Karlsruhe Institute of Technology

FluidTrust
Trust by fluid access control in Industry 4.0

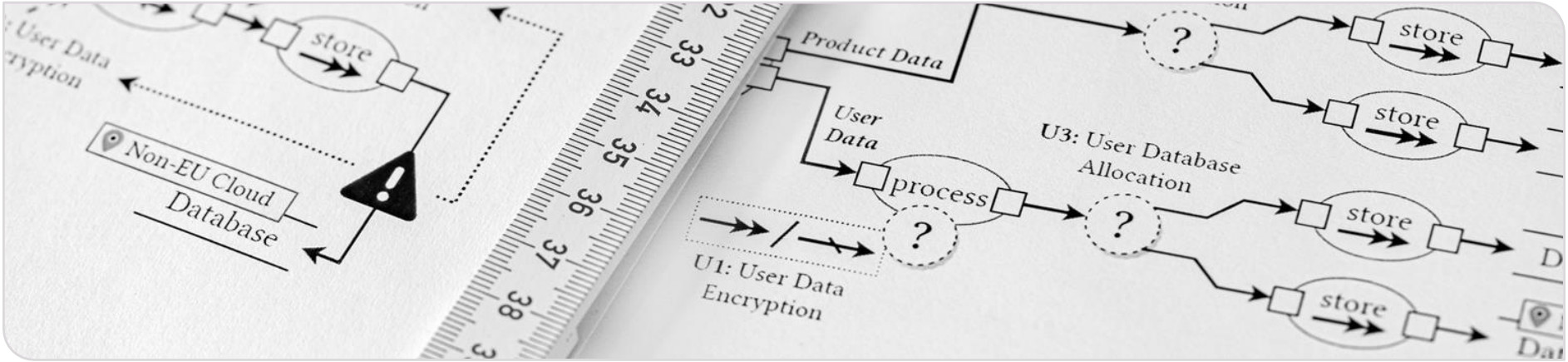
KASTEL

# Model-based Confidentiality Analysis under Uncertainty

3rd International Workshop on Model-driven Engineering for Software Architecture, MDE4SA 2023

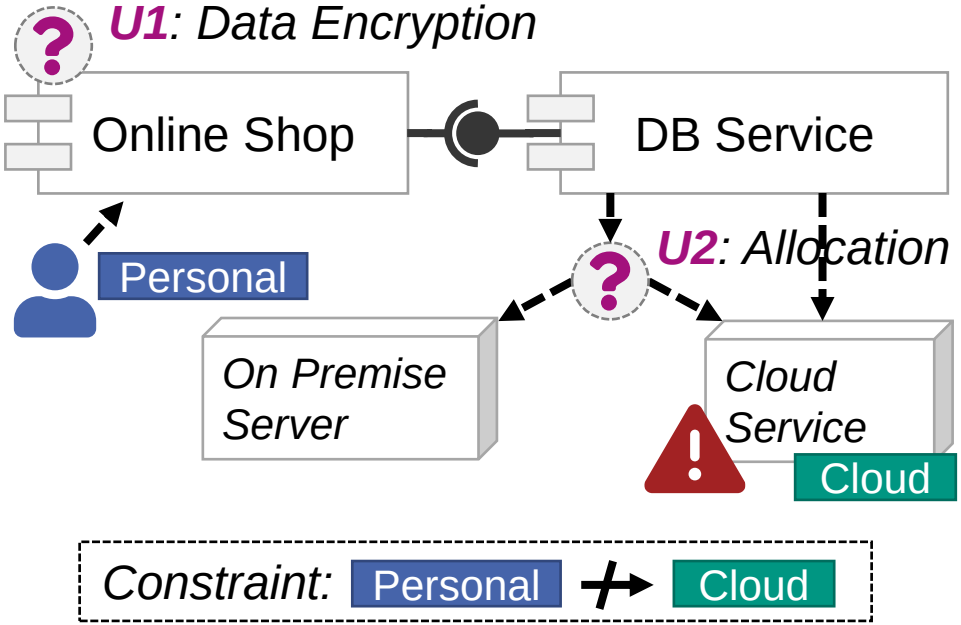
20th IEEE International Conference on Software Architecture, ICSA 2023

