I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing

BlueSky: Towards Convergence of Zero Trust Principles and Score-Based Authorization for IoT Enabled Smart Systems

Safwa Ameer

Institute for Cyber Security (ICS)
Center for Security and Privacy Enhanced Cloud Computing (C-SPECC)
Department of Computer Science
University of Texas at San Antonio

Maanak Gupta
Department of Computer Science
Tennessee Tech University

Smriti Bhatt
Department of Computer Science
Purdue University

Ravi Sandhu

Institute for Cyber Security (ICS)
Center for Security and Privacy Enhanced Cloud Computing (C-SPECC)
Department of Computer Science
University of Texas at San Antonio

ACM Symposium on Access Control Models and Technologies

June 8-10th, 2022

safwa.ameer@utsa.edu

© Safwa Ameer

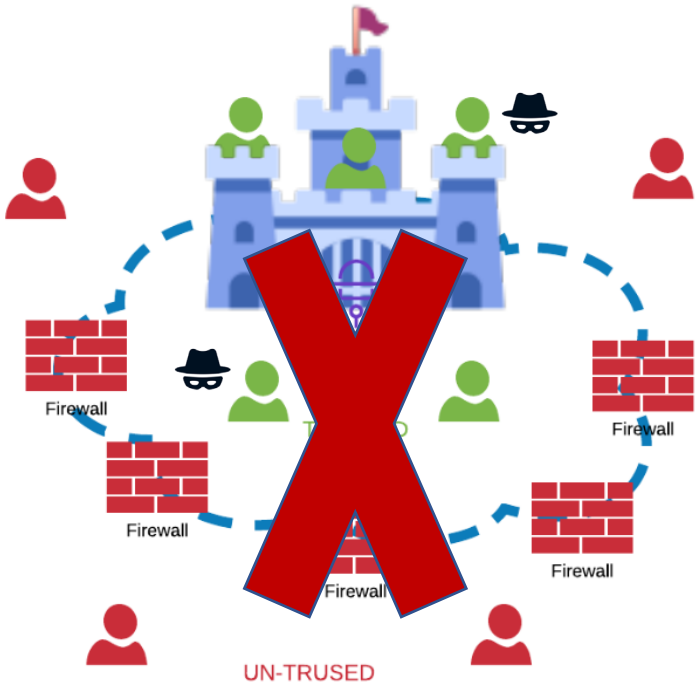
World-Leading Research with Real-World Impact!

UTSA Computer Science

Traditional Security

- The traditional approach to securing an enterprise's infrastructure is to use network perimeter-based protection (known as the castle and moat approach).
- The corporate firewall becomes the moat that encircles and protects the network castle and anyone inside is trusted while the rest of the world is untrusted.

- The inherent weakness in this approach is the de facto classification of inside devices and users as trusted.
- This problem is further aggravated by the growing adoption of SaaS/IaaS cloud services, more remote users, and bring your own device (BYOD) policies.
- This complexity has outstripped legacy methods of perimeter-based network security as there is no single, easily identified perimeter for the enterprise.
- This complexity has led to the development of a new model for cybersecurity known as "zero trust" (ZT) [1].



© Safwa Ameer

Zero Trust Basic Idea

- Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.

- It assumes no implicit trust is granted to assets or user accounts based solely on their physical or network location.

© Safwa Ameer

Our Contribution

In This Paper:

1. We highlight the importance of considering ZT concepts when designing, enforcing, and implementing authorization models.

2. We propose the ZT authorization requirements framework (ZT-ARF).

3. We motivates the need to implement ZT principles when developing access control models for smart IoT systems.

4. We analyze access control requirements in IoT systems and accordingly specify which requirements components from our proposed ZT-ARF we need to include when designing an authorization model for integrated ZT IoT systems.

5. We propose our novel framework for ZT score-based authorization (ZT-SAF).

6. We highlight future research directions and propose a plan for designing, enforcing, and implementing the proposed ZT-SAF in smart connected IoT systems.

© Safwa Ameer

Our Contribution

In This Paper:

1. We highlight the importance of considering ZT concepts when designing, enforcing, and implementing authorization models.

Identify during which part of the design process we need to incorporate the ZT tenets when developing an authorization model for a ZT system.

2. We propose t

3. We motivates the need to implement ZT principles when developing access control models for smart IoT systems.

For this purpose, we provide a structured mapping between the ZT tenets and the PEI models framework .

