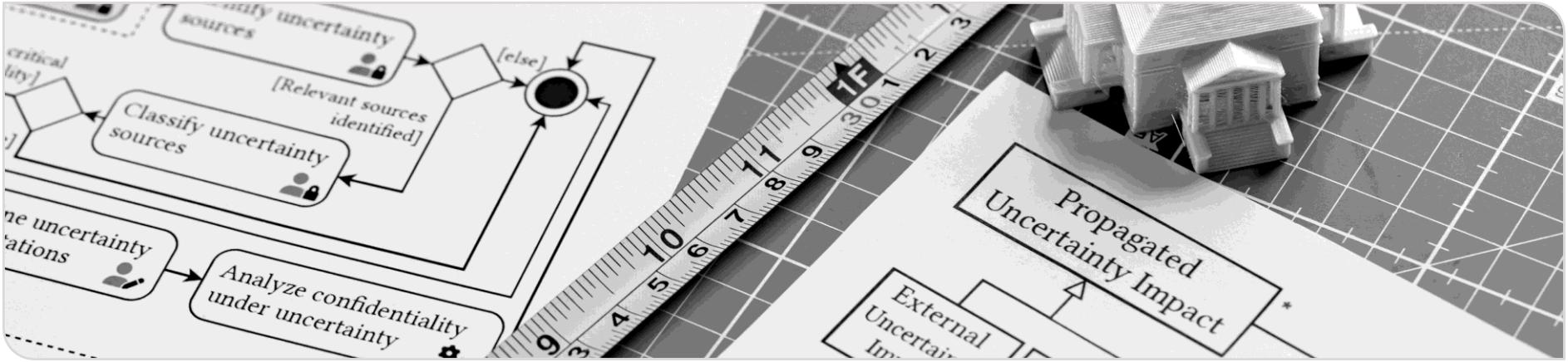
Architecture-Based and Uncertainty-Aware Confidentiality Analysis – The (very) short version

Dr.-Ing. Sebastian Hahner

CyberSec Seminar, April 8th, 2025

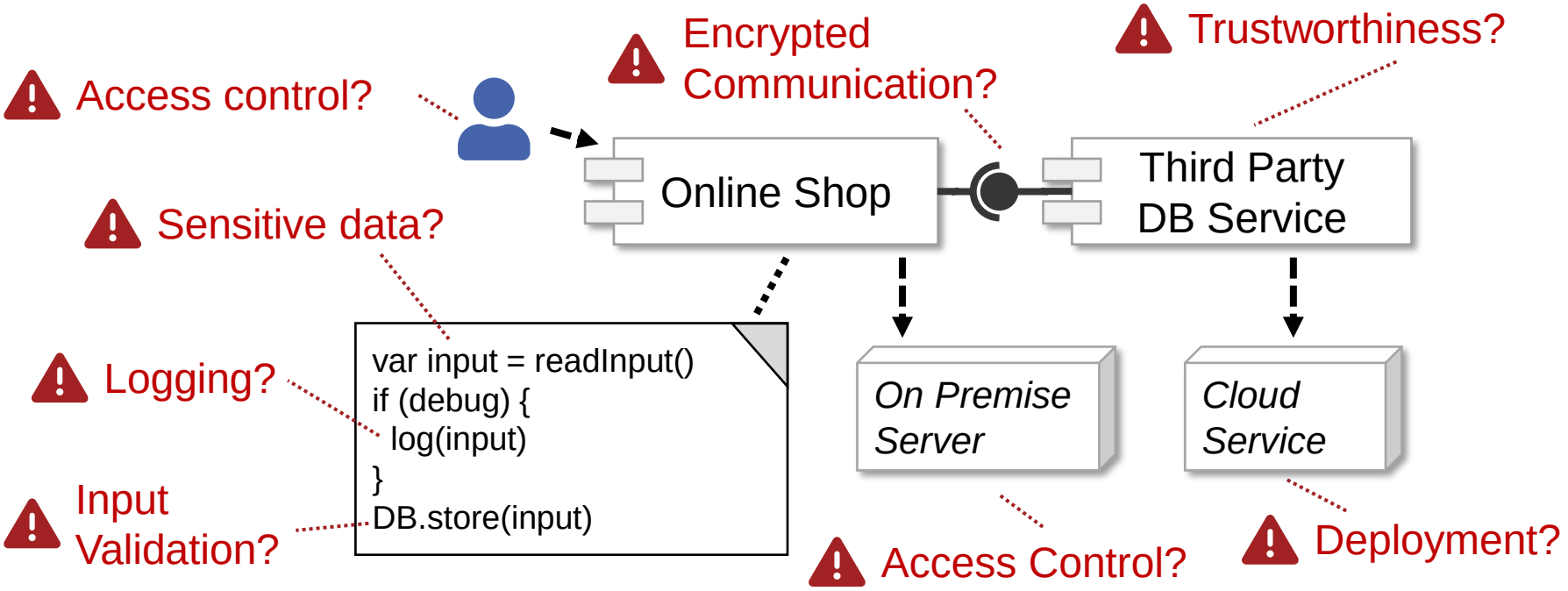


Architecture?

Architecture-Based and Uncertainty-Aware Confidentiality Analysis

Architecture and Confidentiality Violations?

Architecture-Based** and Uncertainty-Aware **Confidentiality Analysis



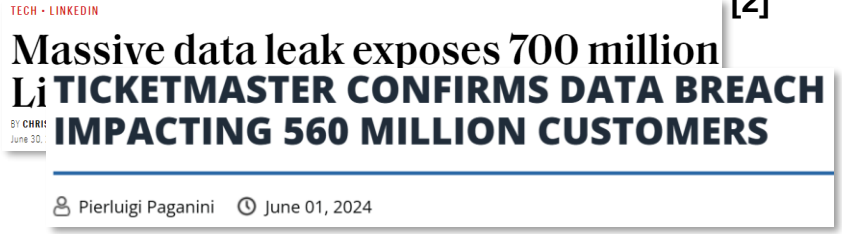
Data Breaches, Cyber Attacks and Confidentiality


TECHNOLOGY | CYBERSECURITY

What's Behind the Increase in Data Breaches?

