, collective past experiences and other factors

Definitions

- **Perception**: Is formed by an entity with regards to the set of possible interactions with a second entity, based on:
  - Own experience
  - Information from other sources and
  - Collective perception

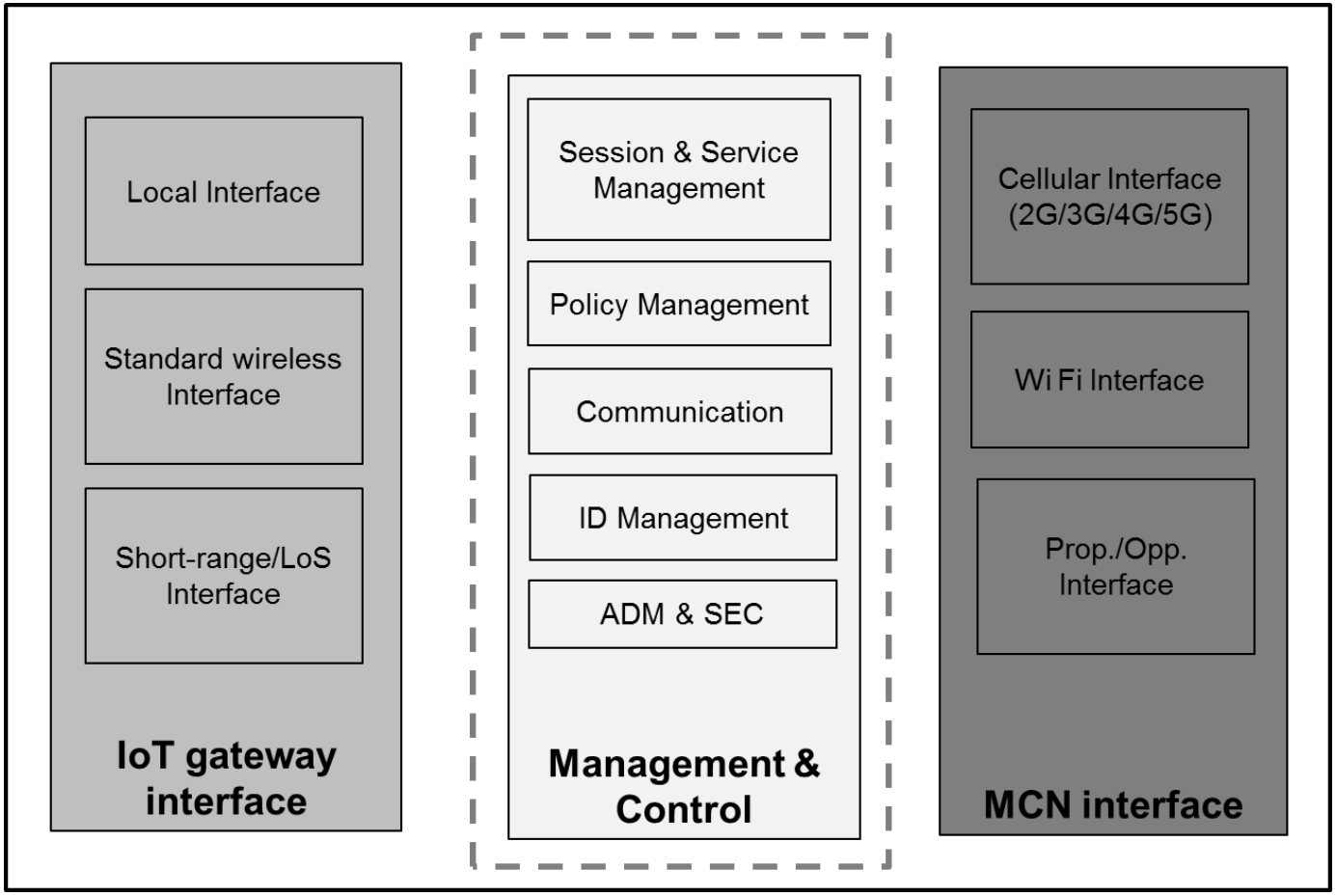
  Perception can evolve before, during and after an interaction.
- **Filter**: Is a mechanism that determines the extent of information to be allowed to pass through.
  - Set of rules and thresholds that will be applied on the messages / contents that are being passed through the filter.
  - Filter can be uni-directional or bi-directional.
- **Engagement**: Represents an interaction session for an IoT network with a second party involving a network (IoT or otherwise) that is interested to obtain or deliver one or more services, exchange information, etc.