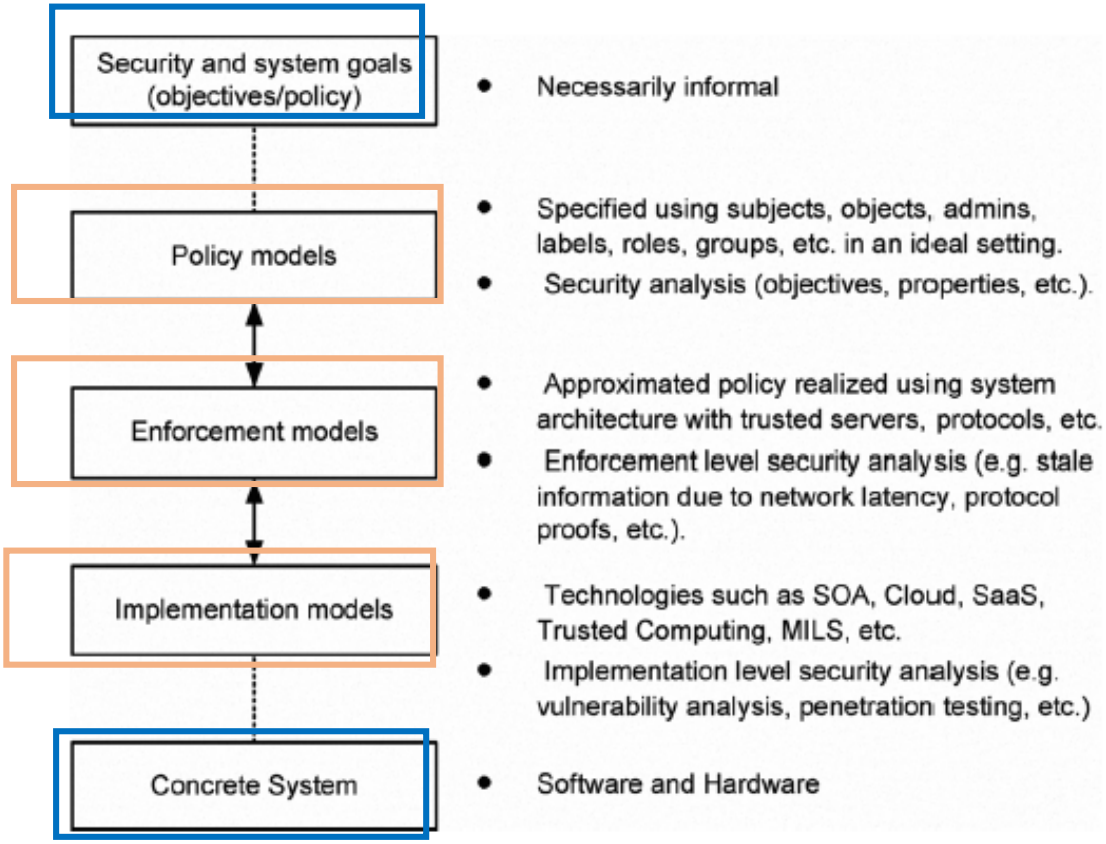
1. We analyze access control requirements in IoT systems and accordingly specify which requirements components from our proposed ZT-ARF we need to include when designing an authorization model for integrated ZT IoT systems.

2. We propose our novel framework for ZT score-based authorization access control policy model (ZT-SAF).

3. We highlight future research directions and propose a plan for designing, enforcing, and implementing the proposed ZT-SAF in smart connected IoT systems.

© Safwa Ameer

The PEI Models Framework:



The PEI Models Framework [2].

© Safwa Ameer

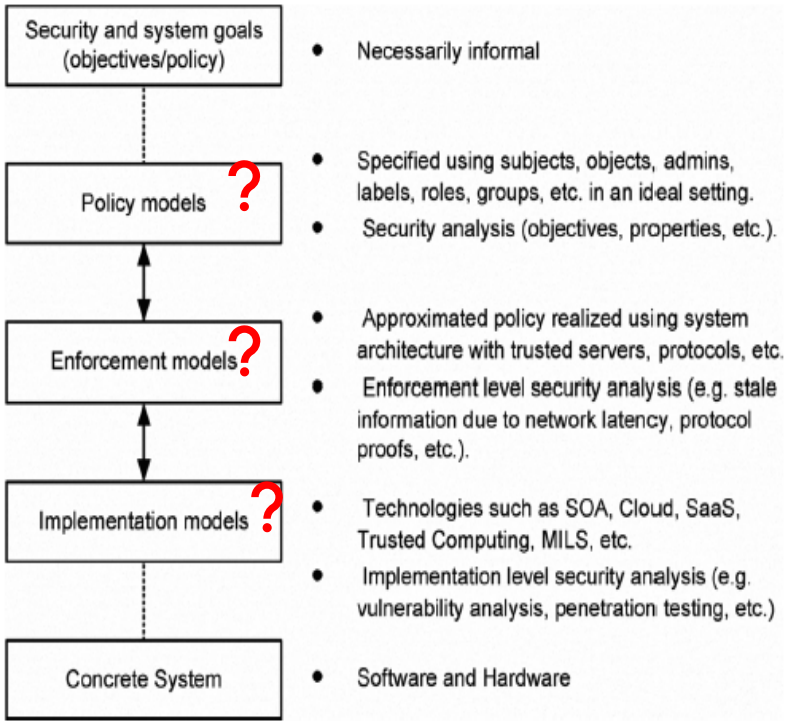
Zero trust Tenets:

- The ZT NIST document [2] offer a way of defining ZT and ZTA in terms of basic tenets that should be adhered to when designing and deploying a ZT system.

© Safwa Ameer

Mapping Between Zero Trust Tenets and The PEI Models Framework Layers

- The question remains, however, when we must consider different tenets? Particularly at which design and implementation stages should we incorporate each tenet into the access control system?



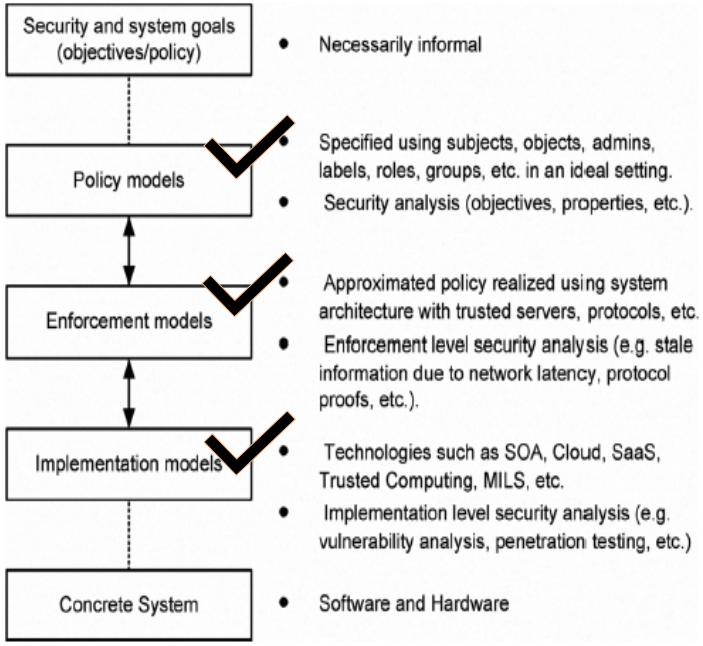
The PEI Models Framework [2].