One reason: Ransomware gangs are on the rise, allowing even criminals with minimal computer knowledge to get into the game

[1]


TECH · LINKEDIN

Massive data leak exposes 700 million Li

TICKETMASTER CONFIRMS DATA BREACH IMPACTING 560 MILLION CUSTOMERS

Pierluigi Paganini June 01, 2024

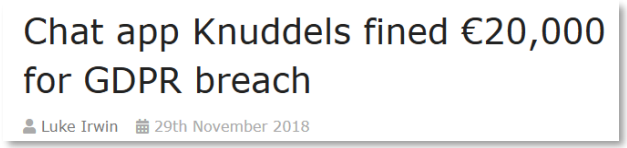
[2]

[3]


Russia accused of EU and Nato cyber-attacks

9 September 2024

[4]


Chat app Knuddels fined €20,000 for GDPR breach

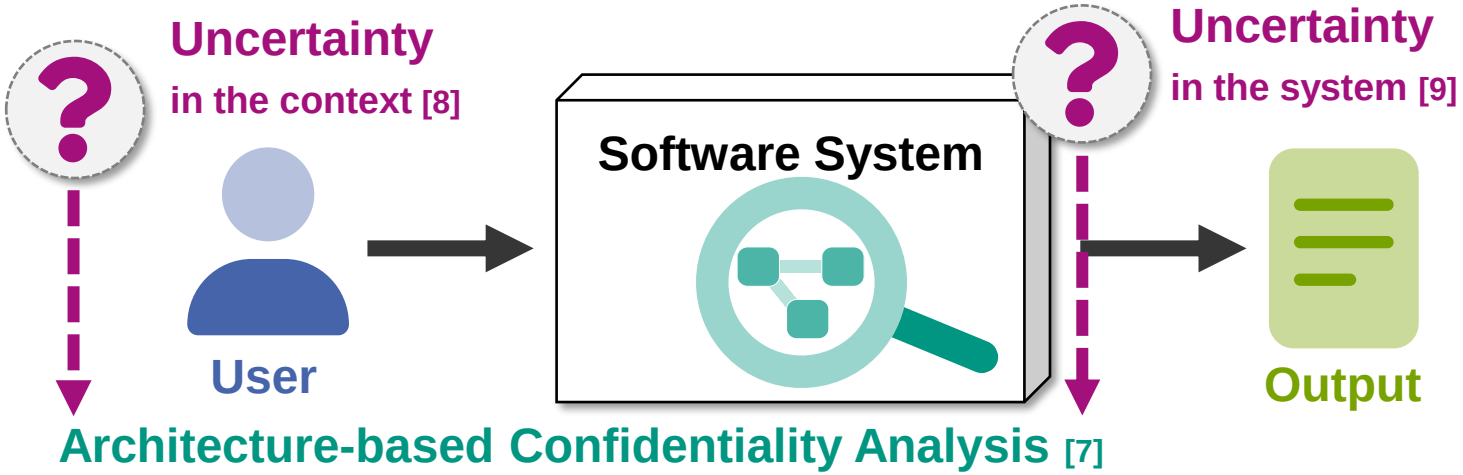
Luke Irwin 29th November 2018

[5]

Confidentiality: "property that information is not made available or disclosed to unauthorized individuals, entities, or processes" [6]

[1] Wall Street Journal, https://www.wsj.com/tech/cybersecurity/why-are-cybersecurity-data-breaches-still-rising-2f08866c, 2024 (last checked: 03.12.24)
[2] FORTUNE, https://fortune.com/2021/06/30/linkedin-data-theft-700-million-users-personal-information-cybersecurity, 2021(last checked: 03.12.24)
[3] Security Affairs, https://securityaffairs.com/163999/data-breach/ticketmaster-confirms-data-breach.html, 2024 (last checked: 03.12.24)
[4] BBC, https://www.bbc.com/news/articles/c984zenjkz5o, 2024 (last checked: 03.12.24)
[5] IT Governance, https://www.itgovernance.eu/blog/en/chat-app-knuddels-fined-e20000-for-gdpr-breach, 2018 (last checked: 03.12.24)
[6] ISO/IEC 27000:2018(E) Information technology – Security techniques – Information security management systems – Overview and vocabulary, 2018.

Software Architecture Analysis under Uncertainty



Uncertainty: “deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood” **[6]**

[7] S. Seifermann, et al., “Detecting violations of access control and information flow policies in data flow diagrams”, JSS, vol. 184, Elsevier, 2022.
[8] D. Garlan, “Software engineering in an uncertain world”, FoSER , ACM, 2010.
[9] S. McConnell, “Software project survival guide”, Microsoft Press, 1998.
[6] ISO/IEC 27000:2018(E) Information technology – Security techniques – Information security management systems – Overview and vocabulary, 2018.

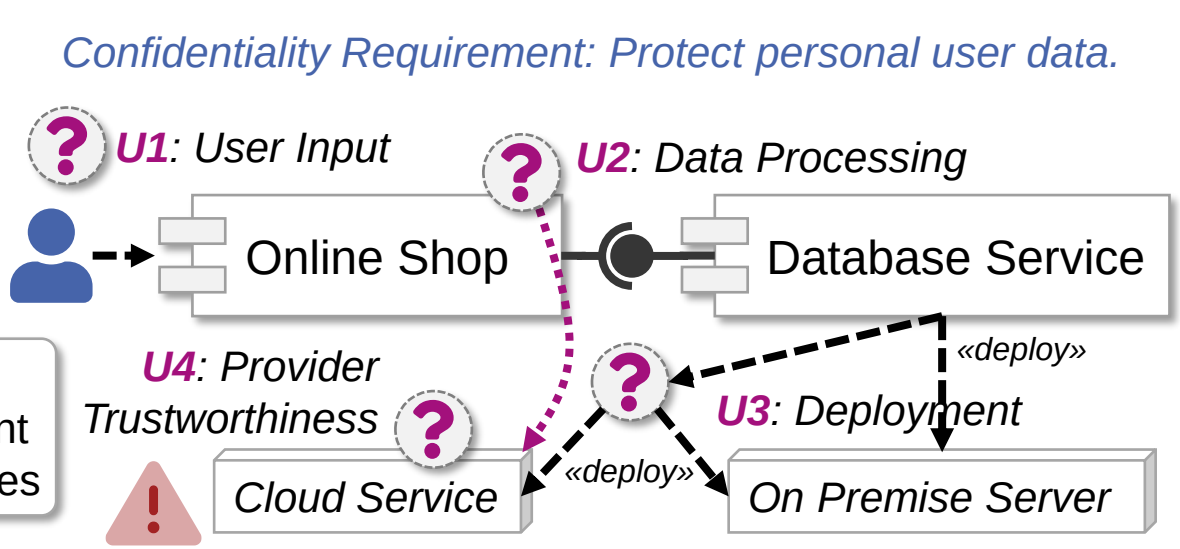
Challenges of Confidentiality and Uncertainty