**Sebastian Hahner, Tizian Bitschi, Maximilian Walter, Tomáš Bureš, Petr Hnětynka, Robert Heinrich**



# Motivation

- Data flow-based design-time analyses identify confidentiality violations in architectural models **[1]**
  - Model software architecture
  - Define characteristics and constraints
  - Analyze data flows on confidentiality
- Challenge: Uncertainty both in the system and its environment **[2]**
- **Gap**: Existing approaches use the modeled information suboptimally




**[1]** S. Seifermann et al., “Detecting violations of access control and information flow policies in data flow diagrams”, In: *JSS*, vol. 184, 2022.
**[2]** M. Acosta et al., “Uncertainty in coupled models of cyber-physical systems”, In: *MODELS-C*, 2022.

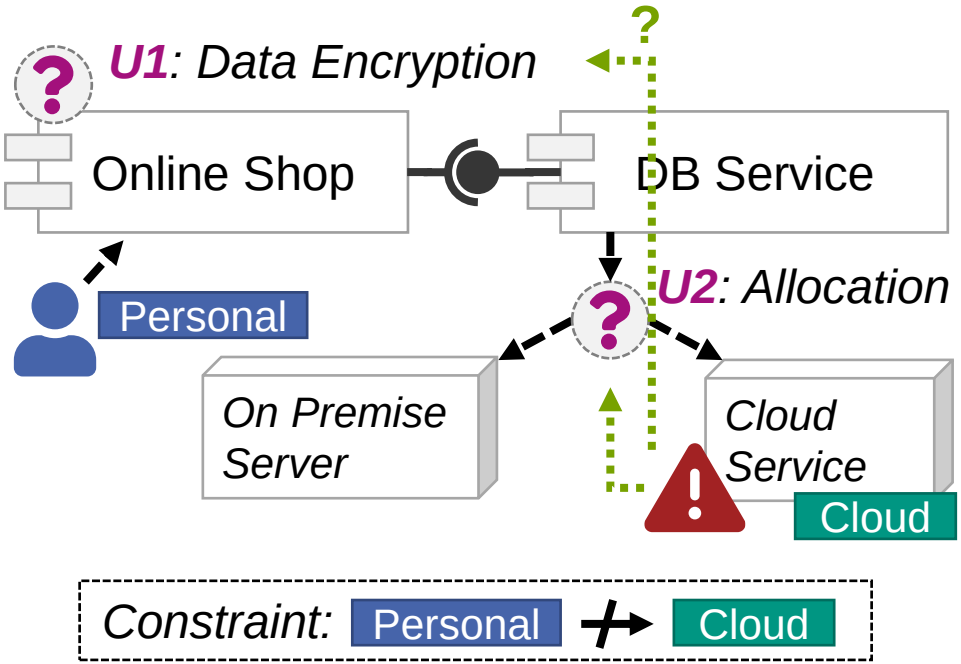
# Overview

**Idea:** Extend an existing data flow-based confidentiality analysis [1]

- Reuse existing modeling techniques
- **Trace** annotated uncertainty

## Contributions

- Discussion of available information at design time and how to use it
- An uncertainty-aware confidentiality analysis based on model variation