© Safwa Ameer

Mapping Between Zero Trust Tenets and The PEI Models Framework Layers

Zero Trust Basic Tenets:

- We carefully investigated each tenet in our paper.
- We concluded that when designing **a ZT authorization system**, it is critical to consider the zero trust tenets that we would like to incorporate at the policy, enforcement, and implementation models layers in the PEI framework.
- Although ZT basic tenets are the ideal goals, not all of them may be implemented in their purest form in every system.
- There are no minimum requirements in terms of tenets or principles.
- Different enterprises may choose to fully or partially incorporate some tenets while neglecting others.



The PEI Models Framework [2].

© Safwa Ameer

Our Contribution

In This Paper:

1. We highlight the importance of considering ZT concepts when designing, enforcing, and implementing authorization models. For this purpose, we provide a structured mapping between the ZT tenets and the PEI models framework [2].

2. We propose the ZT authorization requirements framework (ZT-ARF).

which provides a structured view of different authorization requirements to consider when designing a ZT authorization policy model.

4. We motivates the systems.

5. We analyze access control requirements in IoT systems and accordingly specify which requirements components from our proposed ZT-ARF we need to include when designing an authorization model for integrated ZT IoT systems.

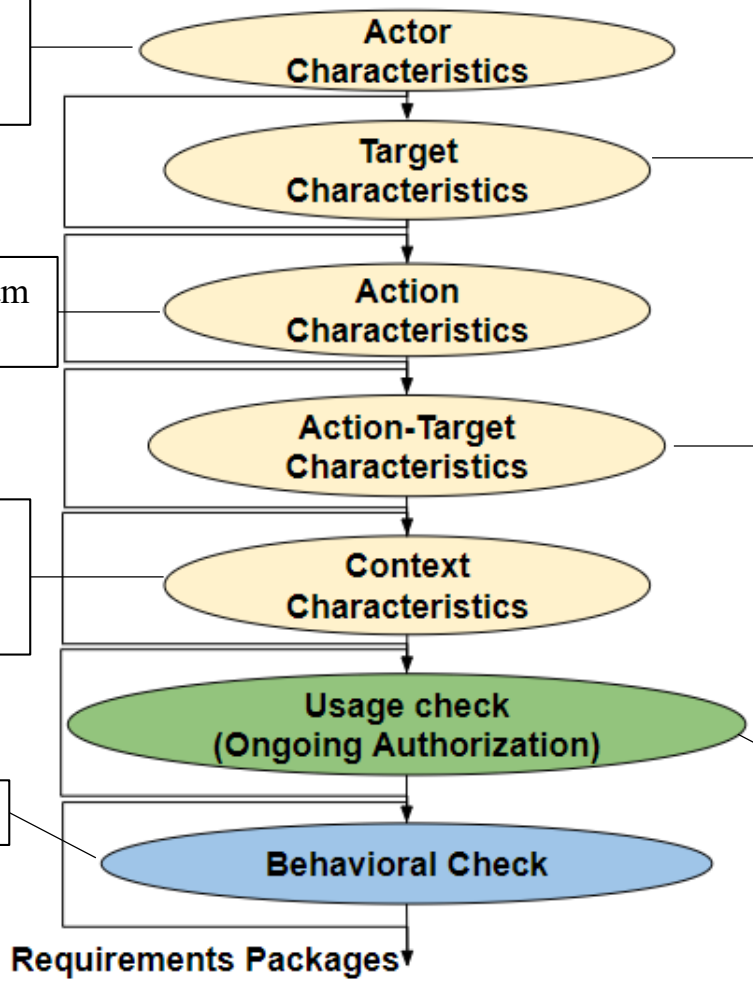
6. We propose our novel framework for ZT score-based authorization (ZT-SAF).

7. We highlight future research directions and propose a plan for designing, enforcing, and implementing the proposed ZT-SAF in smart connected IoT systems.

© Safwa Ameer

The Zero Trust Authorization Requirements Framework (ZT-ARF)

The system entity that initiates the access request (users, services, apps, devices)



Targets are the resources that need to be accessed in the request (users, devices, apps, info)

An executable image of a program (operations)

an approval to perform an action on a specific target (permissions, activities)

a. Environment characteristics.
b. System characteristics.
c. Threats and logs information.

- The continuity of an access Decision.
- The authorization system enforces the security policy:
  a. Before the access execution.
  b. During the execution,
  c. After the execution.

To capture any abnormal behavior.

© Safwa Ameer

Our Contribution

In This Paper:

1. We highlight the importance of considering ZT concepts when designing, enforcing, and implementing authorization models. For this purpose, we provide a structured mapping between the ZT tenets and the PEI models framework [2].

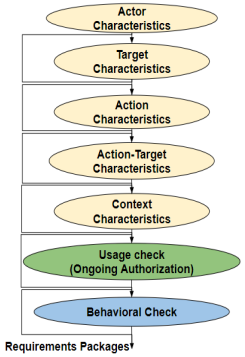
2. We propose the ZT authorization requirements framework (ZT-ARF), which provides a structured view of different authorization requirements to consider when designing a ZT authorization policy model.

3. We motivates the need to implement ZT principles when developing access control models for smart IoT systems.

4. We analyze access control requirements in IoT systems and accordingly specify which requirements components from our proposed ZT-ARF we need to include when designing an authorization model for integrated ZT IoT systems.