Challenge 1
Understanding, describing, and classifying uncertainty

Challenge 2
Identifying relevant uncertainty sources

Challenge 3
Predicting the impact of uncertainty

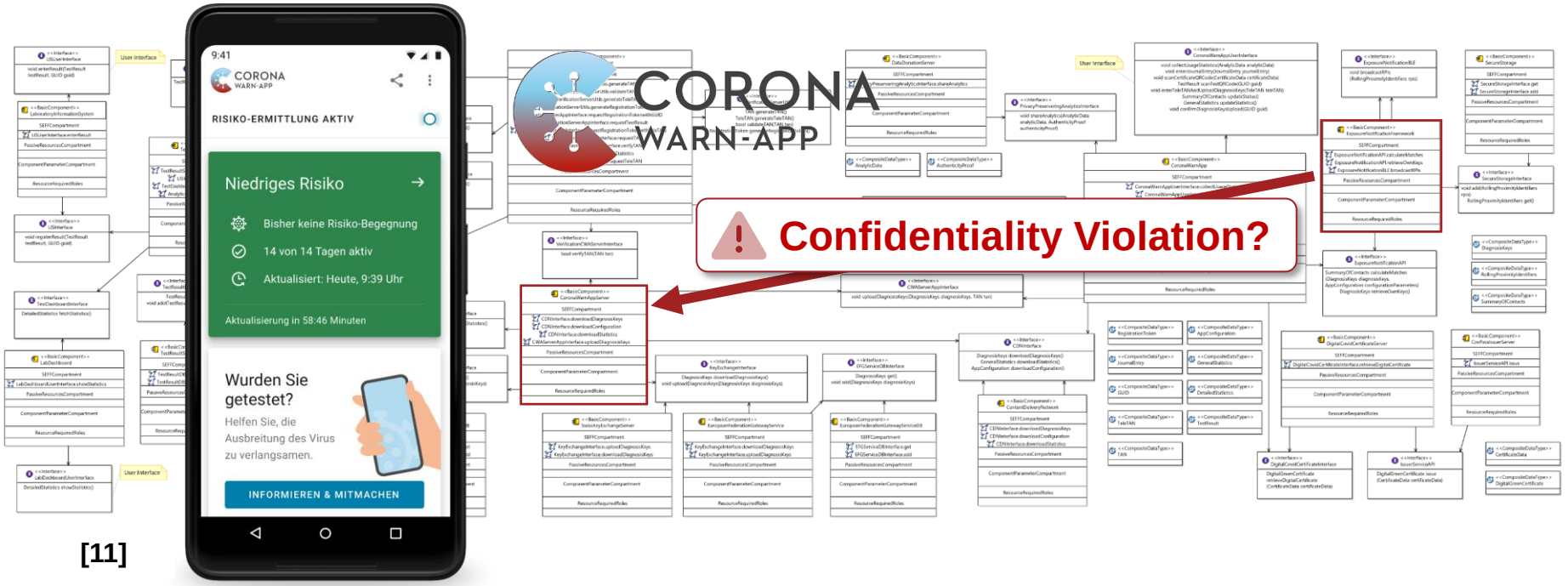
Challenge 4
Identifying confidentiality violations due to uncertainty



Gap: lack of means to identify, describe, and analyze uncertainty regarding confidentiality at design time

[10] S. M. Hezavehi, et al., "Uncertainty in Self-adaptive Systems: A Research Community Perspective," ACM TAAS., vol. 15, no. 4, 2021.

Enabling Architectural Confidentiality Analysis



[11]

[11] Robert Koch Institute, Open-source Corona Warn App, documentation available online: https://github.com/corona-warn-app
[12] S. Hahner, et al., “Architecture-Based Uncertainty Impact Analysis to Ensure Confidentiality”, SEAMS, IEEE/ACM, 2023.

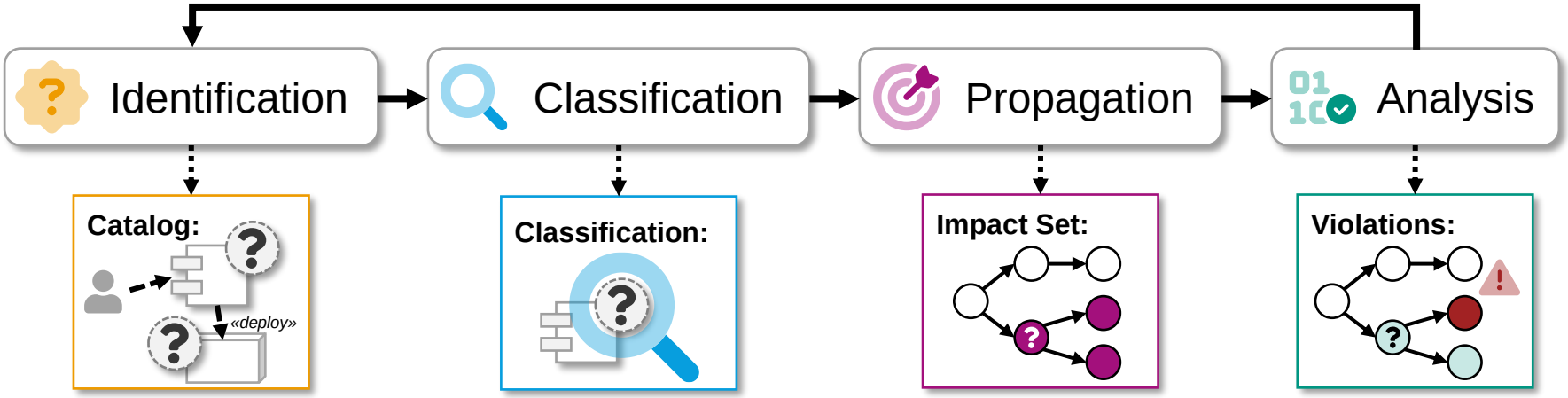
Security be like…

High precision is good…

but not without high recall.

➪ **Architecture-Based and Uncertainty-Aware Confidentiality Analysis**

Uncertainty Management at Design Time [10,13]



Goal: Define a **catalog** and **classification** of uncertainty sources regarding confidentiality. Provide architectural analyses that **predict the impact** of uncertainty and **identify confidentiality violations** due to uncertainty.

[10] S. M. Hezavehi, et al., "Uncertainty in Self-adaptive Systems: A Research Community Perspective," ACM TAAS., vol. 15, no. 4, 2021.
[13] D. Weyns, …, S. Hahner, et al., "Towards a Research Agenda for Understanding and Managing Uncertainty in Self-Adaptive Systems," ACM SIGSOFT SEN, vol. 48, no. 4, 2023.