Proposed Solution - Architecture



Reference: Ghosh, S. et al [18]

Proposed Solution – ICG Architecture



Reference: Ghosh, S. et al [18]

Proposed Solution - Architecture

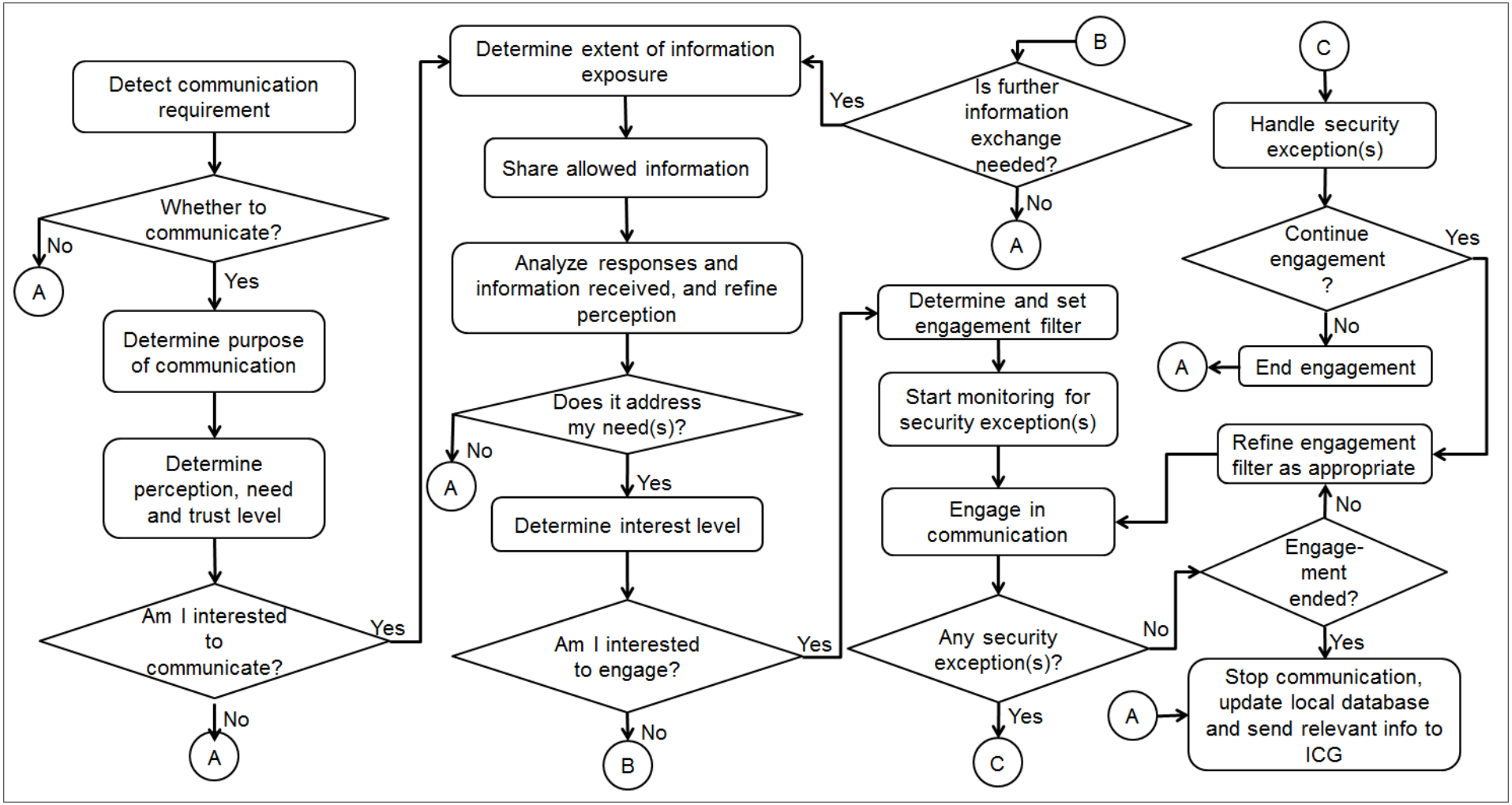
- IoT Gateway: Handles IoT network-specific aspects such as:
  - IoT-function, associated security & privacy at device and IoT-network level
  - Identity of component devices
  - Device and IoT network capability
  - Topology

