INCHEON NATIONAL UNIVERSITY

한국정보처리학회 Korea Information Processing Society

CYBERSECURITY CONVERGENCE LAB

Deep Dive into IAM Security Mechanisms in Serverless Environments

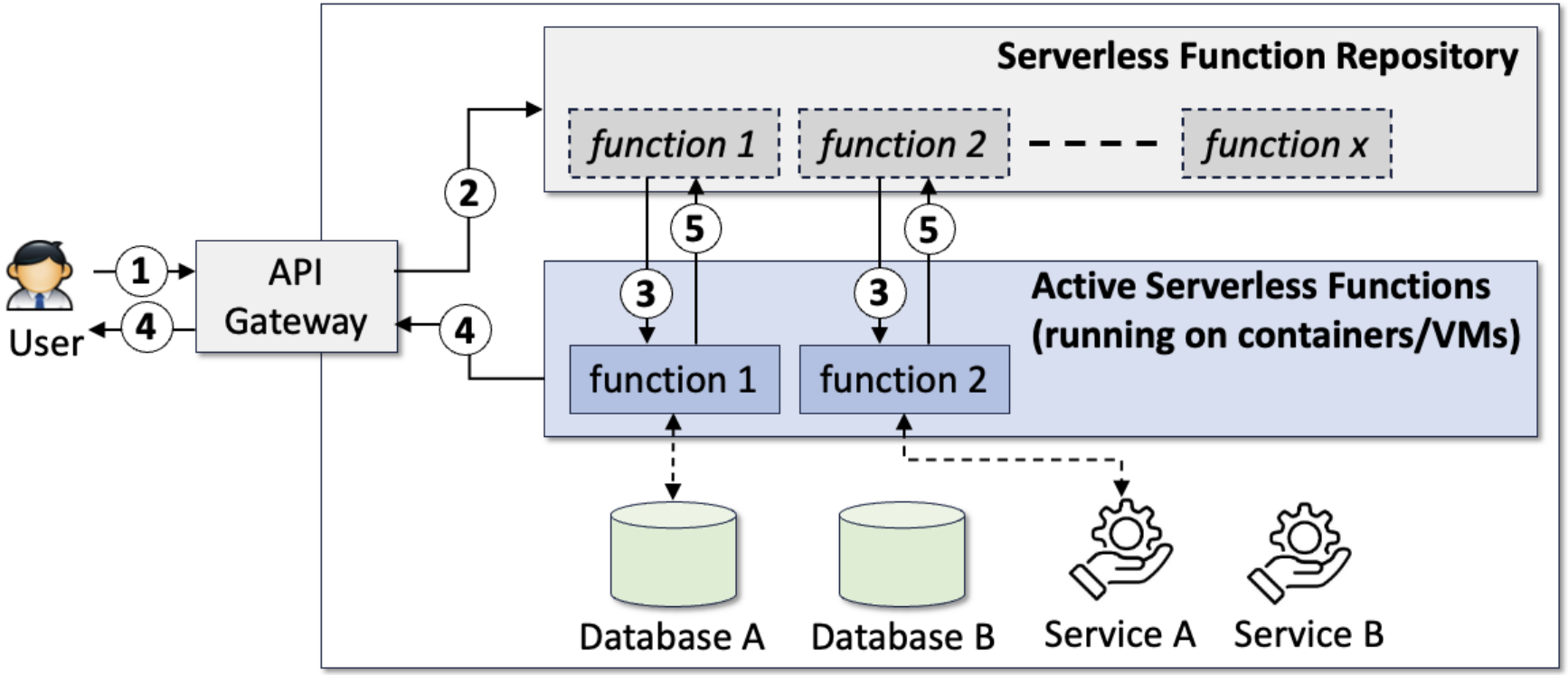
Changhee Shin

Department of Computer Science & Engineering

Incheon National University