Contribution Overview

Identification and Classification of Uncertainty w.r.t. Confidentiality

C1

[ECSA-C 2021] [ACM MODELS-C 2022] [Springer ICETE 2023] [ACM/IEEE MODELS-C 2024]

Architecture-Based Uncertainty Propagation and Impact Analysis

C2

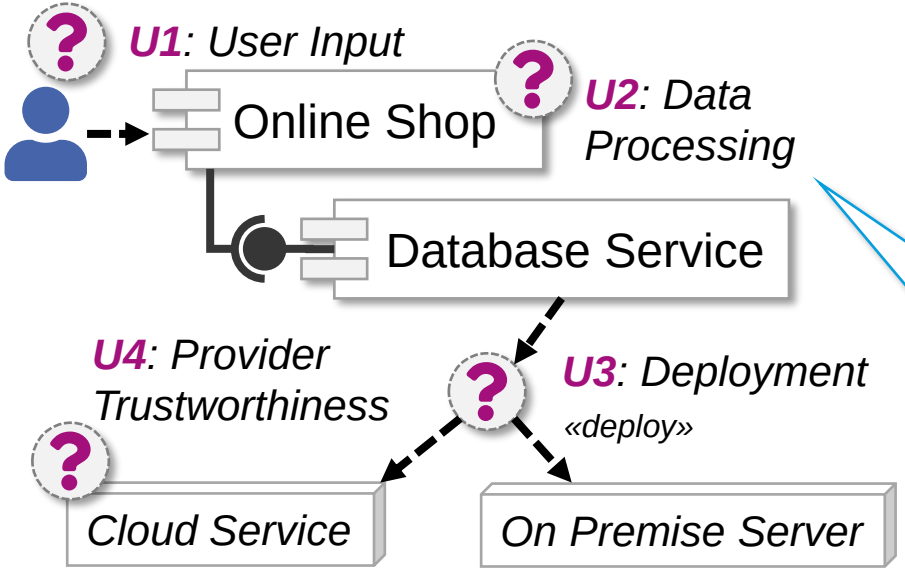
[IEEE/ACM SEAMS 2023] [IEEE/ACM SEAMS 2024]

Uncertainty-Aware Confidentiality Analysis

C3

[IEEE SEAA 2022] [Springer ECSA 2022] [IEEE ICSA-C 2023] [Springer ECSA 2024]

C2 Uncertainty Impact Analysis



What do we have?

- Classified uncertainty sources [14]
- Mapping to data flow diagrams [15]

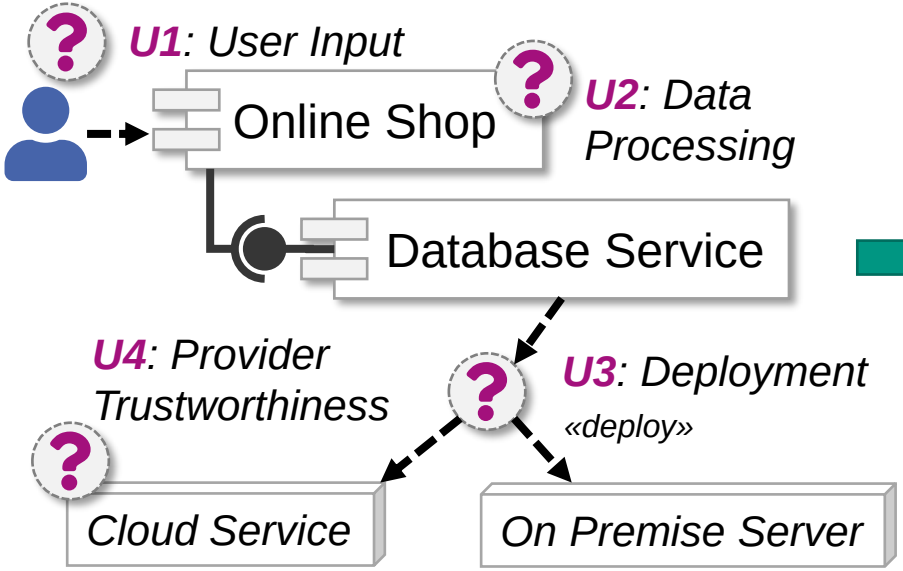
C1

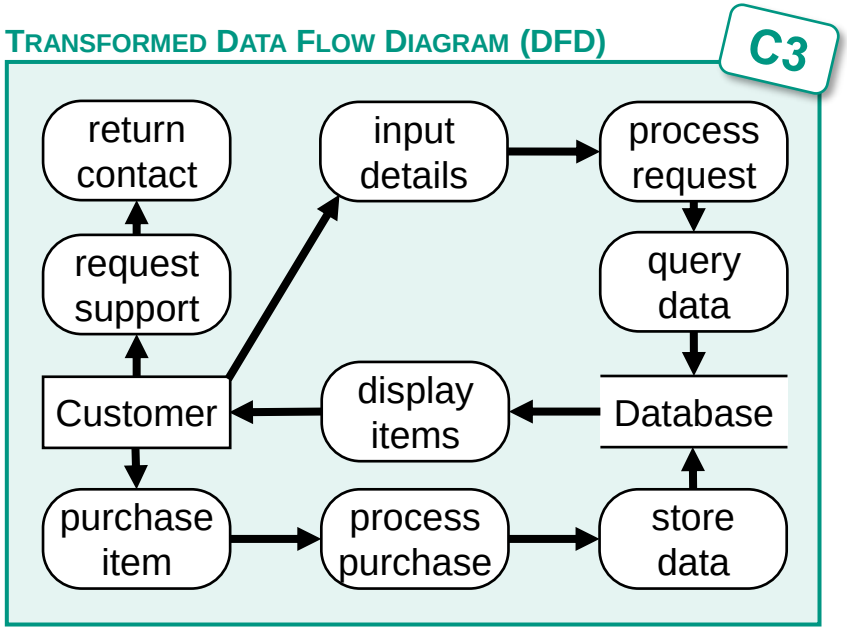
U2: Data Processing

Location:	*Behavior*
Type:	*Scenario Uncertainty*
Manageability:	*Fully Reducible*
Resolution:	*Design Time*

[14] S. Hahner, et al., “A Classification of Software-Architectural Uncertainty Regarding Confidentiality”, ICETE, Springer, 2023.
[15] N. Boltz and S. Hahner, et al., “An Extensible Framework for Architecture-Based Data Flow Analysis for Information Security”, ECSA, Springer, 2024.

