CHESS

UNIVERSITY OF TARTU
Institute of Computer Science

DECEPTWIN: Proactive Security Approach for IoV by Leveraging Deception-based Digital Twins and Blockchain

Mubashar Iqbal [1], Sabah Suhail [2], Raimundas Matulevičius [1]

[1] *University of Tartu, Estonia*
[2] Queen's University Belfast, UK

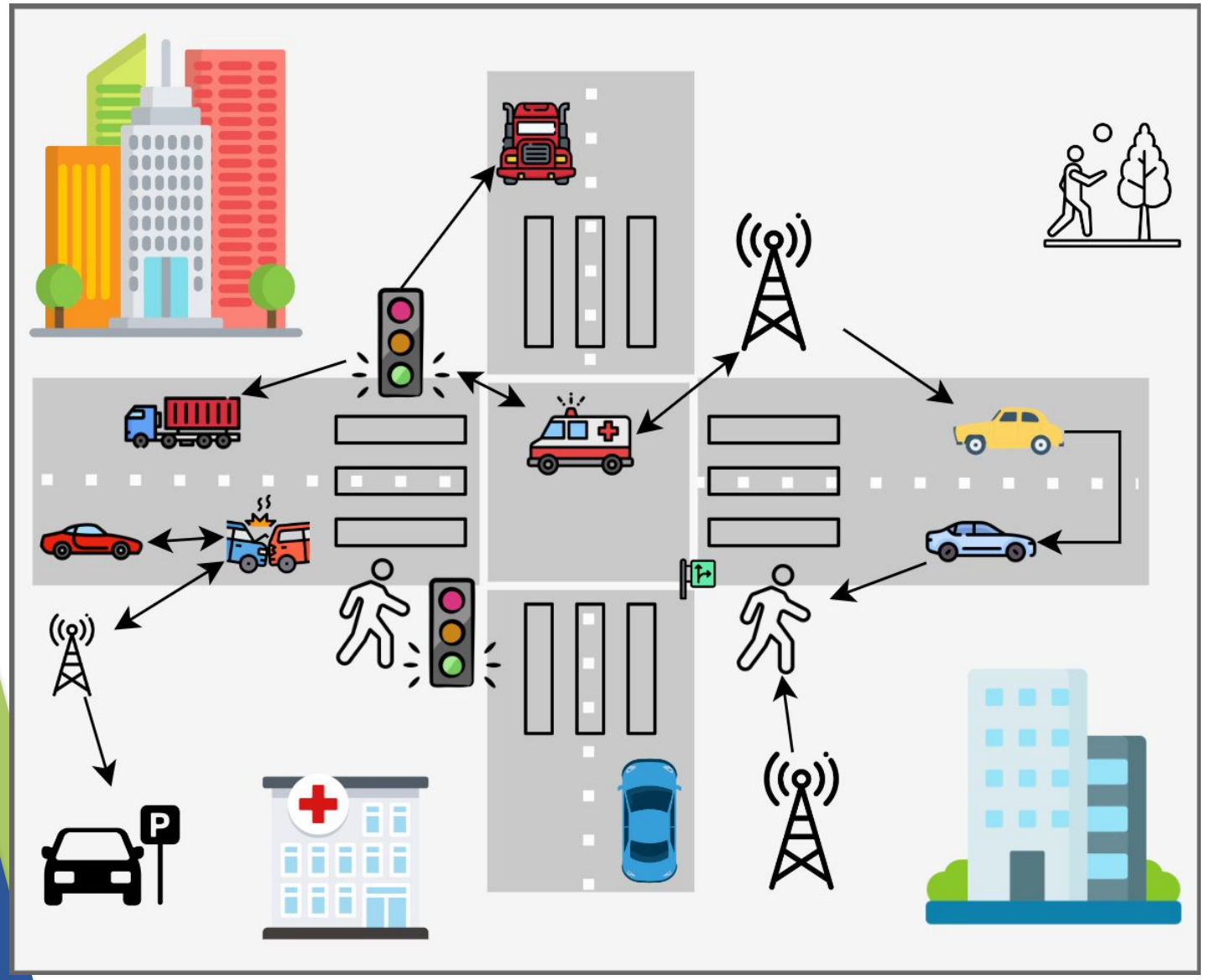
ARES

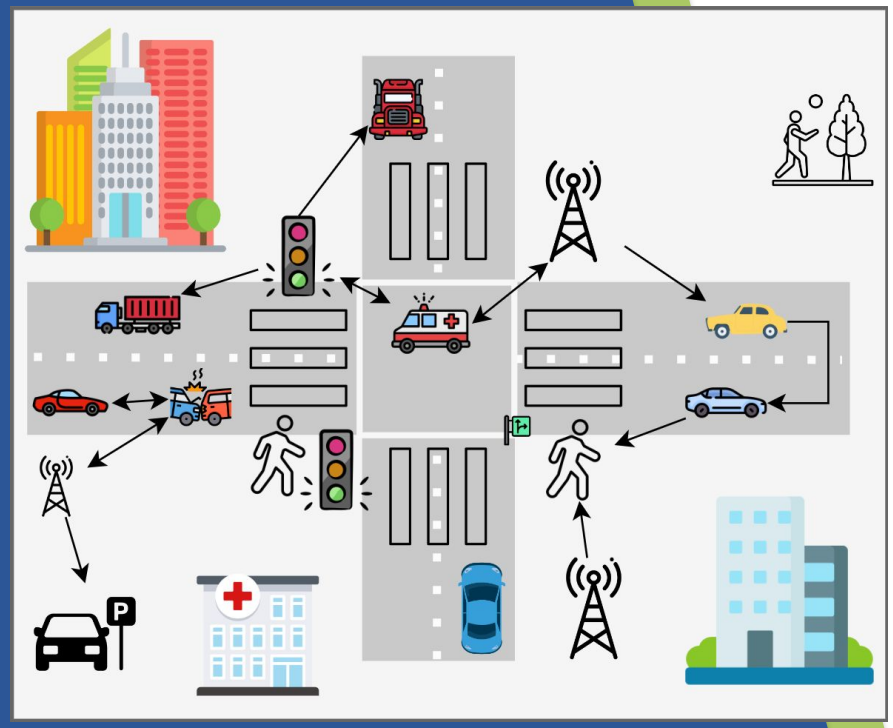
SP2I

Internet of Vehicles (IoV)

IoV enables real-time data sharing, traffic management, autonomous driving capabilities, and transportation services.