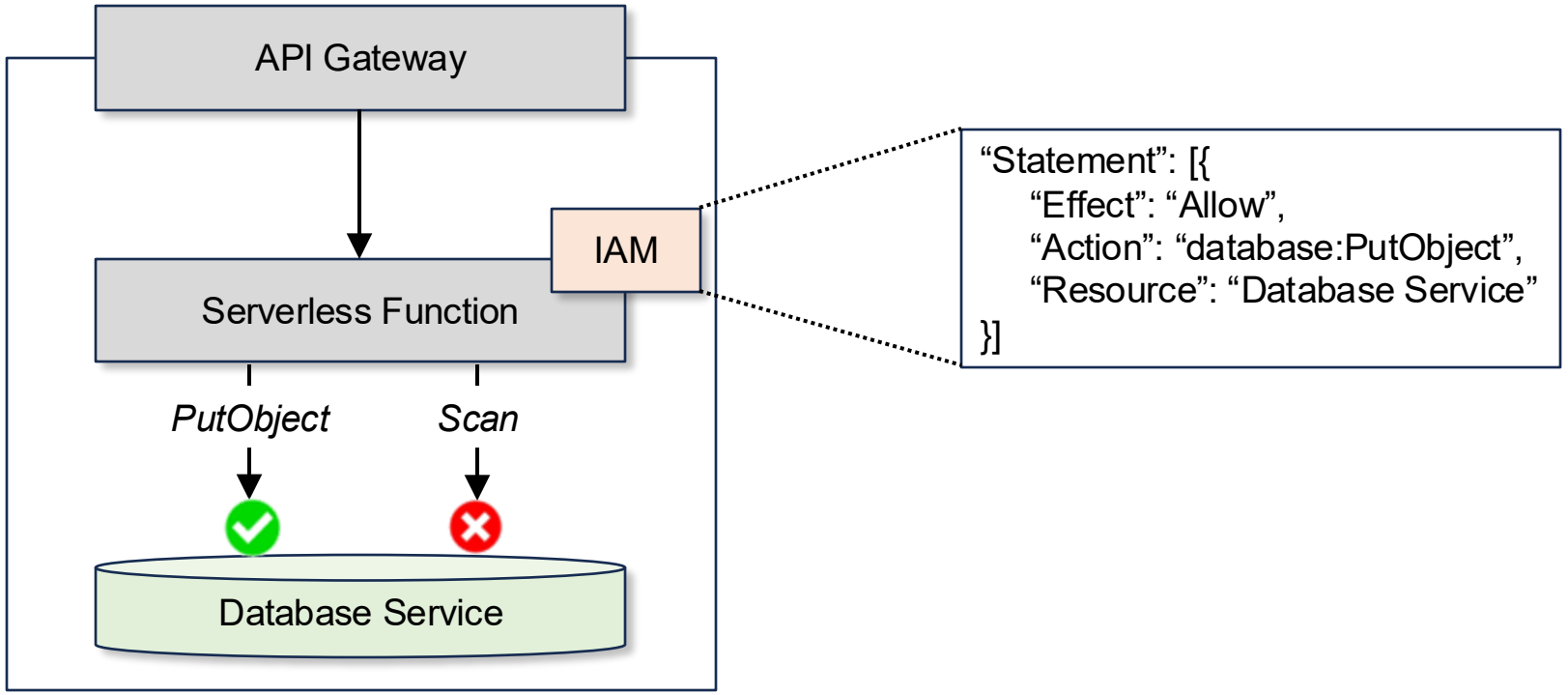
Background

- What is serverless computing?
  - Cloud execution model where developers run code **without managing servers**.



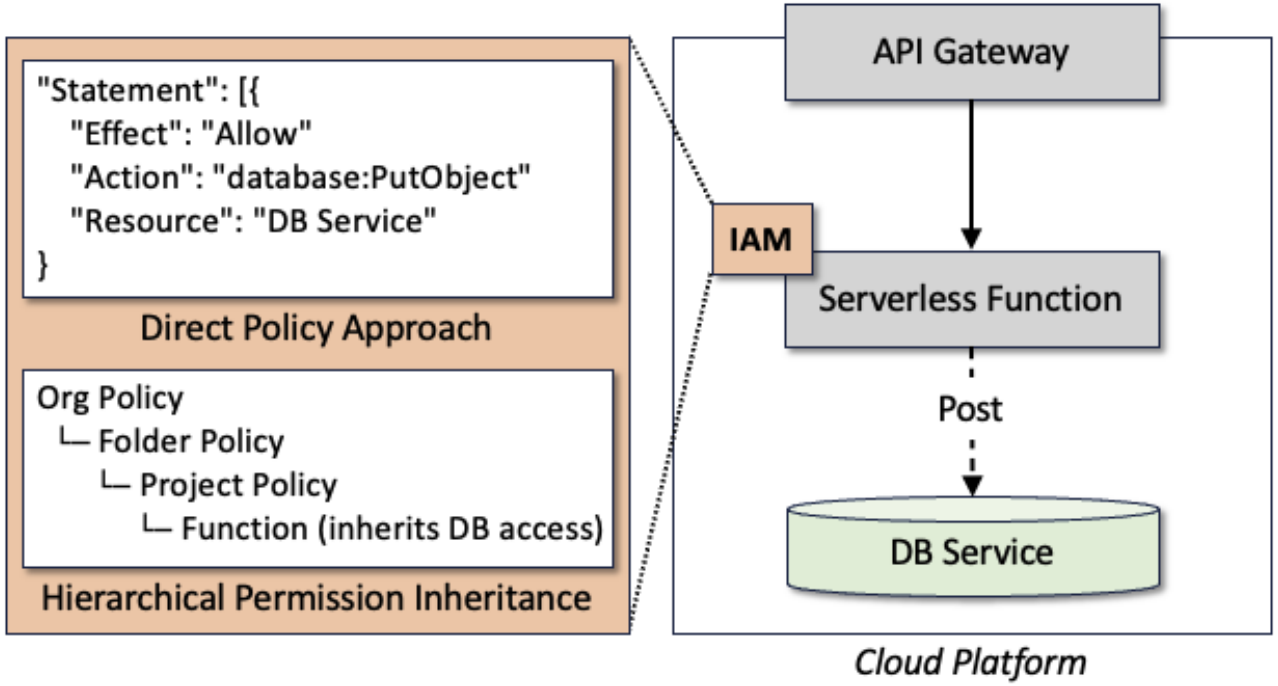
Background

- What is IAM?
  - **Access control policy to resources** and **services** provided by the cloud platform