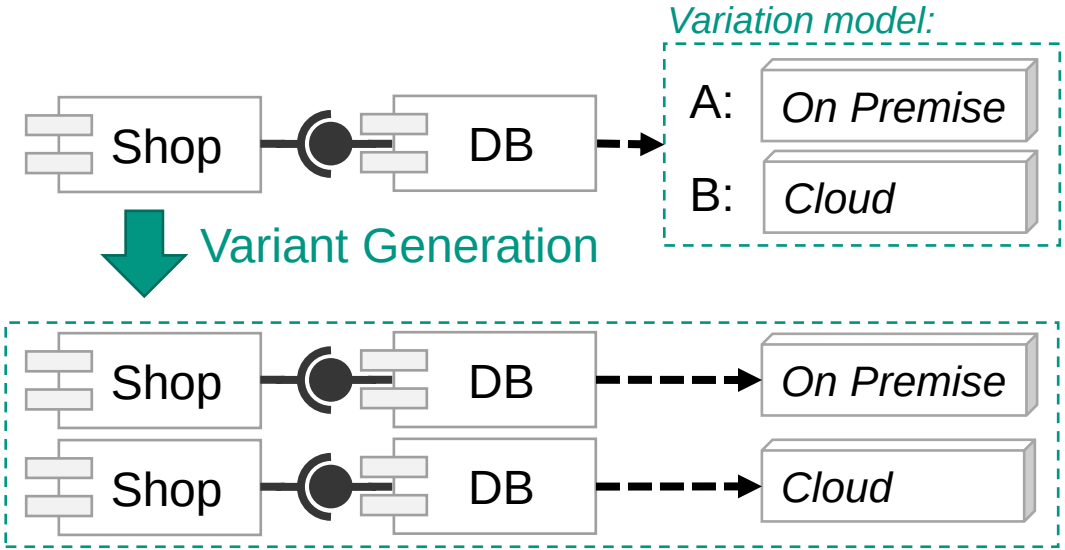



[1] S. Seifermann et al., “Detecting violations of access control and information flow policies in data flow diagrams”, In: *JSS*, vol. 184, 2022.

# Expressing Uncertainty as Model Variation

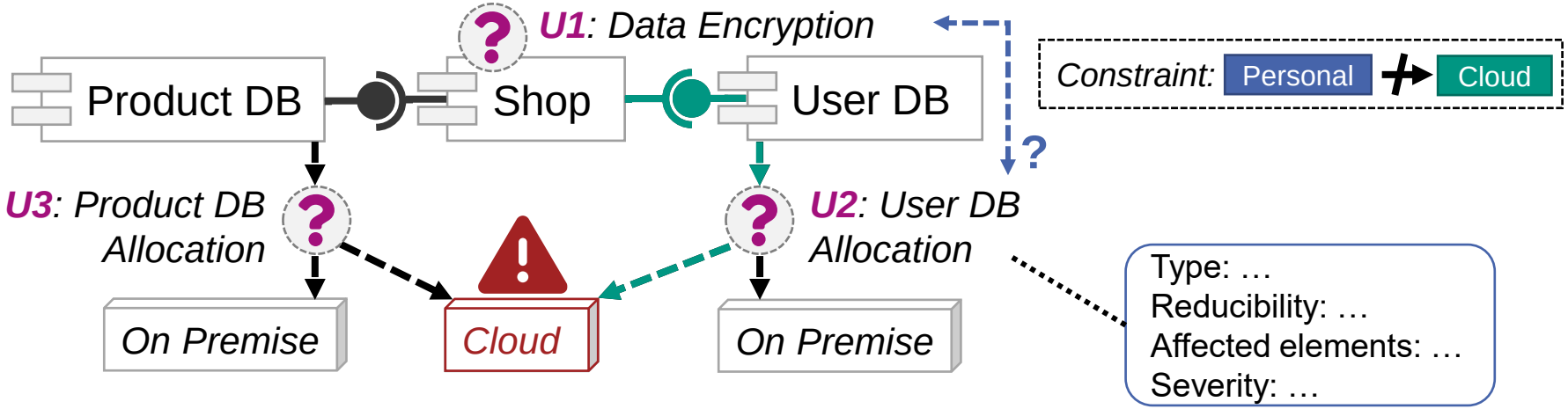
Uncertainty: “any departure from the unachievable ideal of complete determinism” **[3]**