- Internet of Things (IoT)
- Sensors
- Roadside infrastructure





Internet of Vehicles (IoV)

Emerging security attacks:

- Jeep Cherokee remote hijacking attacks
- Rav4 CAN injection attack

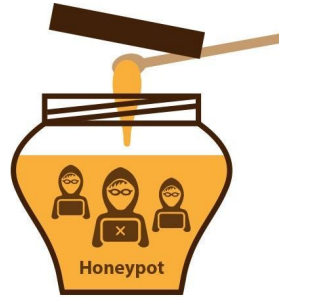
image src: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Proactive security solutions for IoV

e.g., deception solutions:

- **Honeypots**
- **Honeynets**
- **Decoys**

- **Intentionally** lure attackers
- **Compromising scenarios**
- Gather **actionable intelligence**

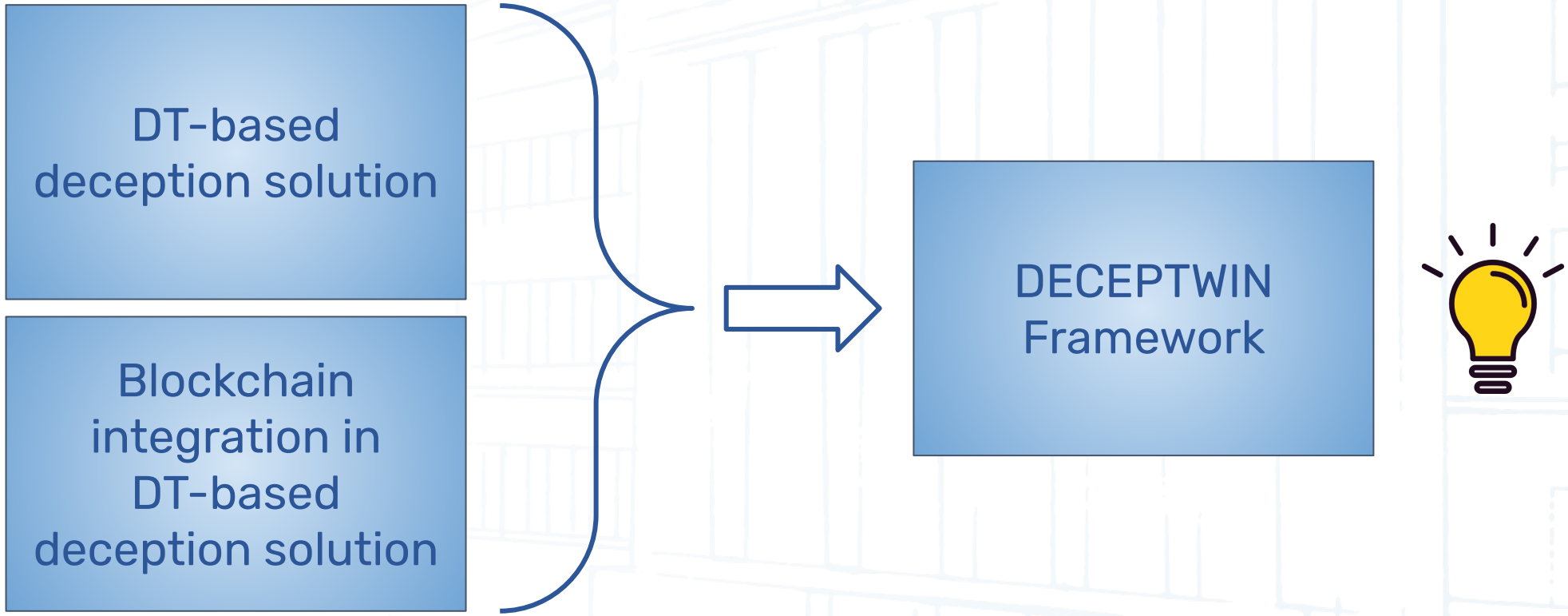


What are the issues/problems?

- Deception solutions challenges:
  - Limited **interaction** capabilities
  - Lacking **realism** to closely mimic real systems
  - **Complex** and **lack scalability**
  - Challenging to **analyze** large volumes of generated **data** in **real-time**
- **Insecure communication**, **data integrity**, and **traceability** challenges