5. We propose our novel framework for ZT score-based authorization (ZT-SAF).

6. We highlight future research directions and propose a plan for designing, enforc enting the proposed ZT-SAF in smart connected IoT systems.



© Safwa Ameer

Why ZT in IoT?

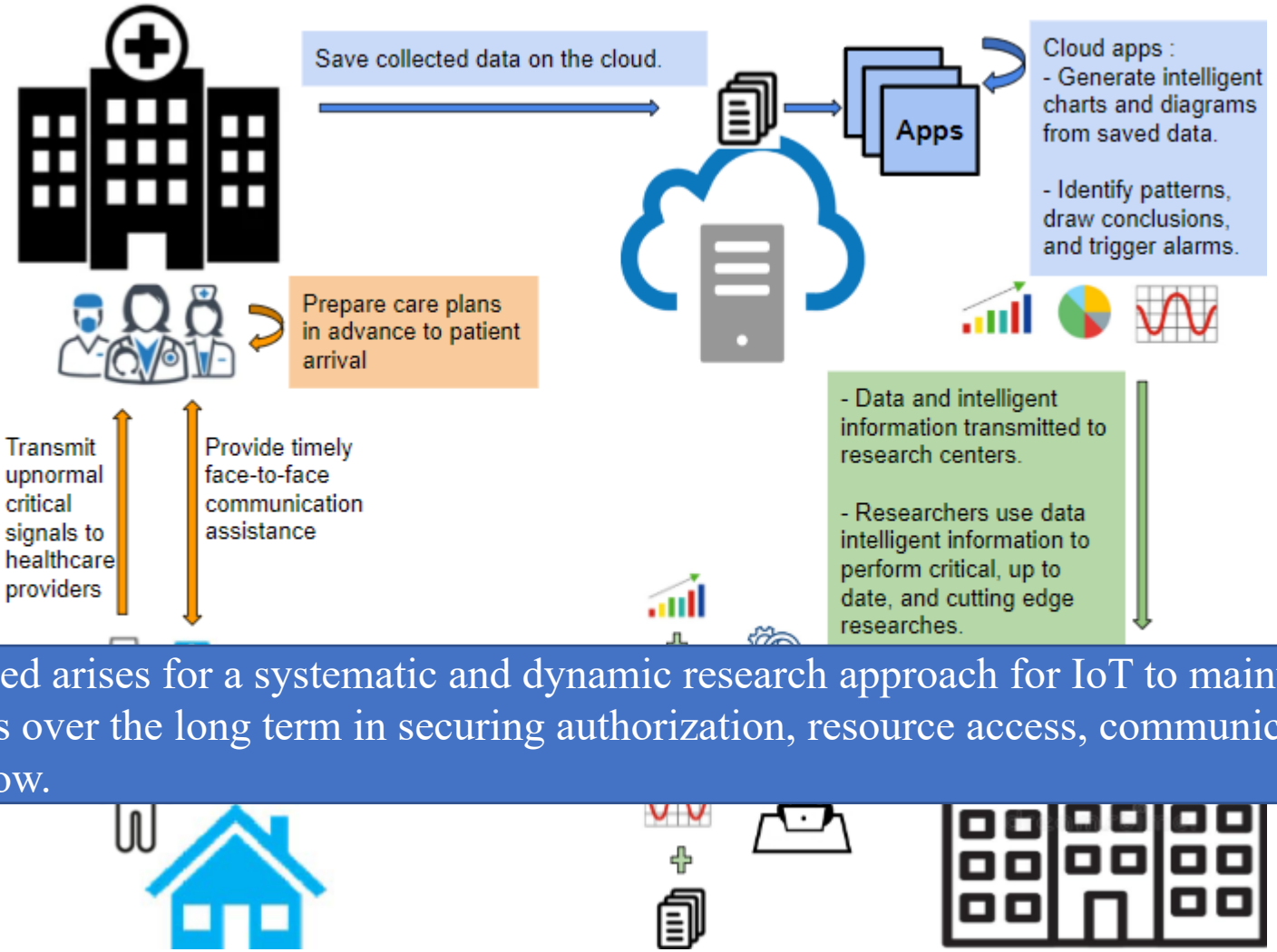
We believe that integrating ZT concepts is crucial when developing IoT systems for the following reasons:

1. ZT is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that do not fall within the enterprise's network boundaries, which is typical for IoT use cases.

2. On the other hand, IoT systems possess some characteristics that make them need to integrate ZT paradigms into their authentication and authorization designs.

© Safwa Ameer

Why ZT in IoT?



The need arises for a systematic and dynamic research approach for IoT to maintain its success over the long term in securing authorization, resource access, communication, and data flow.

© Safwa Ameer

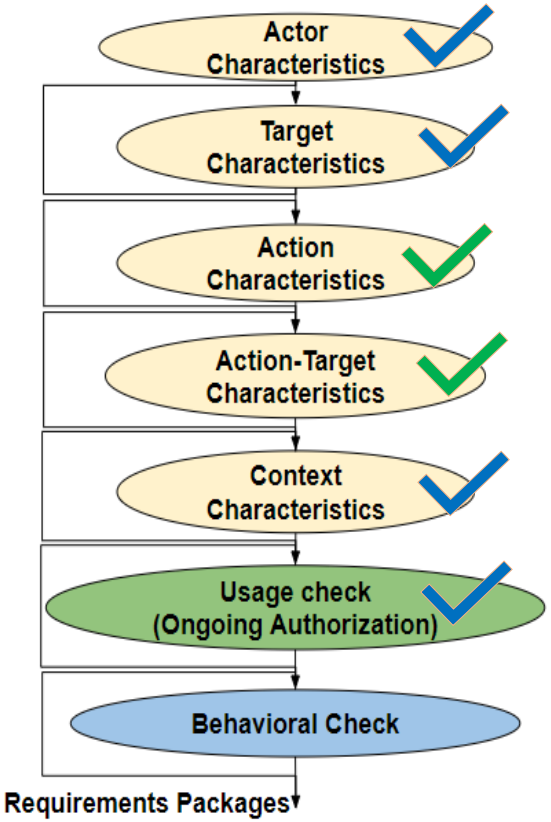
Toward Zero Trust Authorization In IoT Systems

- We analyzed IoT systems authorization requirements.