- Design uncertainty is “normally represented in software models by variability models” **[4]**
- Variation model represents all known uncertainty impacts
- Variant Generation creates all possible variants of the software architecture **[5]**
- Usable with existing analyses




**[3]** W. E. Walker et al., “Defining uncertainty: a conceptual basis for uncertainty management in model-based decision support,” Integrated assessment, vol. 4, 2003.
**[4]** J. Troya et al., “Uncertainty representation in software models: A survey”, In: *SoSyM*, 8, 2021.
**[5]** M. Walter et al., “Architectural attack propagation in industry 4.0”, In: *at – Automatisierungstechnik*, 2023. Accepted, to appear.

# Available Information in Modeling and Analysis



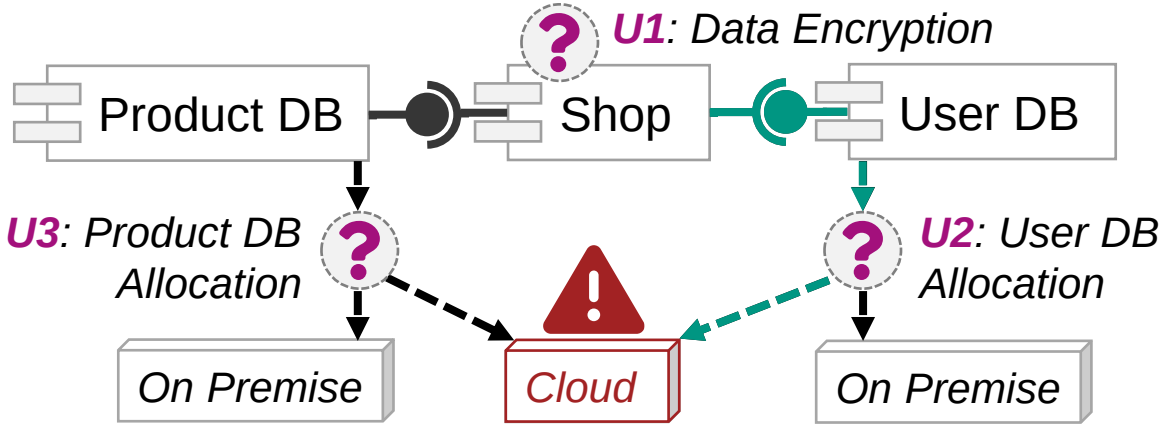

## Confidentiality

- Violation occurrence
- Violated constraint
- Location in the model
- Affected data flow
- Variable state

## Uncertainty

- Source
- Classification
- Impact in the model
- Mitigation
- Uncertainty Interaction

# Towards Uncertainty Awareness




Encrypted, On Premise, On Premise
Encrypted, On Premise, Cloud
Encrypted, Cloud, On Premise
Encrypted, Cloud, Cloud
¬Encrypted, On Premise, On Premise
¬Encrypted, On Premise, Cloud
¬Encrypted, Cloud, On Premise
¬Encrypted, Cloud, Cloud