Contributions

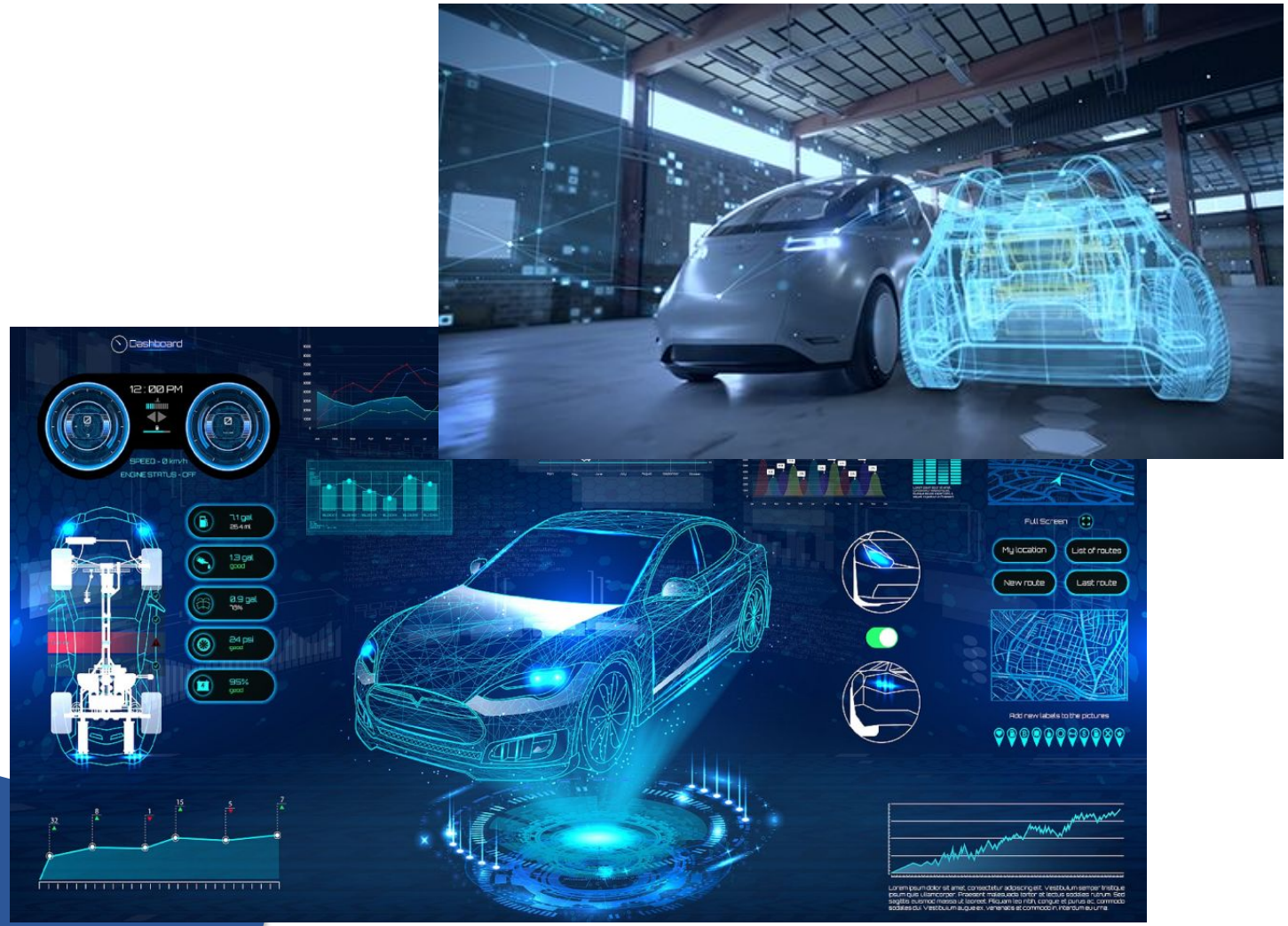
*Proactive security approach for IoV by leveraging **DECEP**tion-based digi**T**al t**W**ins and blockcha**IN** (DECEPTWIN).*



DTs are **virtual (digital)** representations.

DTs support **continuous** and **accurate reflection** of the physical entity for

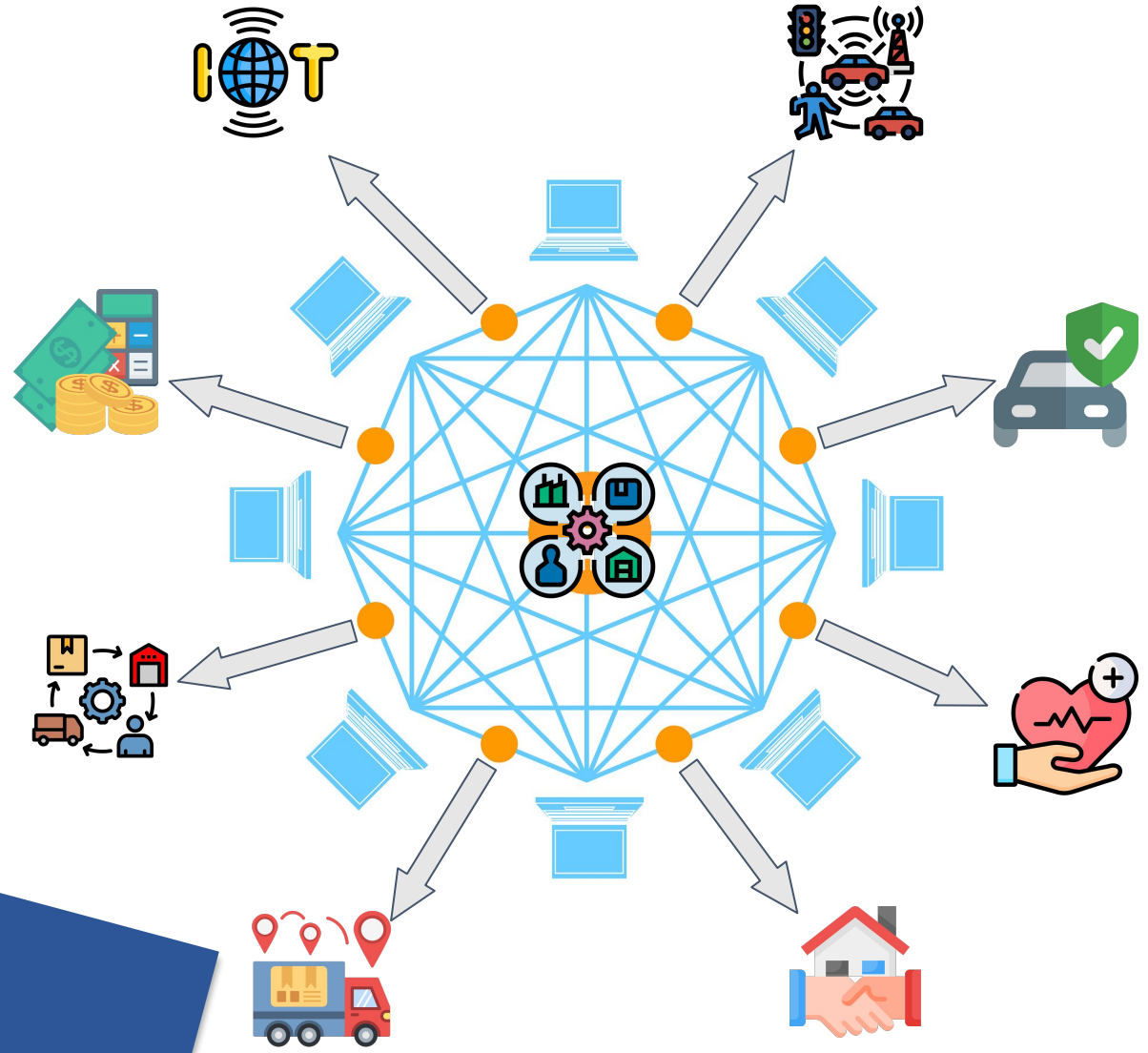
real-time monitoring, analysis, and **simulation**.