- To develop a ZT authorization system for an IoT application domain, we need to include the following components from the proposed ZT-ARF.
  1. Actor characteristics, target characteristics, context characteristics, and usage check requirements components to build a dynamic authorization model.
  2. Action and action-target characteristics components are critical in maintaining a fine-grained authorization model.

- While the behavioral check requirements component provides more dynamic authorization models capable of capturing deviations from normal behaviors, it requires sophisticated policy and enforcement models.

➢ Hence, we believe that including the behavioral check requirements components depends on the specific IoT application domain. Since it requires a trade-off between the sensitivity of the resources and data, the business needs on the one hand, and the cost and acceptable level of complexity on the other hand



© Safwa Ameer

Toward Zero Trust Authorization In IoT Systems

Criteria-Based Authorization Vs Score-Based Authorization:

The ZT paradigm differentiate between two types of authorization models based on how the input factors are evaluated to decide on access requests.

1. **Criteria-based authorization model:**

- Assumes certain qualifications (conditions, characteristics, etc) must be met before access to a resource (e.g., read/write) can be granted. Access is granted or action applied to a resource only if all the criteria are met.
- RBAC, UCON, ACON, ABAC.

2. **Score-based authorization model:** ✓

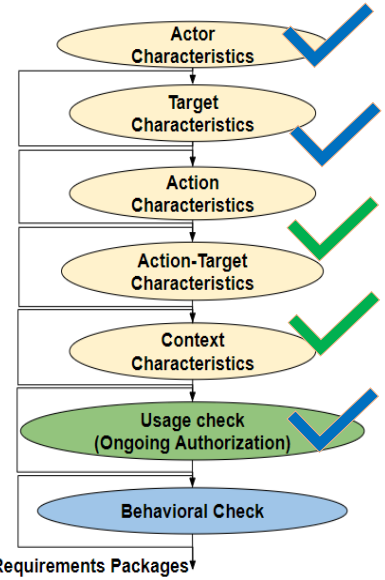
- Computes a confidence level (score) for the requested access. As long as the score exceeds the threshold value configured for the resource, access to the resource is granted or the action performed. Otherwise, the request is declined, or access privileges are reduced.
- We believe that score-based models are more suitable for IoT systems, for the following reasons:
  - They are more dynamic since the score provides a current confidence level for the requesting actor and adjusts to changing factors more quickly than static policies modified by human administrators.
  - Many of the inputs from the sensors are subjective and probabilistic rather than absolute.

➢ Therefore, it is imperative that authorization models considers the confidence level (score) of different access requests and that their policies can accommodate subjective information and uncertainty.

© Safwa Ameer

Toward Zero Trust Authorization In IoT Systems

Score –Based Authorization



ZT-ARF

➢ To develop a ZT IoT system, the need arises for a contextual aware access control model capable of :

1. Incorporating actor, targets, action, action-target, context characteristics, and the usage check components from the ZT-ARF.
2. Dynamically deciding on access requests based on calculated score (confidence level) rather than on static access control policies.

© Safwa Ameer

Our Contribution

In This Paper:

1. We highlight the importance of considering ZT concepts when designing, enforcing, and implementing authorization models. For this purpose, we provide a structured mapping between the ZT tenets and the PEI models framework [2].

2. We propose the ZT authorization requirements framework (ZT-ARF), which provides a structured view of different authorization requirements to consider when designing a ZT authorization policy model.

