CloakVM

A Runtime System for Confidential Serverless Functions

Michael Hackl (michael.hackl@tum.de)
Advisors: Patrick Sabanic, Dimitrios Stavrakakis
Chair of Computer Systems
https://dse.in.tum.de/

01.10.2024 – 15.04.2025

Serverless Functions & Confidentiality

- Serverless Functions (FaaS)
  - Developers focus on code (functions), not infrastructure
  - Provider manages scaling, OS, runtime
- Problem: sensitive data is exposed
  - Users must trust the provider/host OS/hypervisor

Confidential Computing & TEEs

- Confidential Computing
  - Protects data during execution using hardware-based **trusted execution environments** (TEEs) from the host (OS, hypervisor, administrators)
  - Provides confidentiality & integrity
  - Remote attestation
- TEE categories
  - Process-based (e.g., Intel SGX) → enclaves
  - VM-based (e.g., AMD SEV-SNP, Intel TDX) → confidential virtual machines (CVMs)

FaaS & TEE Challenges

Straightforward approaches for confidential serverless functions:

- Function execution models
  - One TEE per function execution → high startup overhead, inefficient chaining
  - A single TEE for multiple function executions → weak isolation, attestation
- TEE implementations
  - CVMs → large TCB, long attestation
  - Enclaves → inefficient communication

CloakVM:
A Runtime System for Confidential Serverless Functions

CloakVM design goals:

- Confidentiality and integrity for functions
- Strong function isolation
- Small TCB
- Fast function startup
- Efficient function chaining

CloakVM:
A Runtime System for Confidential Serverless Functions

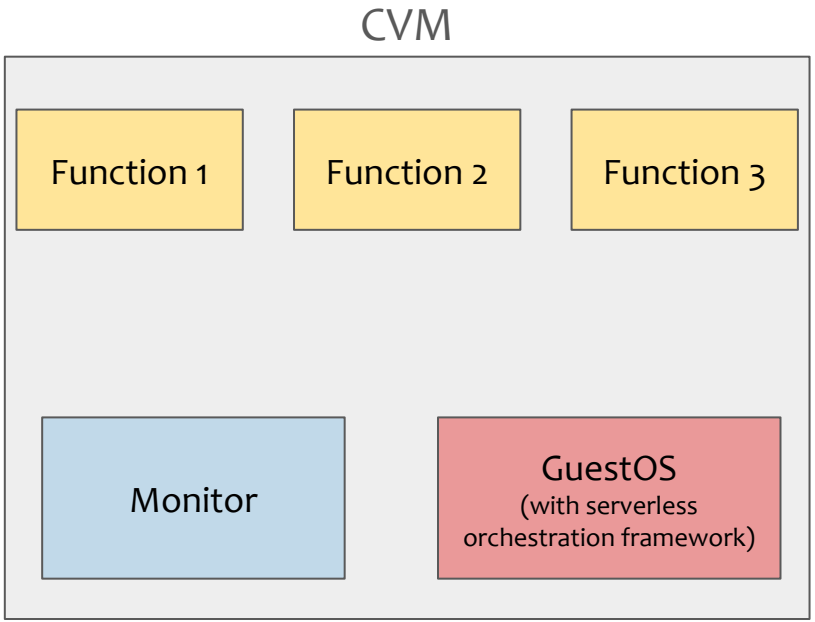
CloakVM design goals:

- Confidentiality and integrity for functions
- Strong function isolation
- Small TCB
- Fast function startup
- Efficient function chaining