Digital Twin (DT)

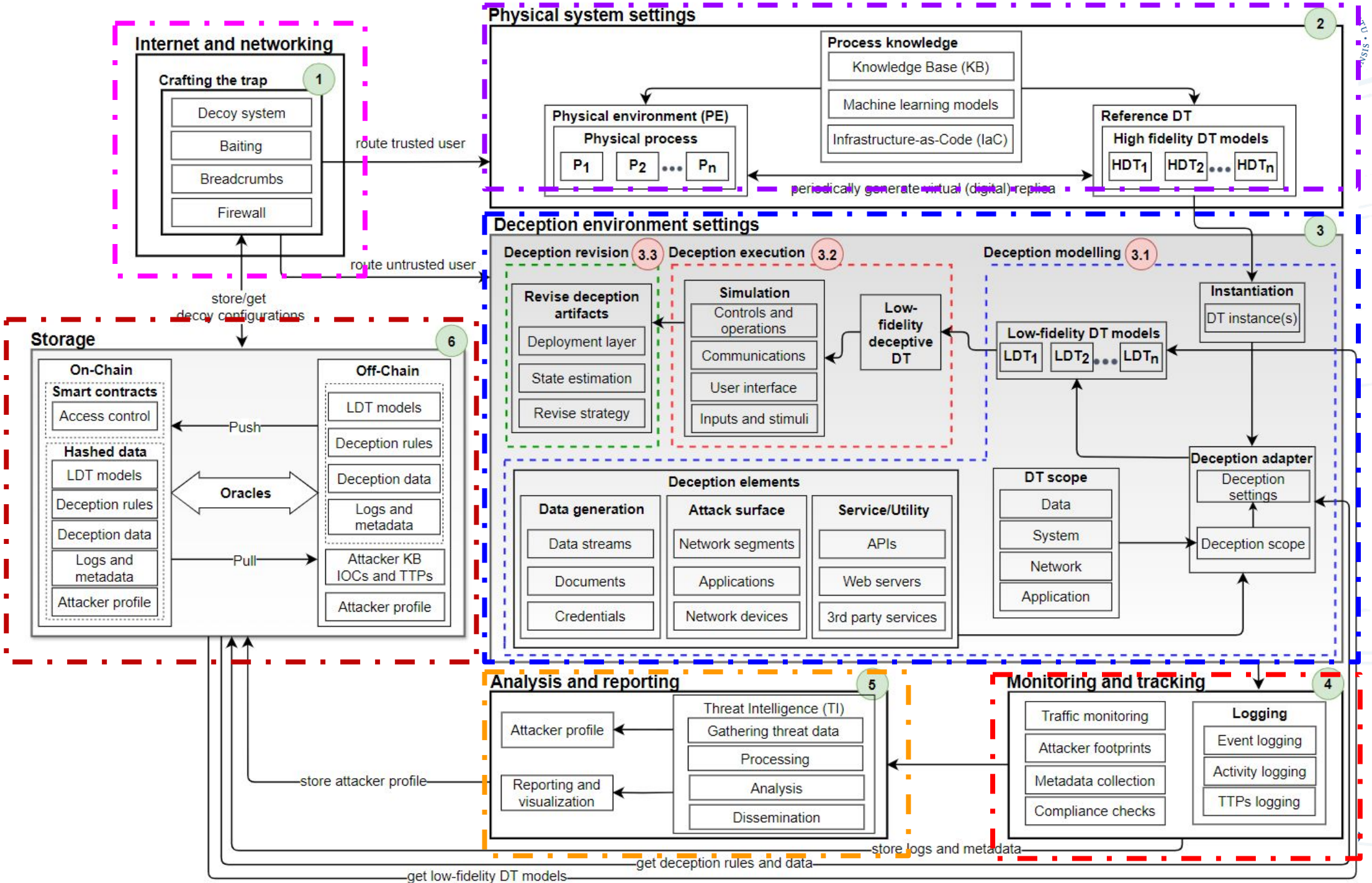
image src: https://www.linkedin.com/pulse/unleashing-power-virtual-replicas-digital-twins-electric-ankita-saraf/

Decentralized and **distributed** ledger technology that **securely** records and **verifies** transactions across a **network of computers**.