3. We motivates the need to implement ZT principles when developing access control models for smart IoT systems.

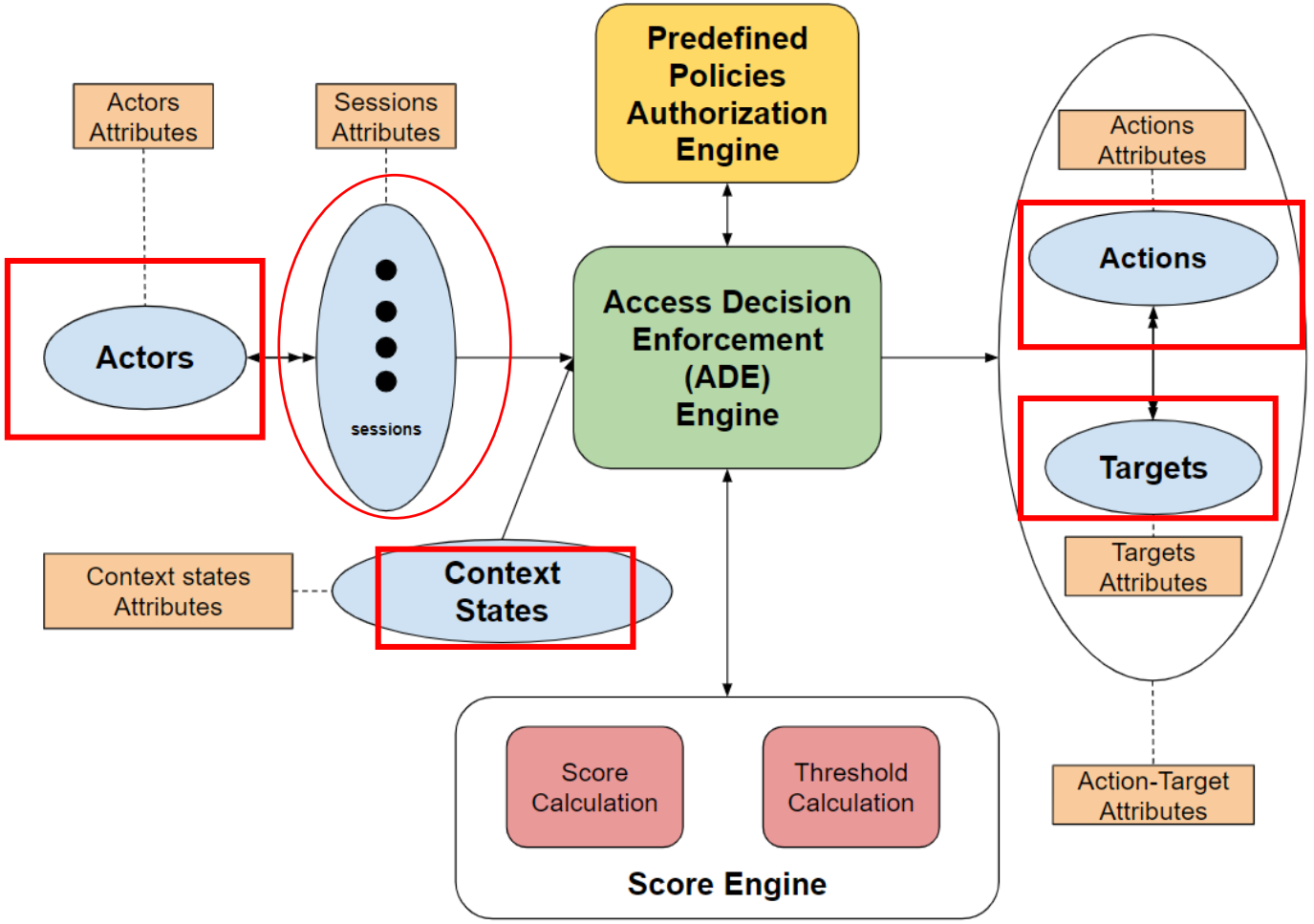
4. We analyze access control requirements in IoT systems and accordingly specify which requirements components from our proposed ZT-ARF we need to include when designing an authorization model for integrated ZT IoT systems.

5. We propose our novel framework for ZT score-based authorization (ZT-SAF).

6. We highlight future research directions and propose a plan for designing, enforcing, and implementing the proposed ZT-SAF in smart connected IoT systems.