## Naive approach

- Rejects the complete architecture
- Uses the violation occurrence only

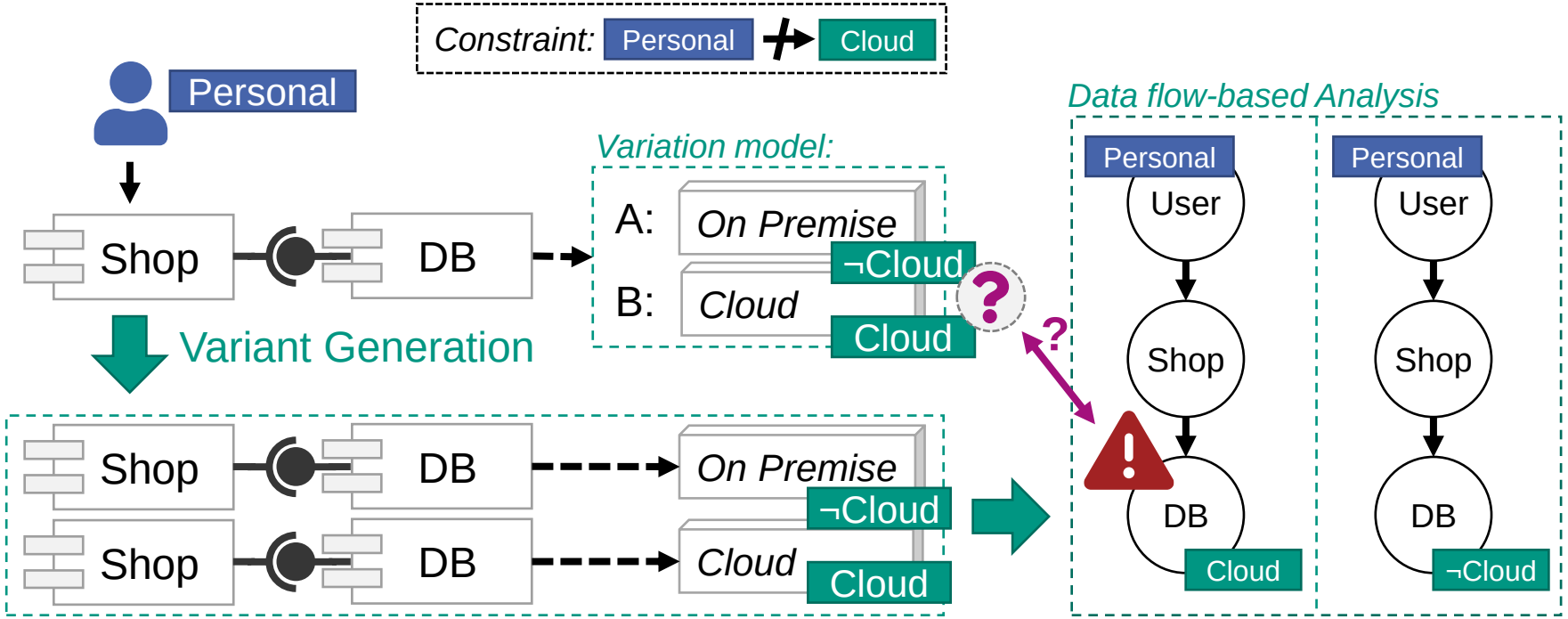
## Scenario-aware

- Only rejects variants with violations
- Uses uncertainty impact and violation occurrence