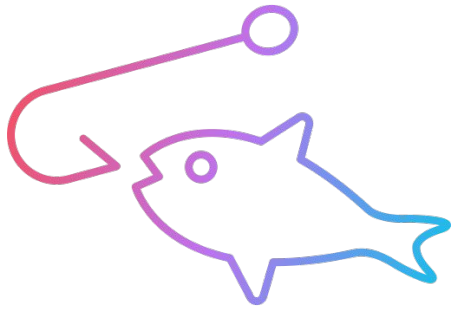


Blockchain

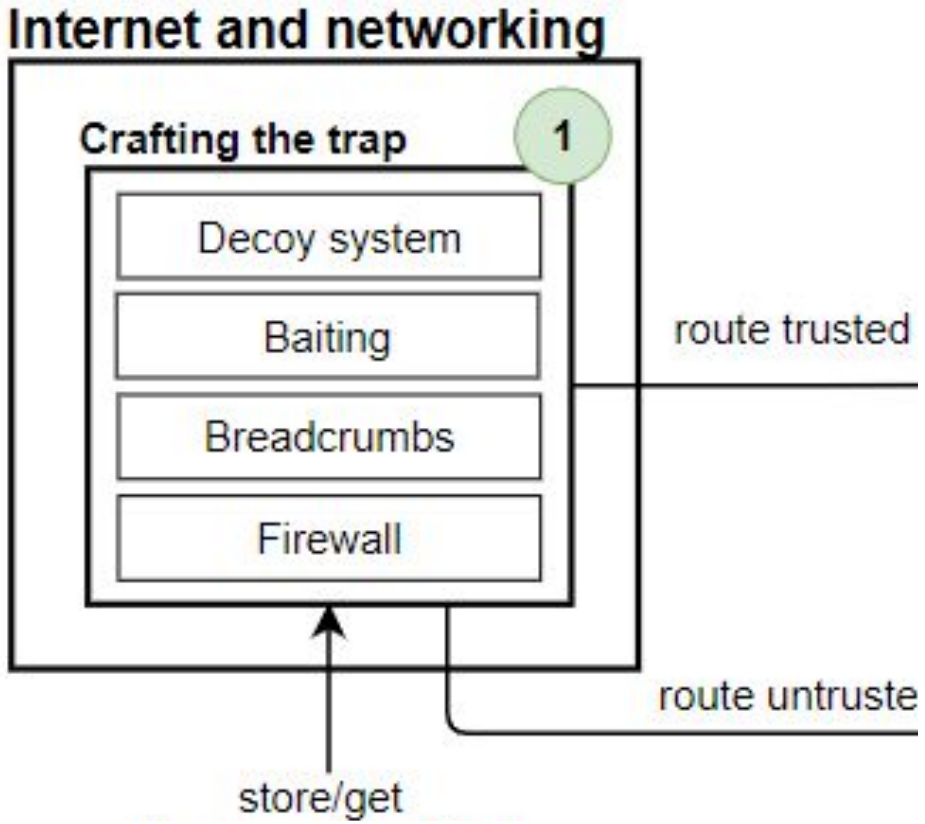
DECEPTWIN Framework



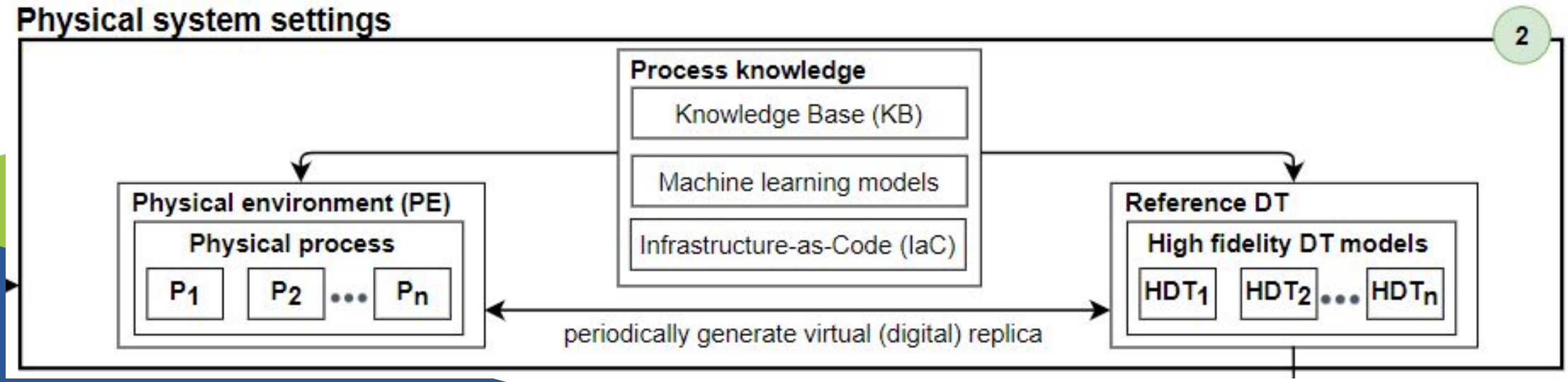
- Intentional traps
  - Decoys, baiting, breadcrumbs
- Lure and divert attackers