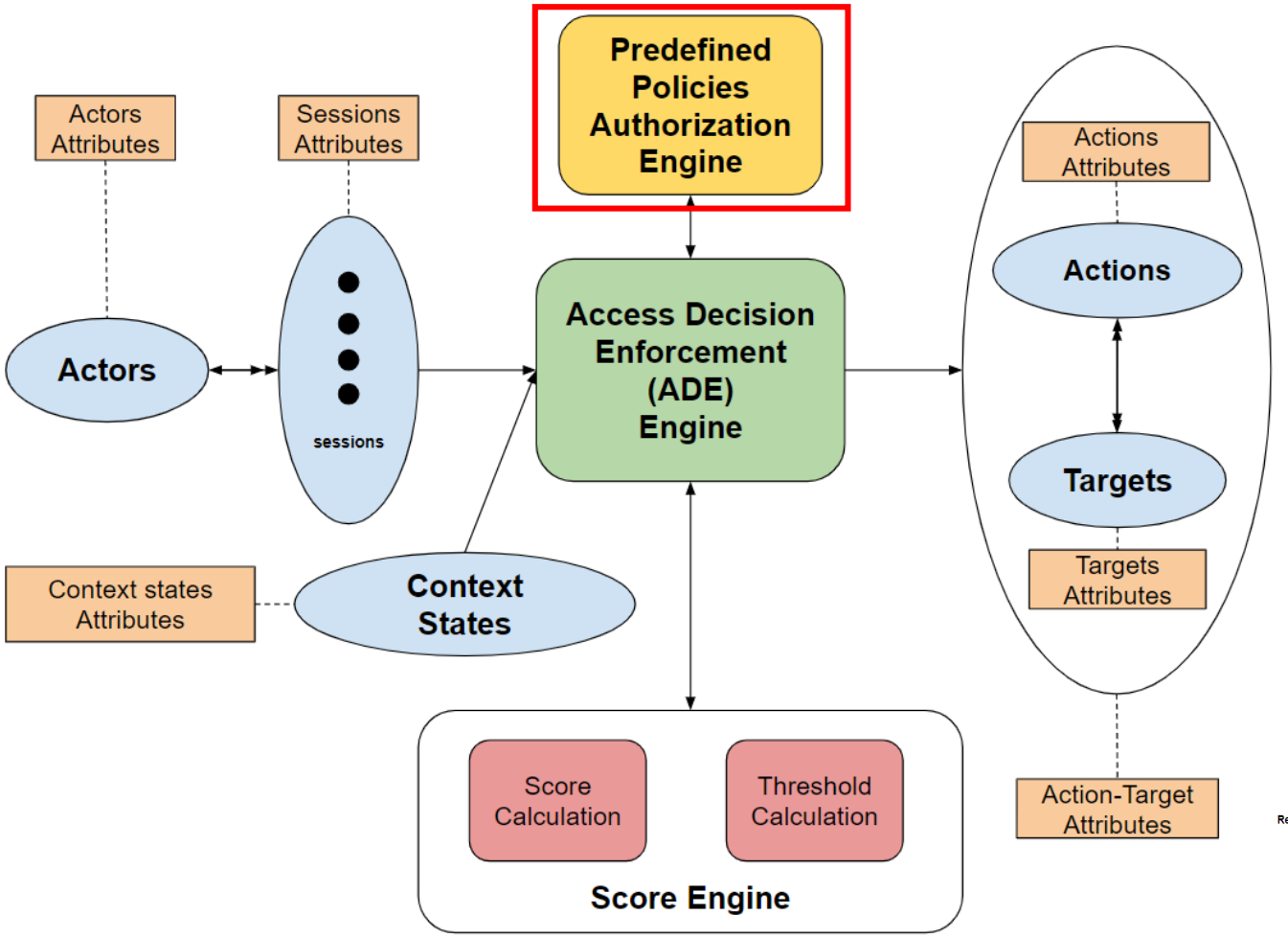
© Safwa Ameer

The Zero Trust Score-based authorization framework (ZT-SAF)



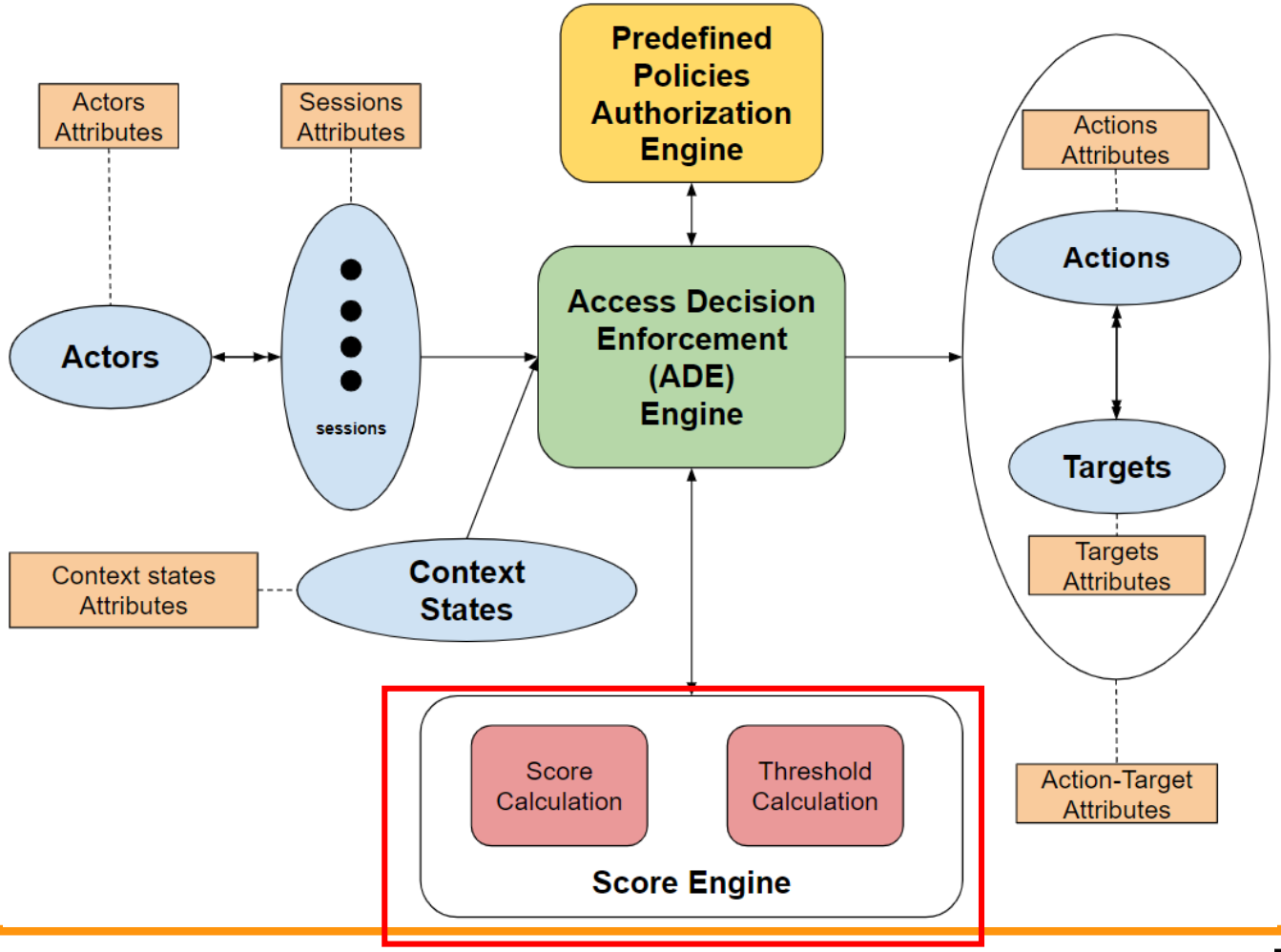
© Safwa Ameer

The Zero Trust Score-based authorization framework (ZT-SAF)