Secure and efficient execution of confidential serverless functions

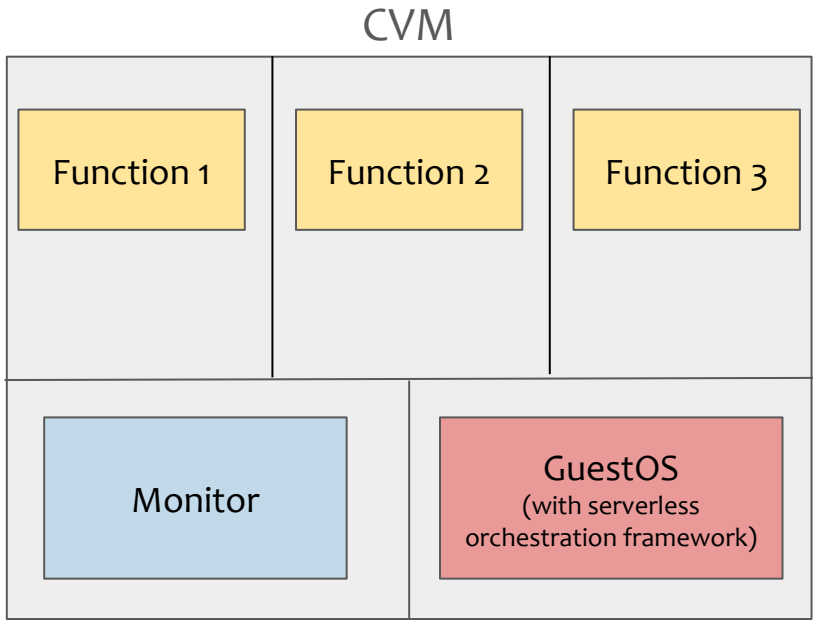
Architecture

- Single CVM with AMD SEV-SNP
- Monitor
  - Manages security and function execution
- GuestOS
  - OS (e.g., Ubuntu) for networking, storage, and orchestration (e.g., OpenWhisk)
- Functions
  - Isolated function processes



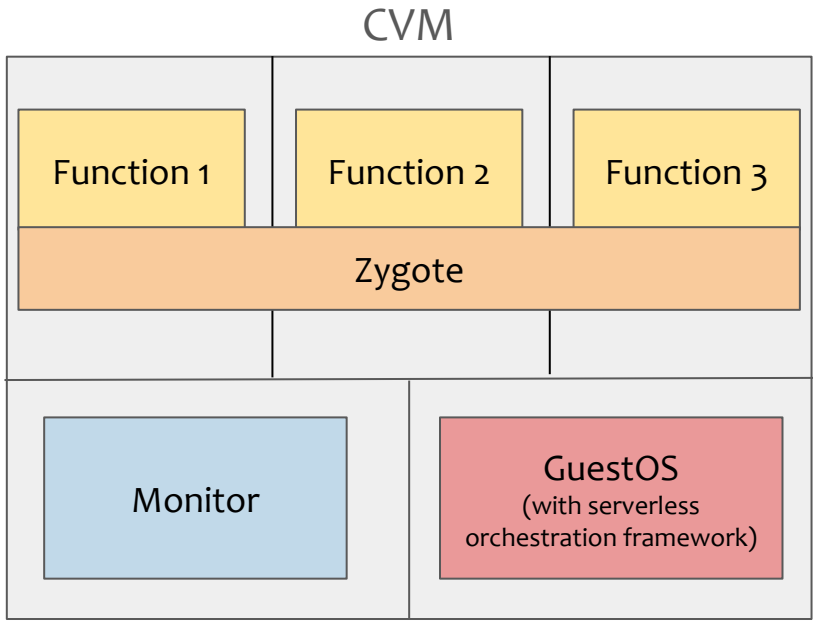
Design: Security

- Small TCB
  - Small Monitor + Function itself
  - *Host system + GuestOS are untrusted*
- Attestation
  - AMD SEV-SNP provides remote attestation
- Isolation
  - CVM from host ⟶ hardware TEE
  - Components from each other ⟶ Virtual Machine Privilege Levels (VMPLs) and separate address spaces