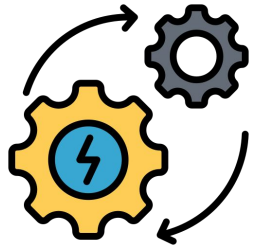
1. Crafting the trap

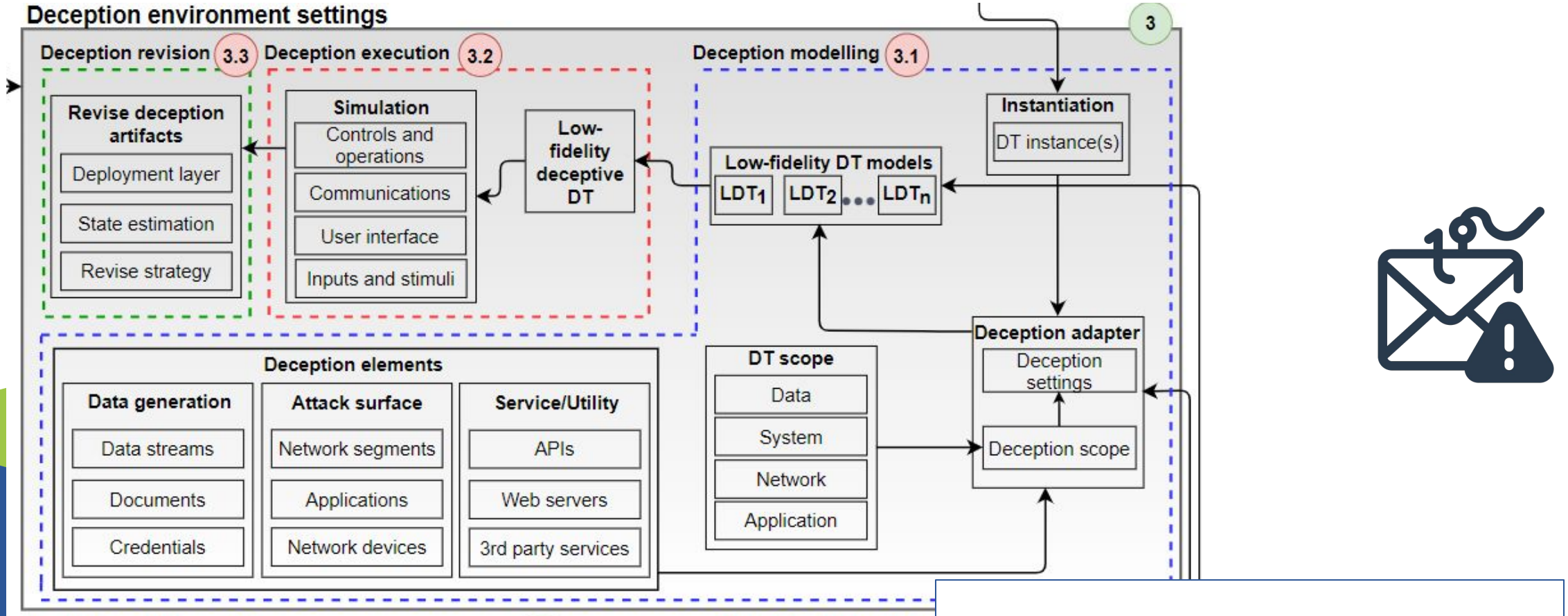


- Identify physical process
- High fidelity DTs



2. Physical system settings



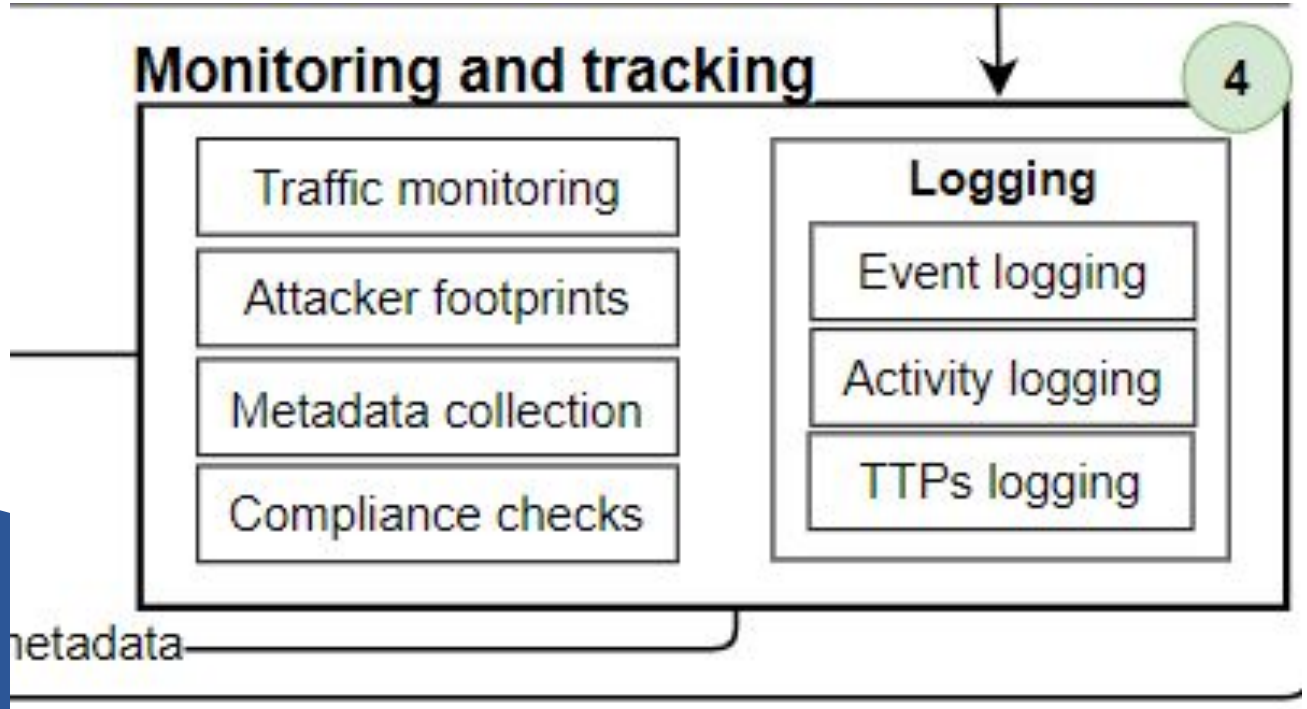


3. Deception environment settings

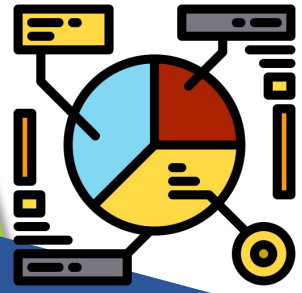
- Deception modelling
- Deception execution
- Deception revision

- Monitor attacker's TTPs
- Detect and log anomalous patterns

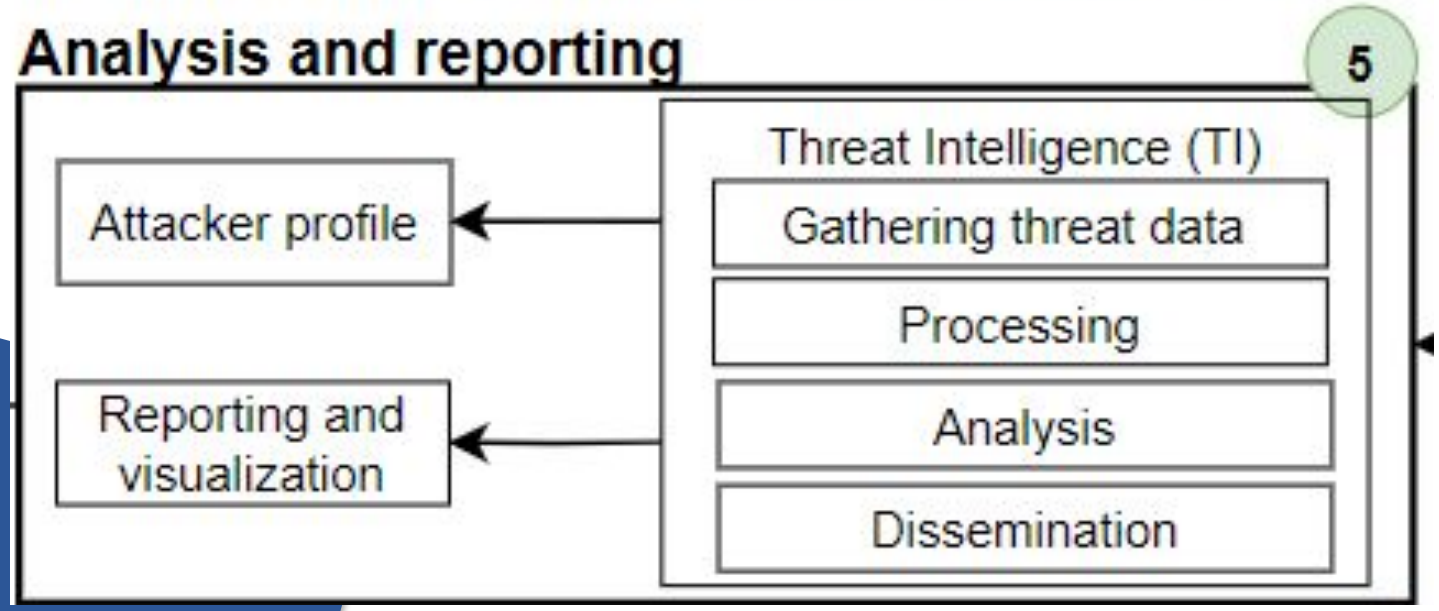
4. Monitoring and tracking



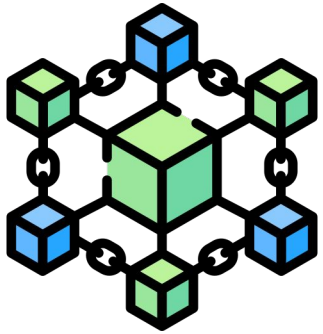
- Conduct Threat Intelligence (TI)
  - Build attacker profile
- Facilitating the interpretation of actionable intelligence