  Also contains relevant information of neighboring IoT gateways and handles intra-IoT network communication aspects.
- Interconnect Gateway (ICG): Handles all aspects of inter-IoT communication including:
  - Managing the communication channels towards IoT Gateway and MC cloud
  - Session and service management
  - Security and privacy (broader view than IoTGW)
  - Identity management
  - Policy formulation and application
- MC Cloud: Macro-cellular network

Proposed Solution - Architecture

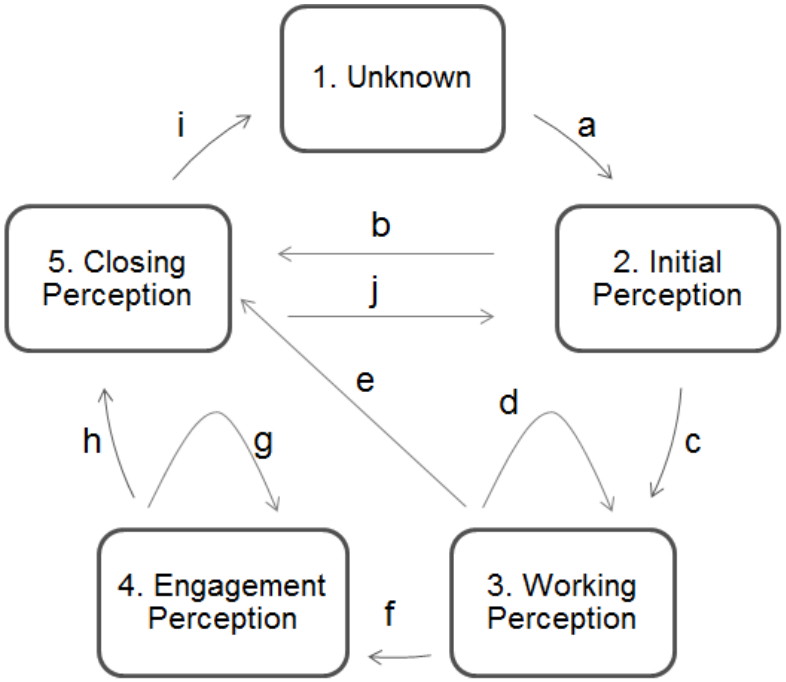
- Perception Management Entity (PME):
  - Collects perception-related inputs (PRI) from different sources
  - Organizes and manages PRI
  - Provides relevant inputs upon request from the ICG.
- IoT Management Application: Manages IoT network functions and policies.
- IoT Consumer Application: Makes use of information from one or more IoT devices and IoT networks to provide service(s) to the user, IoT network, or other entities.
- External Application: Any service-provider or third-party application that may interact with the IoT network.