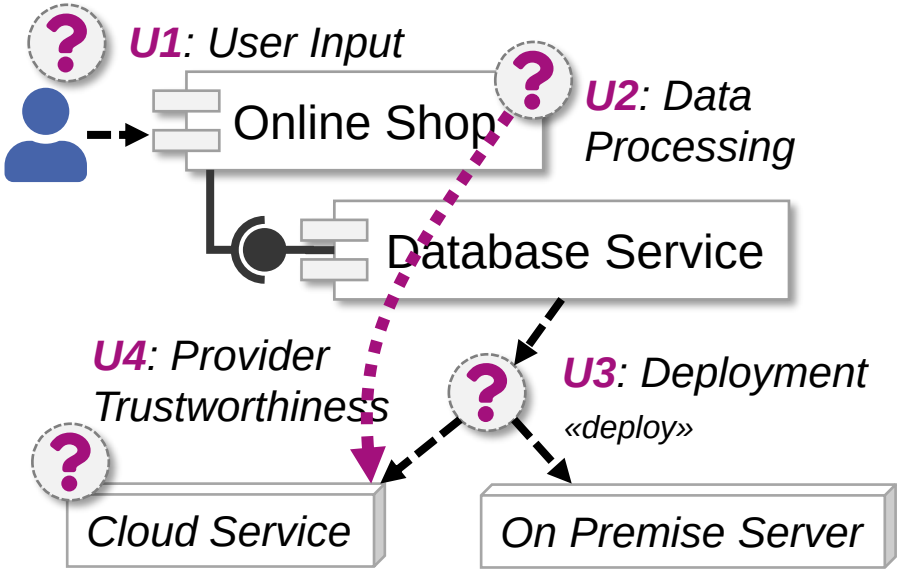
C2 Uncertainty Impact Analysis





[14] S. Hahner, et al., "A Classification of Software-Architectural Uncertainty Regarding Confidentiality", ICETE, Springer, 2023.
[15] N. Boltz and S. Hahner, et al., "An Extensible Framework for Architecture-Based Data Flow Analysis for Information Security", ECSA, Springer, 2024.

C2 Uncertainty Impact Analysis



What do we have?

- Classified uncertainty sources [14]
- Mapping to data flow diagrams [15]

What do we want?

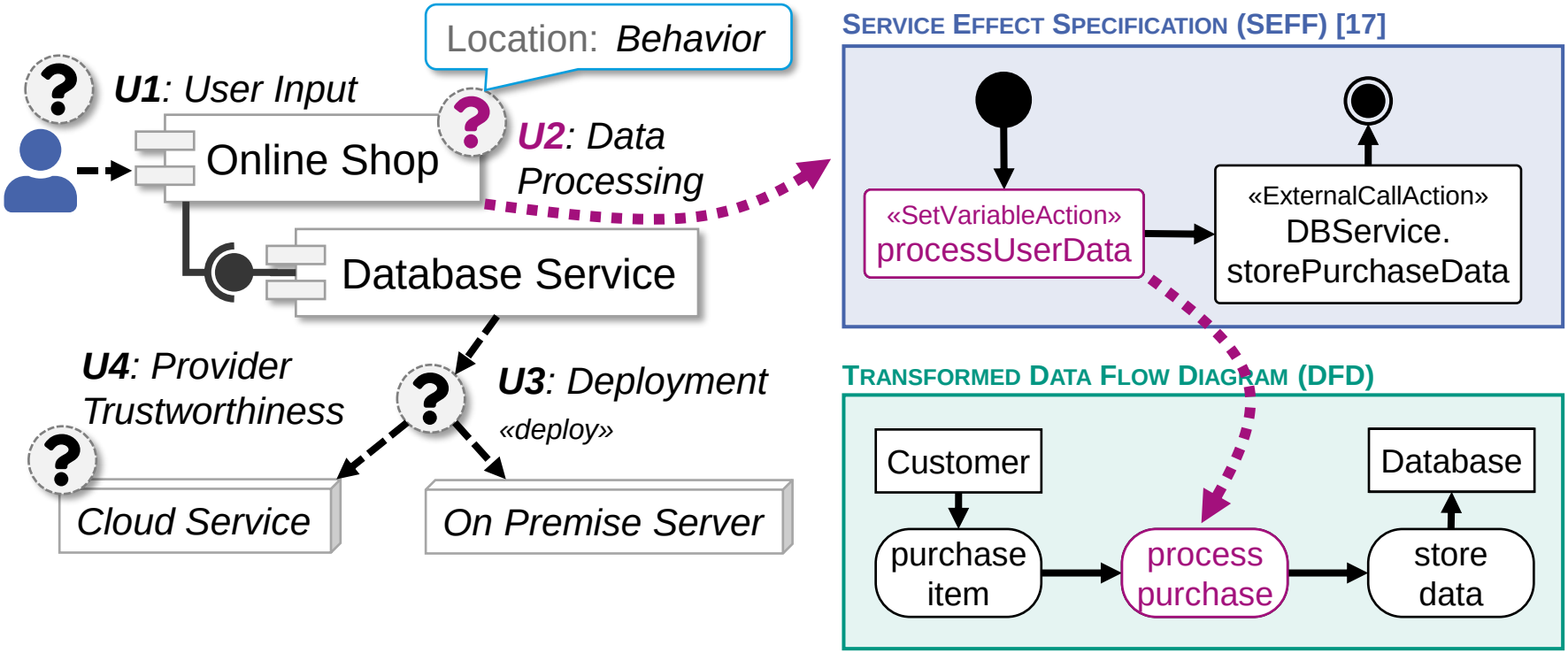
- **Propagating** uncertainty sources
- Assessing the uncertainties' impact

How do we get there?

- Change impact analysis [16]
- Data flow-based propagation [7]