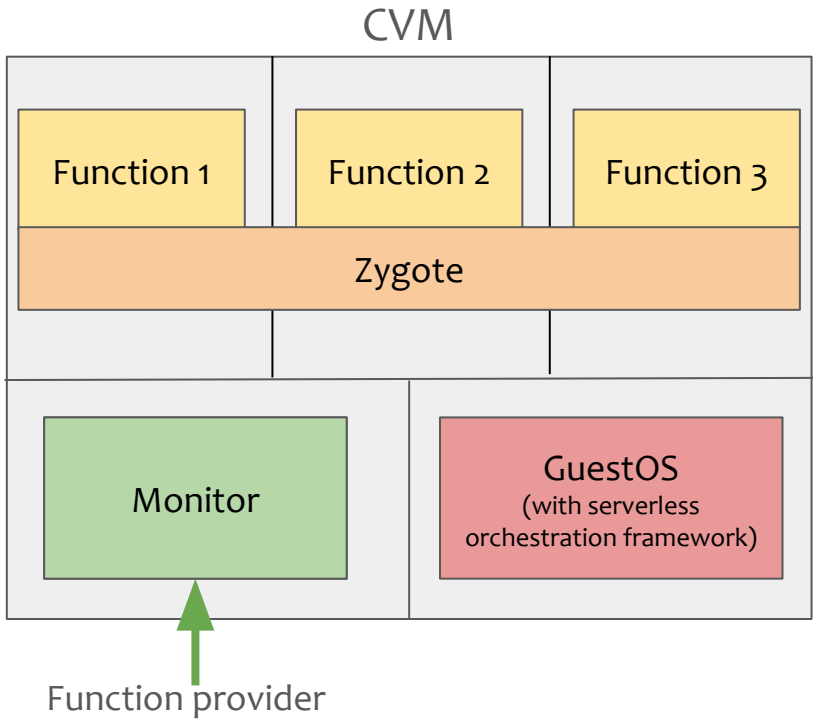
Design: Performance

- Startup overhead
  - Copy-on-write & pre-initialized template processes (Zygotes)
  - Incremental attestation
  - Local attestation with Policies
- Function chaining
  - Through shared memory channels



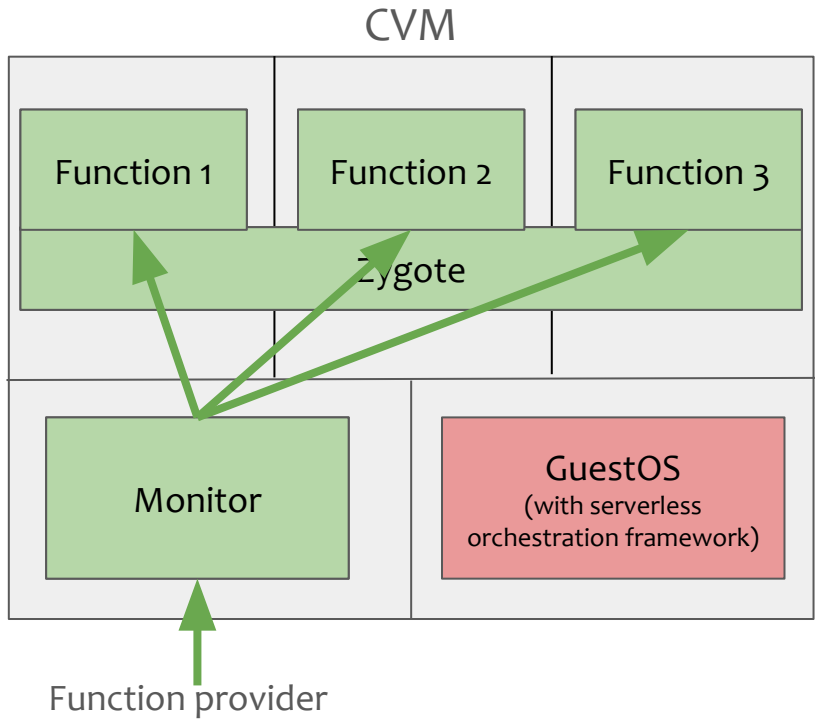
Design: Performance

- Startup overhead
  - Copy-on-write & pre-initialized template processes (Zygotes)
  - Incremental attestation
  - Local attestation with Policies
- Function chaining
  - Through shared memory channels