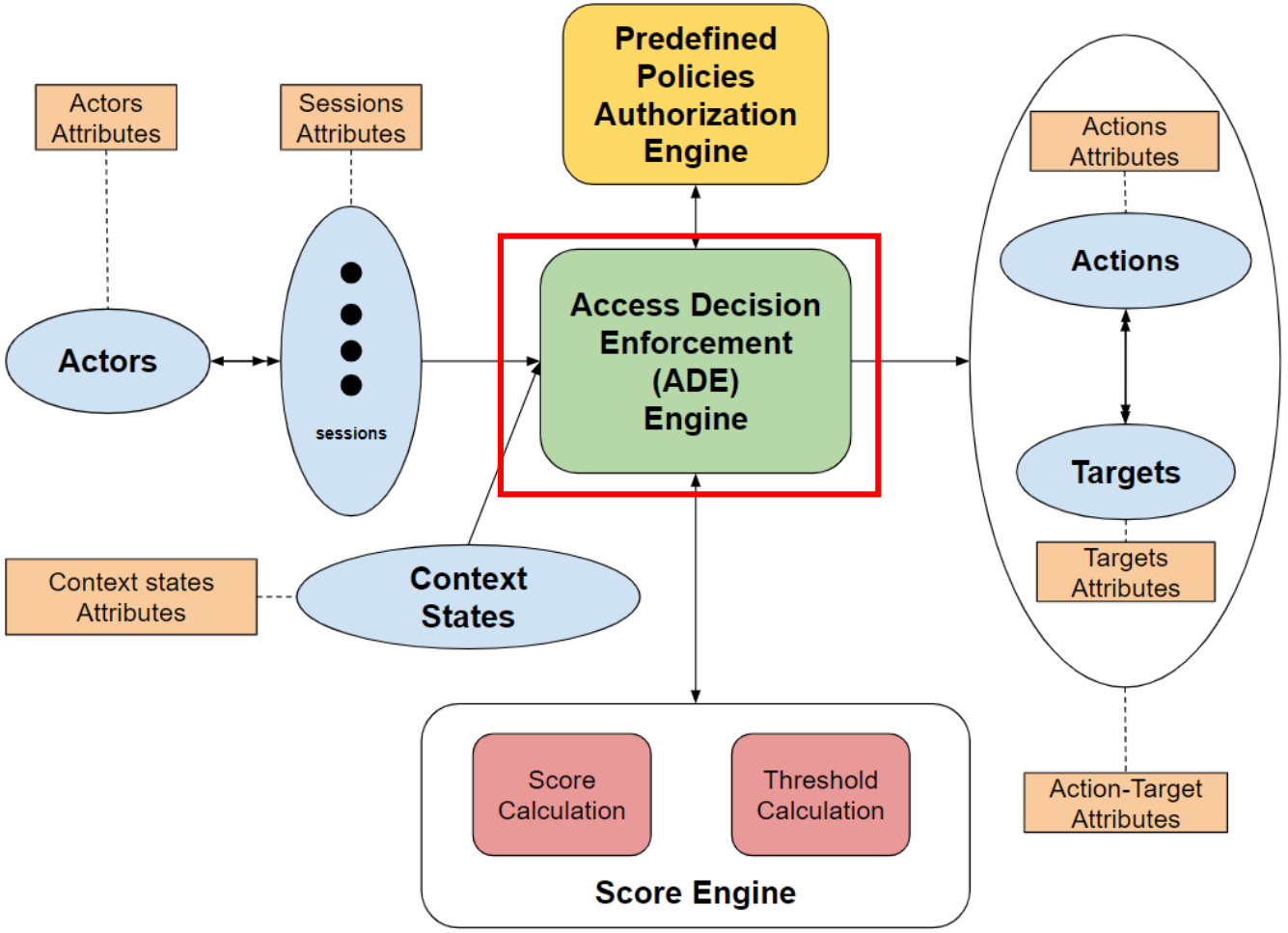
© Safwa Ameer

The Zero Trust Score-based authorization framework (ZT-SAF)



© Safwa Ameer

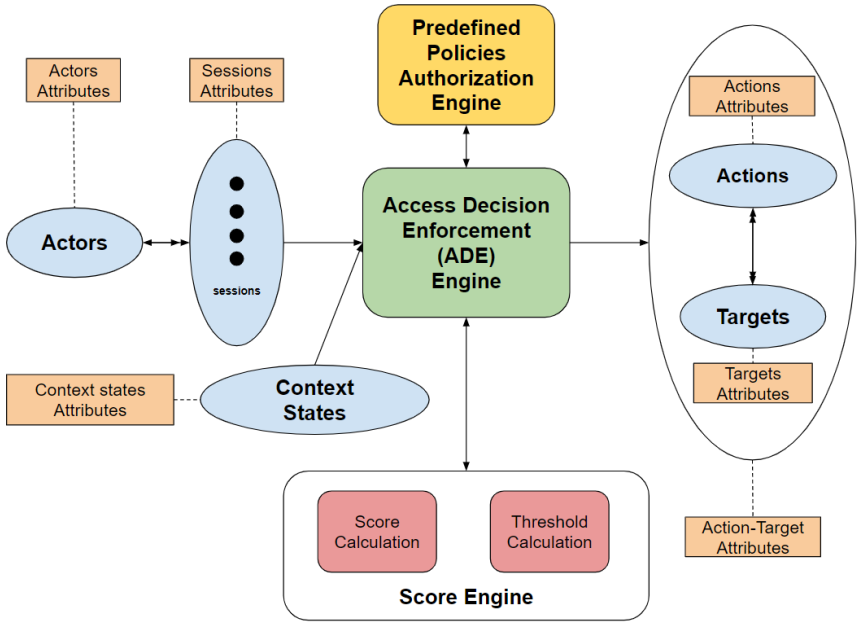
The Zero Trust Score-based authorization framework (ZT-SAF)



© Safwa Ameer

Future Research Agenda

- Authorization Operational Policy Models and Extensions.
- Framework Algorithms.
- Administrative Policy Models.
- Policy Language.
- Enforcement Architectures.
- Implementation Models.
- Behaviorally Aware Models.
- AI and Data Driven Deployment.
- Applications domains in IoT.



ZT-SAF

© Safwa Ameer


Q&A

Thank You

References

[1] R. Sandhu, et al. 2006. Secure information sharing enabled by trusted computing and PEI models. In ASIACCS '06

[2] S. W. Rose, et al. 2020. Zero trust architecture. (2020).

© Safwa Ameer