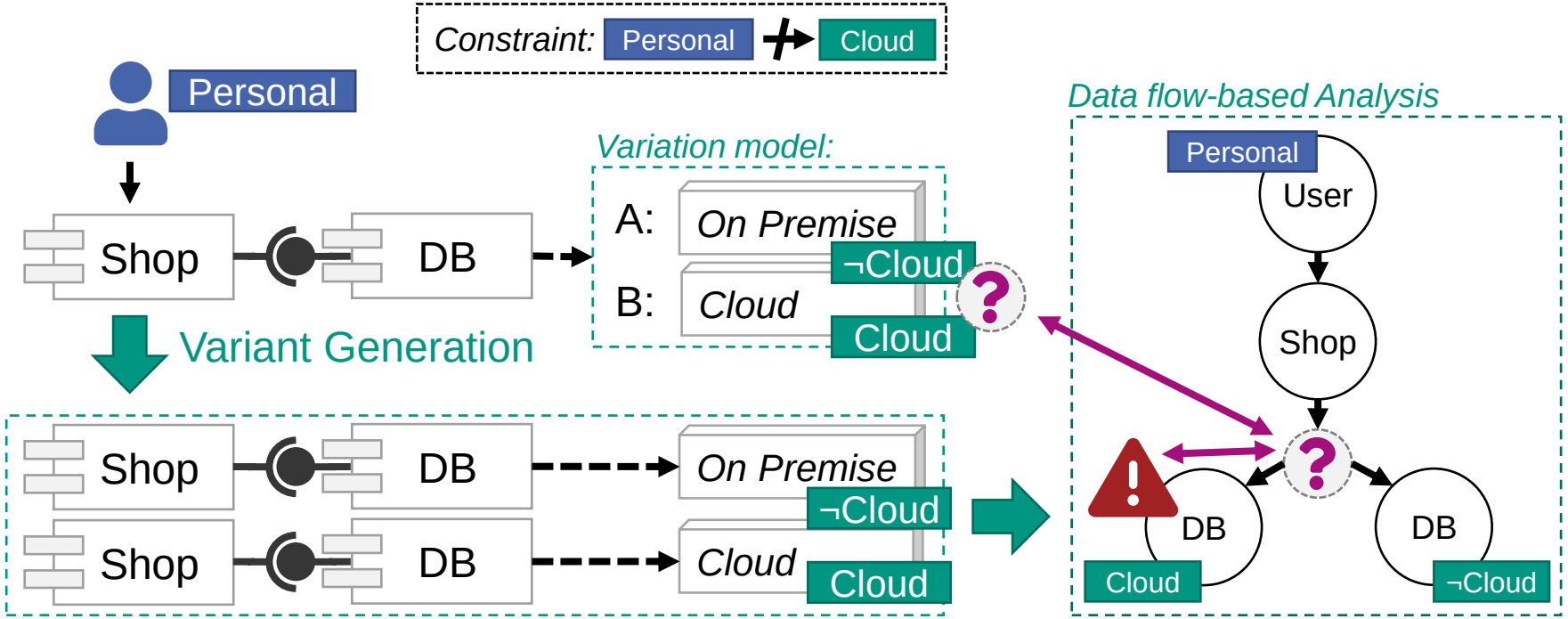
## Data flow-aware

- Traces violations back to potentially causing uncertainty impacts
- Yields affected data flows

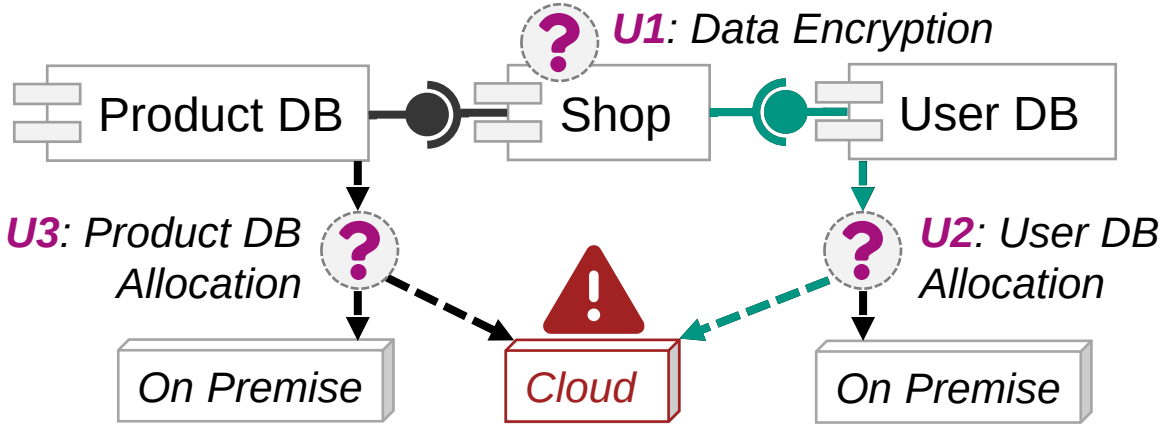
# Uncertainty-Aware Confidentiality Analysis