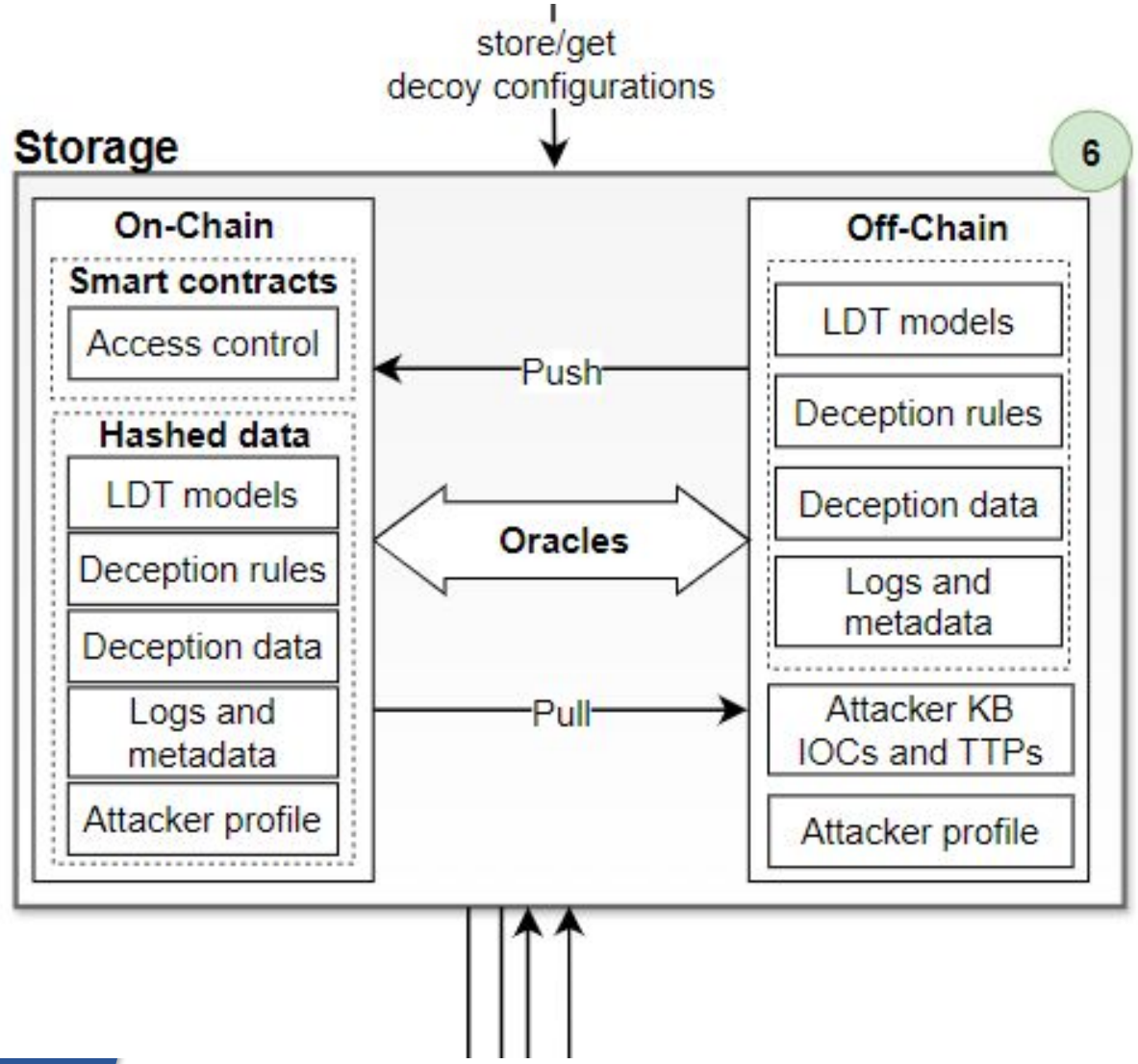
5. Analysis and reporting



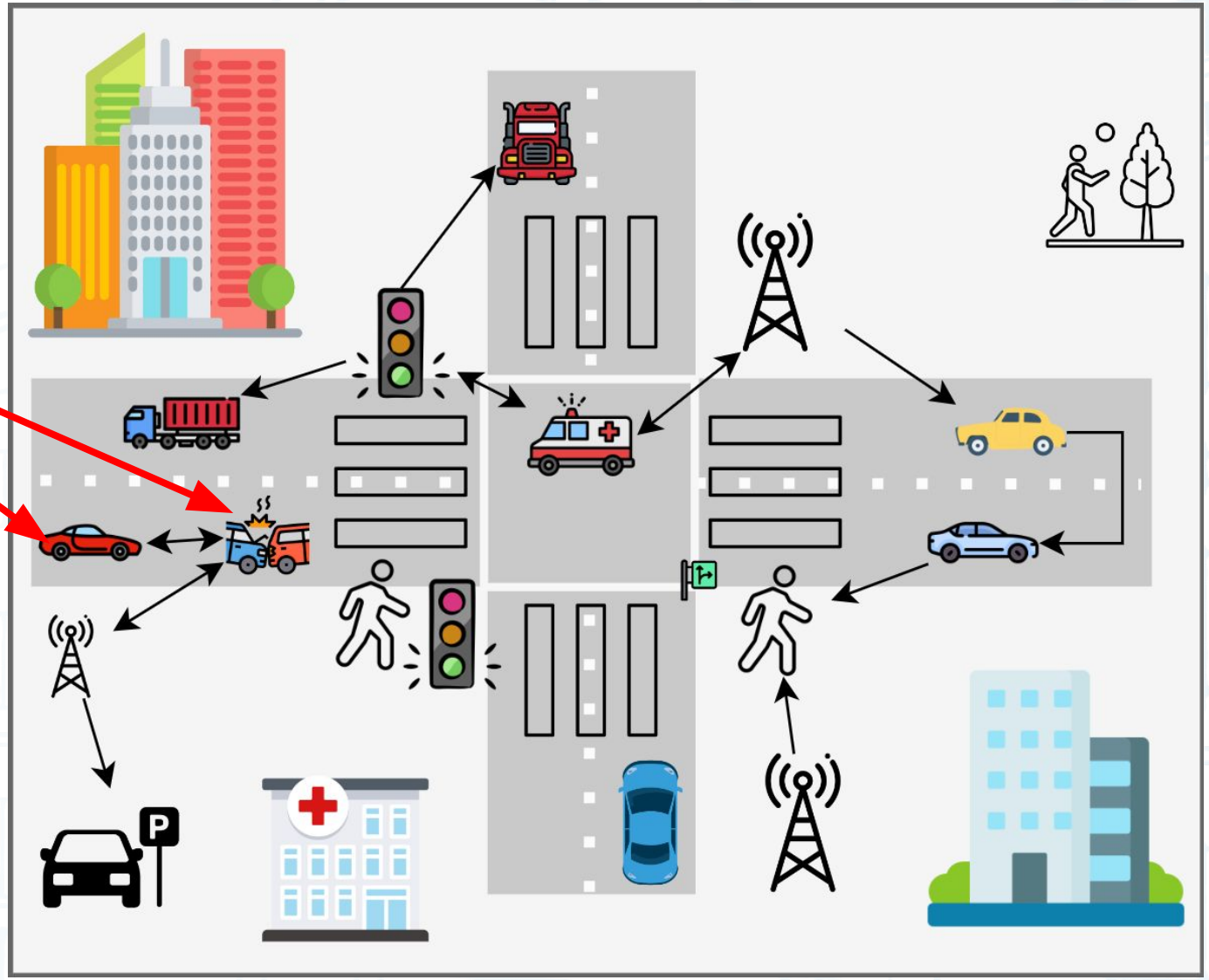
- On-chain storage
- Off-chain storage
- Oracles support



6. Blockchain integration

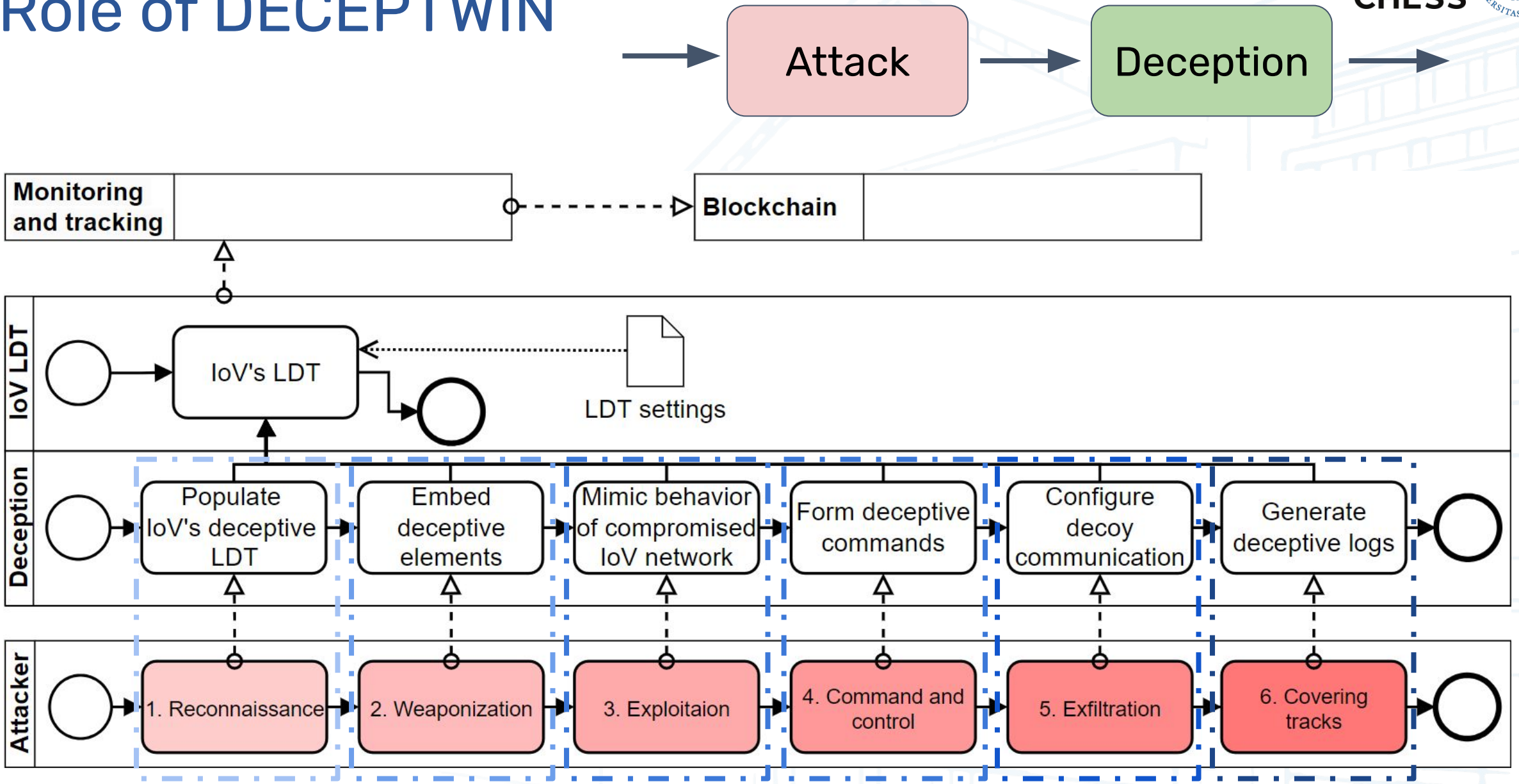


Role of DECEPTWIN



Remote access attack scenario within IoV context

Role of DECEPTWIN



Future Work

Real-world implementation of DECEPTWIN to show its practicality as a deception-based security solution.

image src: https://adl.cs.ut.ee/lab/vehicle

Thank You!

Mubashar Iqbal, PhD
Lecturer of Information Security

mubashar.iqbal@ut.ee

https://infosec.cs.ut.ee

DECEPTWIN Framework