Serverless IAM Policy Template

- Direct Policy Approach(AWS, Alibaba)
  - Policy attached **directly to each function**
- Hierarchical Permission Inheritance (Google Cloud, Azure)
  - Permissions **propagate from upper levels** (org → project → function)

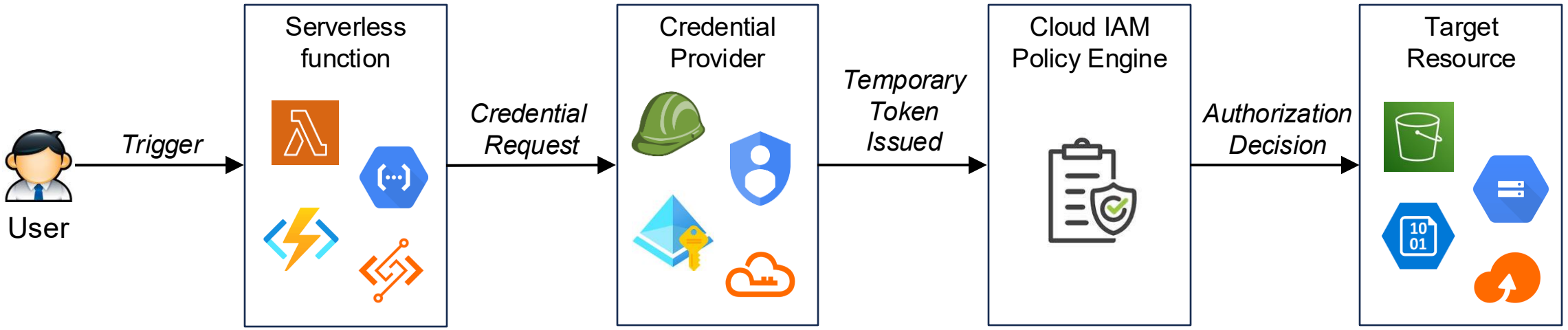


Permission Unit Structure for Serverless Functions

Model	Vendor	Advantages	Limitations
Multi-Identity	Azure	Combine or separate identities, Reuse role sets across functions	Complex isolation, Potential cross-function privilege exposure
Single-Entity	AWS, Google Cloud, Alibaba	Clear auditing & traceability, Simple management	Hard to split per-function privileges, Over-privilege risk if multiple tasks in one function

- Azure: **Flexible & reusable** identities across functions
- Others: Simple but **coarse-grained and less separable**
- Impact: **Affects least-privilege and attack surface size**

Serverless Function Execution Credentials



- AWS: Strong standardization but **complex role setup**
- GCP / Azure: Secure and flexible keyless identity model
- Alibaba Cloud: Minimal but **functional credential automation**

Security Tools and Limitations by Vendor

Vendor	Main Tools	Functions
AWS	Access Analyzer, CloudTrail	Policy exposure analysis, API logging
Google Cloud	Recommender, Security Command Center	Least privilege suggestions, threat overview
Azure	PIM, Conditional Access	Privileged account control, contextual access enforcement
Alibaba	STS, ActionTrail	Temporary tokens, access activity tracking

- Limitations
  - Static or post-execution analysis only
  - Account-level granularity
  - Lack of serverless-specific metrics & alerts

Serverless Attack Cases and IAM Effectiveness

- Attack cases
  - CloudGoat
    - Exploits **over-privileged IAM roles** and **vulnerable function code**
  - Warmonger
    - Abuses **shared egress IP pools** to bypass network isolation
  - LeakLess
    - Launches **transient execution–based attacks** exploiting speculative execution flaws

Attack Case	IAM Effectiveness
CloudGoat	O
Warmonger	X
LeakLess	X

IAM Research Trends and Future Works

- Research Trends
  - Dynamic Log Analysis
  - Static Function Analysis
  - Graph based Flow Detection
  - Allow-List Access Control

- Future Directions
  - **Context-aware** IAM with **runtime adaptation**
  - **Consistent policy generation** across **multi-clouds**
  - **Unified IAM** integrating **runtime & context**

Conclusion

- In this paper, we conducted an in-depth analysis of ***IAM***, the core security mechanism in serverless environments.

- Unlike prior works limited to specific platforms, it ***systematically compared IAM architectures and vulnerabilities*** across major cloud providers.

- The findings ***reveal current limitations of IAM*** and provide ***practical insights*** for policy design and future cloud security research.