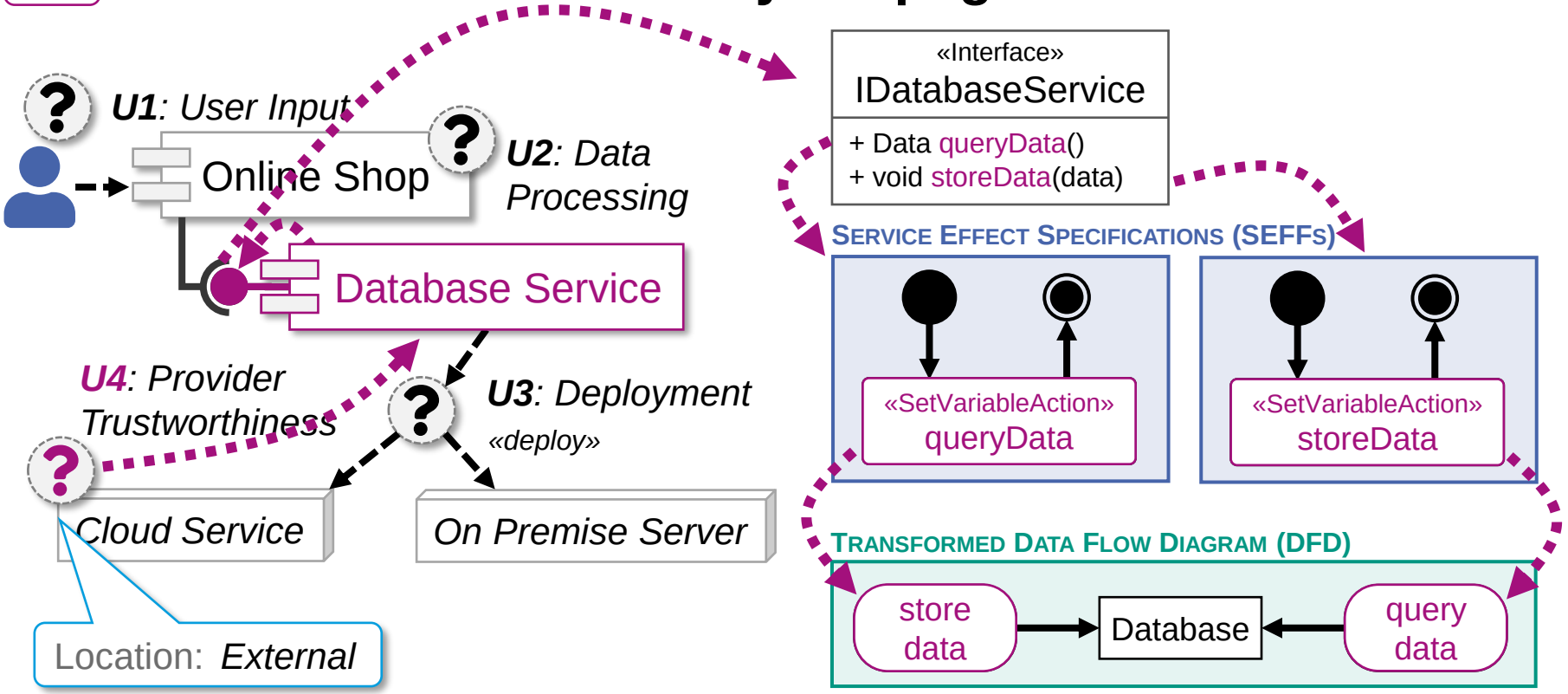
[14] S. Hahner, et al., "A Classification of Software-Architectural Uncertainty Regarding Confidentiality", ICETE, Springer, 2023.
[15] N. Boltz and S. Hahner, et al., "An Extensible Framework for Architecture-Based Data Flow Analysis for Information Security", ECSA, Springer, 2024.
[16] K. Rostami, et al. "Architecture-Based Change Impact Analysis in Information Systems and Business Processes", ICSA, IEEE, 2017.
[7] S. Seifermann, et al., "Detecting violations of access control and information flow policies in data flow diagrams", JSS, vol. 184, Elsevier, 2022.

C2 Architectural Uncertainty Propagation



[17] R. Reussner et al., “Modeling and Simulating Software Architectures: The Palladio Approach”, The MIT Press, 2016.

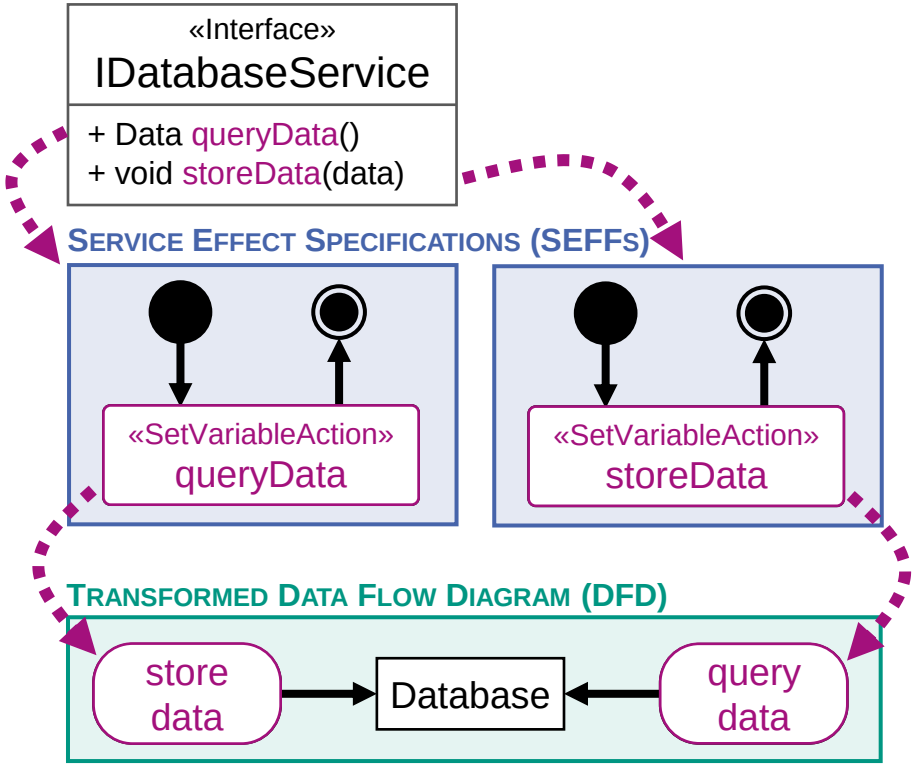
C2 Architectural Uncertainty Propagation



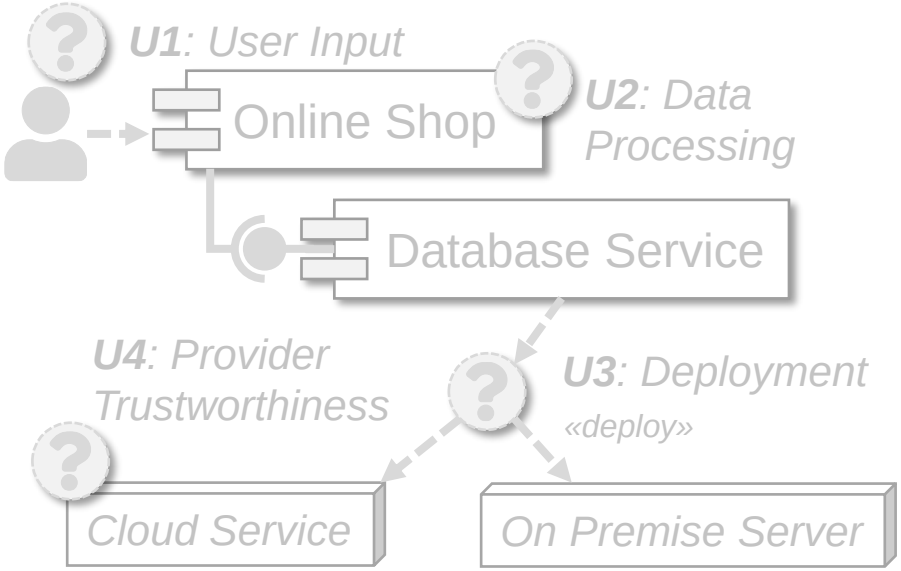
C2 Architectural Uncertainty Propagation