# Uncertainty-Aware Confidentiality Analysis



# Using Available Information in the Analysis




Encrypted, On Premise, On Premise
Encrypted, On Premise, Cloud
Encrypted, Cloud, On Premise
Encrypted, Cloud, Cloud
¬Encrypted, On Premise, On Premise
¬Encrypted, On Premise, Cloud
¬Encrypted, Cloud, On Premise
¬Encrypted, Cloud, Cloud

## Scenario-aware Analysis

- There are 4 variants with confidentiality violations
- The variants have the following characteristics: …

## Data flow-aware Analysis

- There are 4 confidentiality violations
- All violations happen in the *User DB*
- This is due to uncertainties: **U1**, **U2**
- *Product DB* and **U3** are not involved

# Case Study-based Evaluation

## Goal Question Metric Plan [6]

- Accuracy: Measure precision and recall regarding uncertainty, compare with SOTA
- Usability: Reducing effort and complexity for software architects at design time

## Case Study

- Reusing existing scenarios **[1]** with different confidentiality requirements
- Apply the naive approach, the scenario-aware and the data flow-aware approach

## Results

- Expected: All approaches have a high recall, but the precision differs
- The data flow-aware approach correctly identifies relevant uncertainty impacts
- Effort reduction compared to manual analysis only using design time information

**[1]** S. Seifermann et al., “Detecting violations of access control and information flow policies in data flow diagrams”, In: *JSS*, vol. 184, 2022.
**[6]** V. Basili and D. Weiss. “A methodology for collecting valid software engineering data”, In: *TSE* 6, 1984.

# Related Work

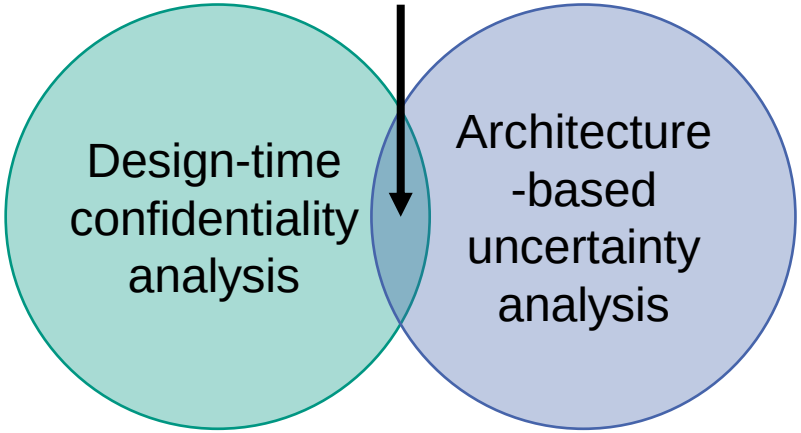
- Pattern-based **[7]** or data flow-based analysis **[1]**

⇨ *No uncertainty*

- Design space exploration like GuideArch **[8]** or PerOpteryx **[9]**

⇨ *No confidentiality*

*Our approach*




- Uncertainty-aware confidentiality analysis is only *scenario-aware*
  - Combination of data flow-based analysis with PerOpteryx **[10]**
  - Extending data flow-based analysis with fuzzy inference **[11]**