Proposed Solution - Functioning



Perception Lifecycle

IoTGW Perception Lifecycle



ICG Perception Lifecycle

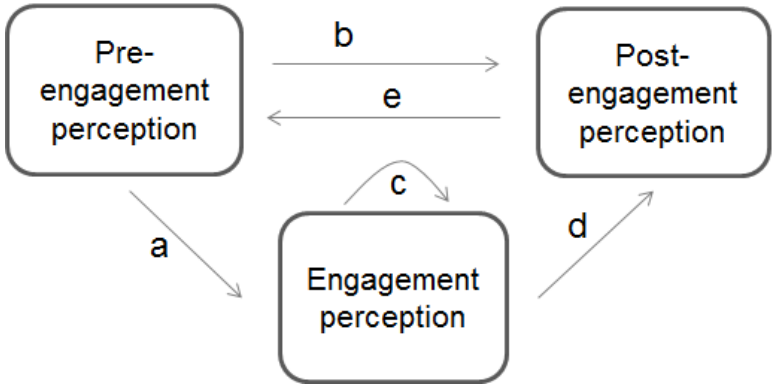
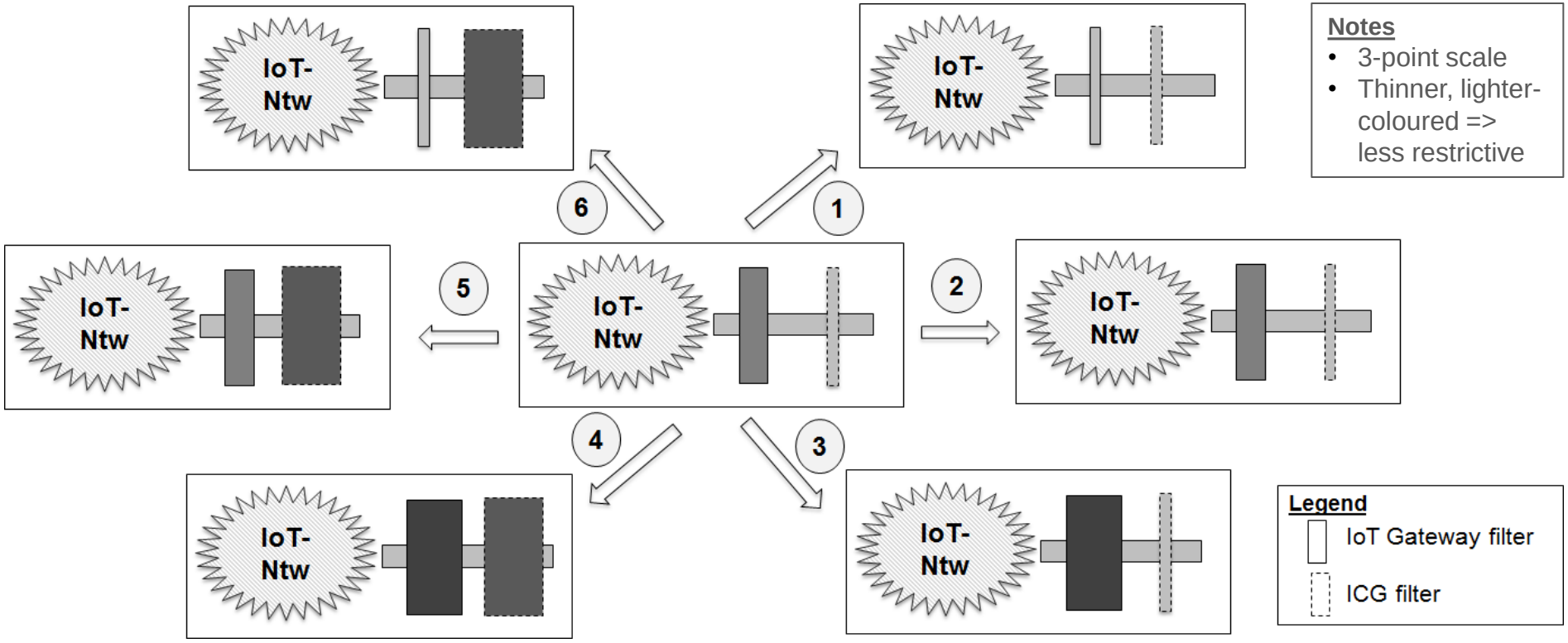


Illustration of Inter-IoT interaction



ICG Filter

- Formed based on perception input from PME, trust assumptions about IoT Gateway, etc.
- Concerned with network-level communication aspects
- Mostly static for a single engagement except for a few exceptions

IoT Gateway Filter

- Formed based on perception input from PME, trust assumptions about the ICG and based on own earlier perception.
- Highly dynamic, and changes continuously during the engagement.

Future Work

- Alignment of IoTGW and ICG perceptions, and correlation of the IoTGW and ICG filters
  - Will it lead to a more intelligent, accurate & optimized handling of security and privacy needs?
- Evaluate the benefits of stateful IoTGW and ICG filters across engagements
  - Taking into account the last filter setting for a similar engagement and the overheads involved.
- Examine security/privacy-related interactions between IoTGW and ICG for very short-lived engagements, and initial interactions with very low latency requirements
- Implement our approach in a real-world setting for connected cars and WBAN
  - Fine-tune the proposed mechanism to function better to enable wider deployability.