Algorithm for External Uncertainty Propagation

```
1: procedure PROPAGATEEXTERNALUNCERTAINTY(uncertainty, model)
2:     result ← ∅
3:     annotatedElement ← GETANNOTATEDELEMENT(uncertainty, model)
4:     switch TYPEOF(annotatedElement) do
5:         case UsageScenario
6:             actions ← GETACTIONS(annotatedElement, model)
7:             for action ∈ actions do
8:                 if TYPEOF(action) = EntryLevelSystemCall then
9:                     result ← result ∪ {action}
10:                end if
11:            end for
12:        case ResourceContainer
13:            allAssemblyContexts ← GETALLASSEMBLYCONTEXTS(model)
14:            for context ∈ allAssemblyContexts do
15:                if GETALLOCATION(context, model) = annotatedElement then
16:                    component ← GETREPOSITORYCOMPONENT(context, model)
17:                    seffs ← GETSEFFS(component, model)
18:                    for seff ∈ seffs do
19:                        actions ← GETACTIONS(seff, model)
20:                        result ← result ∪ APPLYTOASSEMBLY(actions, context)
21:                    end for
22:                end if
23:            end for
24:    return result
25: end procedure
```



C2 Uncertainty Impact Analysis



What do we have?

- Classified uncertainty sources [14]
- Mapping to data flow diagrams [15]

What do we want?

- **Propagating** uncertainty sources
- Assessing the uncertainties' impact

How do we get there?

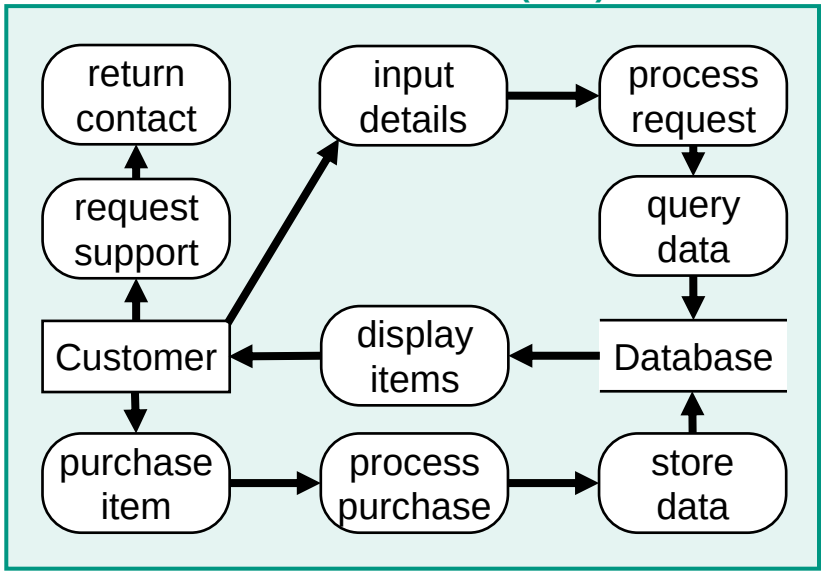
- Change impact analysis **[16]**
- Data flow-based propagation [7]

[14] S. Hahner, et al., "A Classification of Software-Architectural Uncertainty Regarding Confidentiality", ICETE, Springer, 2023.
[15] N. Boltz and S. Hahner, et al., "An Extensible Framework for Architecture-Based Data Flow Analysis for Information Security", ECSA, Springer, 2024.
[16] K. Rostami, et al. "Architecture-Based Change Impact Analysis in Information Systems and Business Processes", ICSA, IEEE, 2017.
[7] S. Seifermann, et al., "Detecting violations of access control and information flow policies in data flow diagrams", JSS, vol. 184, Elsevier, 2022.

C2 Data Flow-Based Propagation

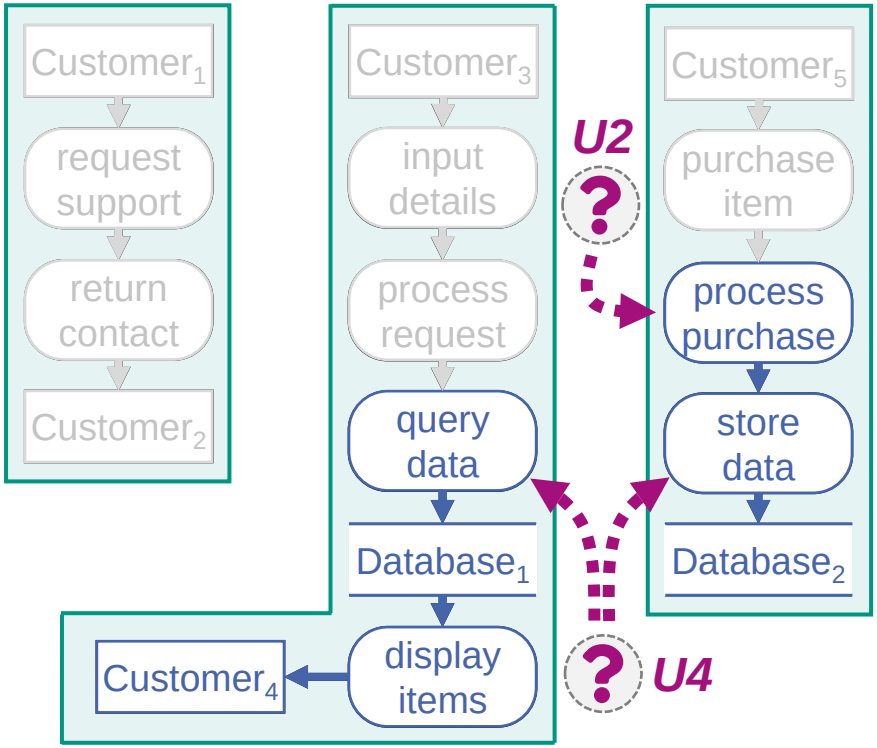
- Data flow diagrams can be represented as Directed Acyclic Graph (DAG) **G** = (**V**, **E**)
  - Data flows in a strict partial order **v' ≺ v"**
  - Split into Transpose Flow Graphs (TFGs)