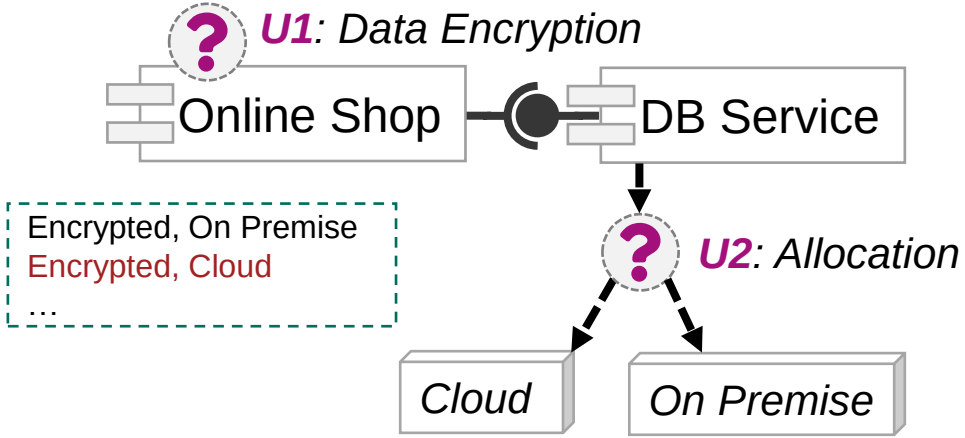
**[1]** S. Seifermann et al., “Detecting violations of access control and information flow policies in data flow diagrams”, In: *JSS*, vol. 184, 2022.
**[7]** K. Tuma et al., “Automating the early detection of security design flaws”, In: *MODELS*, 2020.
**[8]** N. Esfahani et al., “GuideArch: Guiding the exploration of architectural solution space under uncertainty”, In: *ICSE*, 2013.
**[9]** A. Koziolek et al., “PerOpteryx: Automated application of tactics in multi-objective software architecture optimization”, In: *ISARCS*, 2011.
**[10]** M. Walter et al., “Architectural optimization for confidentiality under structural uncertainty”, In: *Software Architecture*, Springer, 2022.
**[11]** N. Boltz et al., “Handling environmental uncertainty in design time access control analysis”, In: *SEAA*, 2022.

# Conclusion

- Problem: Analyzing confidentiality while considering uncertainty at design time
- Contribution: Uncertainty-aware confidentiality analysis based on model variation
- Benefit: Precise confidentiality statements considering data flows and uncertainty

## Future Work

- Connect confidentiality analysis to Uncertainty Impact Analysis **[12]**
- Move variant generation in the data flow analysis
- Support more uncertainty types beyond scenario uncertainty




**[12]** S. Hahner et al., “Architecture-based Uncertainty Impact Analysis to ensure Confidentiality”, In: *SEAMS*, 2023. Accepted, to appear.

# References


**[1]** S. Seifermann et al., “Detecting violations of access control and information flow policies in data flow diagrams”, In: *JSS*, vol. 184, 2022.
**[2]** M. Acosta et al., “Uncertainty in coupled models of cyber-physical systems”, In: *MODELS-C*, 2022.
**[3]** W. E. Walker et al., “Defining uncertainty: a conceptual basis for uncertainty management in model-based decision support,” Integrated assessment, vol. 4, 2003.
**[4]** J. Troya et al., “Uncertainty representation in software models: A survey”, In: *SoSyM*, 8, 2021.
**[5]** M. Walter et al., “Architectural attack propagation in industry 4.0”, In: *at – Automatisierungstechnik*, 2023. Accepted, to appear.
**[6]** V. Basili and D. Weiss. “A methodology for collecting valid software engineering data”, In: *TSE* 6, 1984.
**[7]** K. Tuma et al., “Automating the early detection of security design flaws”, In: *MODELS*, 2020.
**[8]** N. Esfahani et al., “GuideArch: Guiding the exploration of architectural solution space under uncertainty”, In: *ICSE*, 2013.
**[9]** A. Koziolek et al., “PerOpteryx: Automated application of tactics in multi-objective software architecture optimization”, In: *ISARCS*, 2011.
**[10]** M. Walter et al., “Architectural optimization for confidentiality under structural uncertainty”, In: *Software Architecture*, Springer, 2022.
**[11]** N. Boltz et al., “Handling environmental uncertainty in design time access control analysis”, In: *SEAA*, 2022.
**[12]** S. Hahner et al., “Architecture-based Uncertainty Impact Analysis to ensure Confidentiality”, In: *SEAMS*, 2023. Accepted, to appear.