Conclusion

Recap

- IoT networks and their interactions to realize services those are new and even unimagined today is likely to proliferate in the years to come.
- Security and privacy requirements will change depending on the context, purpose, etc., and will change dynamically during an engagement.

We have proposed a context-aware, purpose-aware, dynamic, adaptive and composite privacy and security mechanism. The proposed mechanism is highly adaptive and scalable, and hence can fulfill the security and privacy requirements of almost any kind of real-world IoT network.

References

1. https://www.lora-alliance.org/What-Is-LoRa/Technology
2. http://www.dash7-alliance.org/?product=dash7-alliance-protocol-specification-v1-0
3. https://developer.bluetooth.org/TechnologyOverview/Pages/core-specification.aspx
4. Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D., "*Context Aware Computing for The Internet of Things: A Survey*", IEEE Communications Surveys and Tutorials, Volume 16, Issue 1, Feb 2014.
5. Skarmeta, A.F., Hernández-Ramos, J.L., Moreno, M.V., "*A decentralized approach for Security and Privacy challenges in the Internet of Things*", 2014 IEEE World Forum on Internet of Things (WF-IoT), March 2014.
6. Gusmeroli, S., Piccione, S., Rotondi, D., "*IoT Access Control Issues: A Capability Based Approach*", 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, July 2012.
7. P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "*Identity authentication and capability based access control (iacac) for the internet of things*", Journal of Cyber Security and Mobility, vol. 1, no. 4, pp. 309–348, 2013.
8. Xin Huang, Rong Fu, Bangdao Chen, Tingting Zhang, Roscoe, A.W., "*User interactive Internet of things privacy preserved access control*", International Conference for Internet Technology And Secured Transactions, December 2012.
9. Pohls, H.C., Angelakis, V., Suppan, S., Fischer, K., Oikonomou, G., Tragos, E.Z., Diaz Rodriguez, R., Mouroutis, T., "*RERUM: Building a Reliable IoT upon Privacy- and Security- enabled Smart Objects*", IEEE Wireless Communications and Networking Conference Workshops (WCNCW), April 2014.
10. A. Garcia, et al., "*FI-WARE Security: Future Internet Security Core*" in 'Towards a Service-Based Internet', ser. Lecture Notes in Computer Science, vol. 6994. Springer Berlin Heidelberg, 2011, pp. 144–152.

References

11. Generic Adaptive Middleware for Behavior-driven Autonomous Services (GAMBAS) Consortium, "*Privacy Preservation Specification 1*", Public deliverable D3.1.1, September 2012, Available online: http://www.gambas-ict.eu/download/D3.1.1-Privacy-Preservation-Specification-1.pdf?attredirects=0&d=1.
12. D.F. Ferraiolo, D.R Kuhn: Role-Based Access Control. 15th National Computer Security Conference. pp. 554–563, October 1992.
13. Sarkar, C., Nambi, A.U.S.N., Prasad, R.V., Rahim, A., Neisse, R., Baldini, G., "*DIAT: A Scalable Distributed Architecture for IoT*", IEEE Internet of Things Journal, Vol. 2, No. 3, June 2015.
14. Neisse R, et al., "*SecKit: A Model-based Security Toolkit for the Internet of Things*", Computers & Security, June 2015, http://dx.doi.org/10.1016/j.cose.2015.06.002.
15. Neisse, R., Steri, G., Baldini, G., "*Enforcement of Security Policy Rules for the Internet of Things*", IEEE 10th Int. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMob), October 2014.
16. Neisse, R., Steri, G., Baldini, G., Tragos, E., Nai Fovino, I., Botterman, M., "*Dynamic Context-Aware Scalable and Trust-based IoT Security, Privacy Framework*", Book chapter in Internet of Things - From Research and Innovation to Market Deployment, IERC Cluster Book, 2014, pp.199-224.
17. Gessner, D., Olivereau, A., Segura, A.S., Serbanati, A., "*Trustworthy Infrastructure Services for a Secure and Privacy-respecting Internet of Things*", 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2012.
18. Ghosh, S., Seetharaman, S., "*Mechanism for adaptive and context-aware inter-IoT communication",* IEEE International Conference on Advanced Networks and Telecommunication Systems (ANTS), December 2015, in press.

Thank you!

#ICIN2016

WIPRO
Applying Thought