TRANSFORMED DATA FLOW DIAGRAM (DFD)

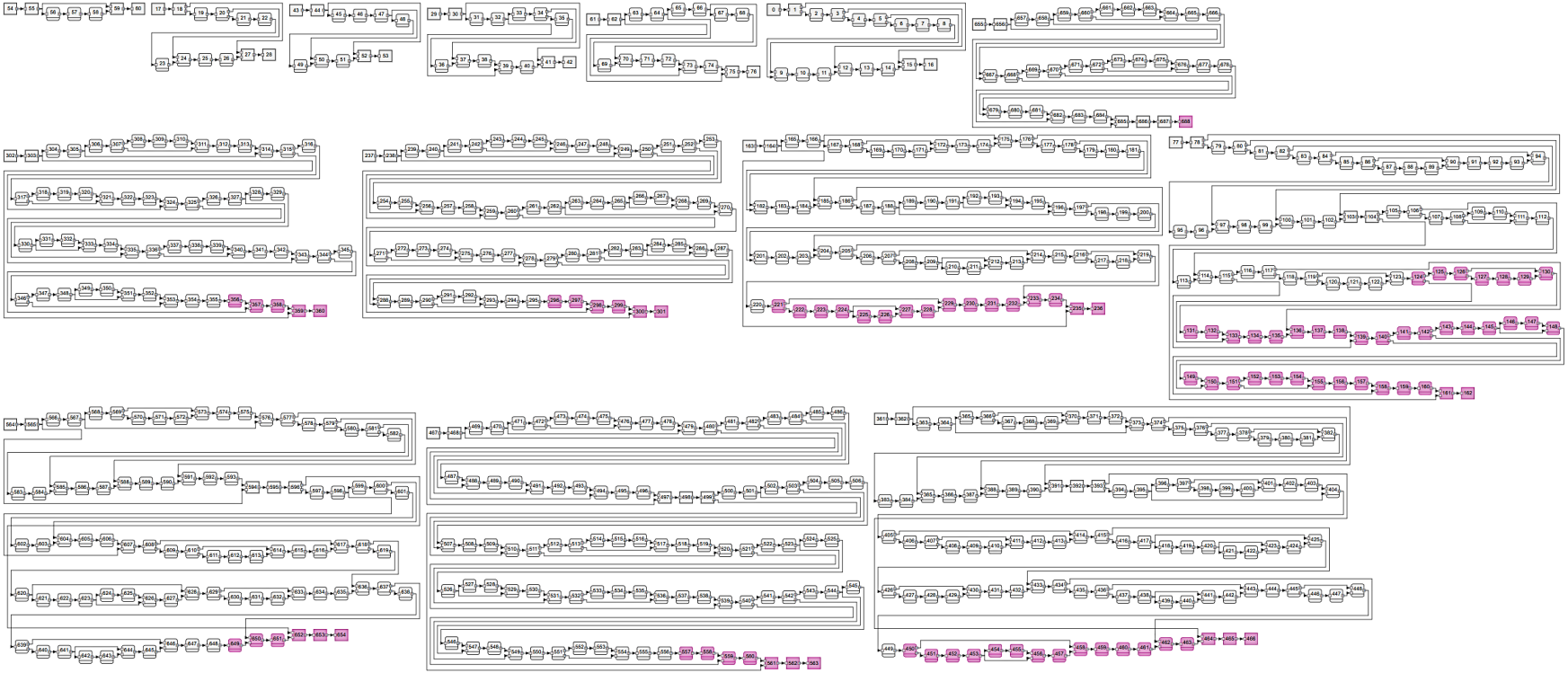


C2 Data Flow-Based Propagation

- Data flow diagrams can be represented as Directed Acyclic Graph (DAG) **G** = (**V**, **E**)
  - Data flows in a strict partial order **v' ≺ v"**
  - Split into Transpose Flow Graphs (TFGs)
- We reuse the annotation function **a**, the architectural propagation p_A, and the mapping **m** from the architecture **A**
- The data flow-based propagation p_D: **V** → **X** ⊆ **V** yields an impact set, represented by an induced subgraph **G[X]**
- Uncertainty impacts follow the data flow: **∀ x ∈ X ⊆ V, ∃ a ∈ A : m(a) = x ∨ m(a) ≺ x**
- The impact analysis of an uncertainty source **S** is a function **u : S → X ⊆ V**, defined as **u** = p_D ∘ **m** ∘ p_A ∘ **a**



Demonstration of Uncertainty Impact Sets

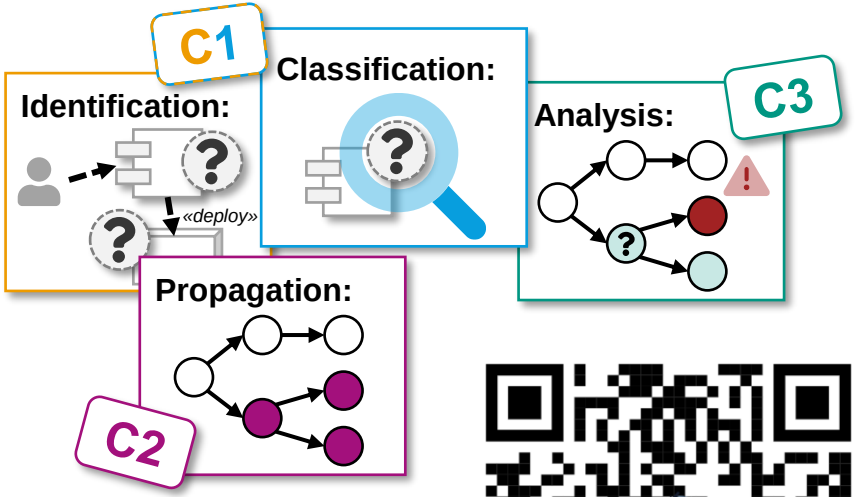


Conclusion

- **Foundation:** Data flow-based confidentiality analysis using the software's architecture
- **Goal:** Enabling to identify confidentiality violations with respect to uncertainty
- **Benefits:** Less expertise and less manual effort required, what-if analysis capabilities

Contributions:

- **C1: Identification** and **classification** of uncertainty regarding confidentiality
- **C2**: Architecture-based uncertainty **propagation** and impact analysis
- **C3**: Uncertainty-aware confidentiality **analysis** to identify violations



Dissertation, Tooling, Data

https://thesis.abunai.dev