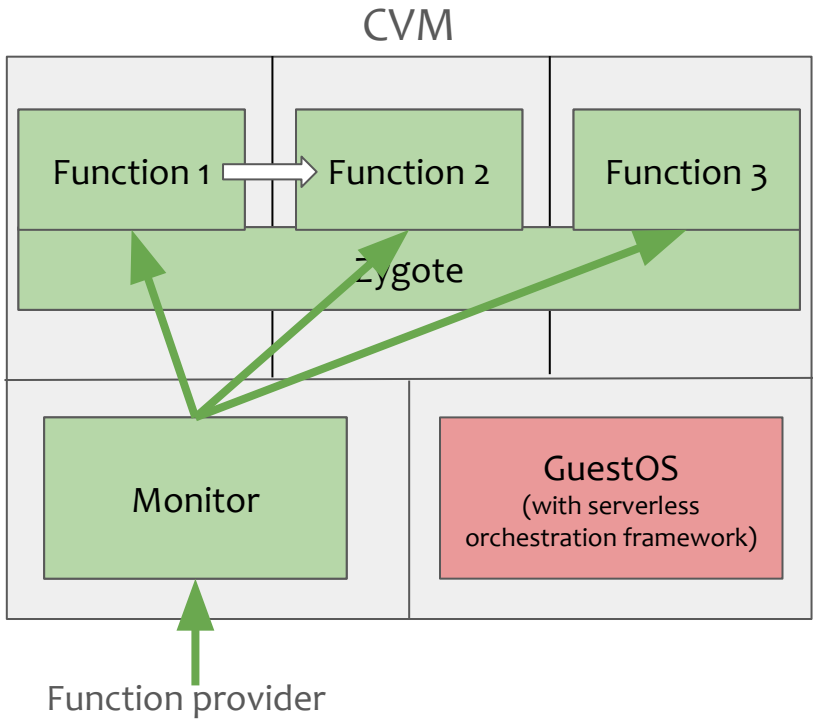
Design: Performance

- Startup overhead
  - Copy-on-write & pre-initialized template processes (Zygotes)
  - Incremental attestation
  - Local attestation with Policies
- Function chaining
  - Through shared memory channels



Design: Performance

- Startup overhead
  - Copy-on-write & pre-initialized template processes (Zygotes)
  - Incremental attestation
  - Local attestation with Policies
- Function chaining
  - Through shared memory channels



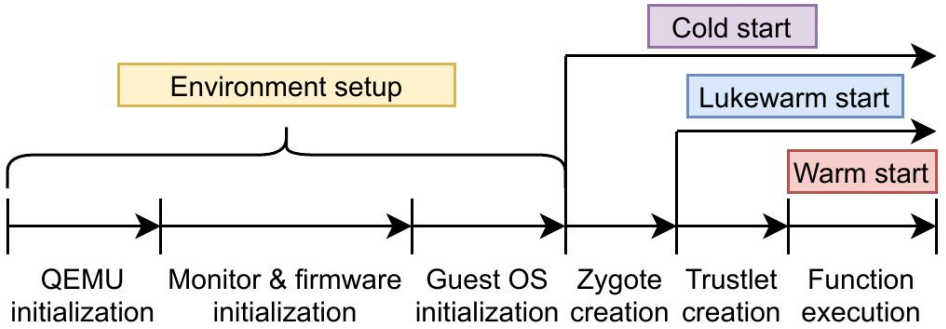
Implementation: Workflow

- System setup
  - Packaging functions (Gramine LibOS, system libraries, runtime, dependencies, function code)
  - Launching the CloakVM Monitor
  - Remote attestation and configuring the Policy
- Function execution
  - Making a request
  - Loading & verifying the Zygotes and Trustlets
  - Executing Trustlets
  - Returning the result

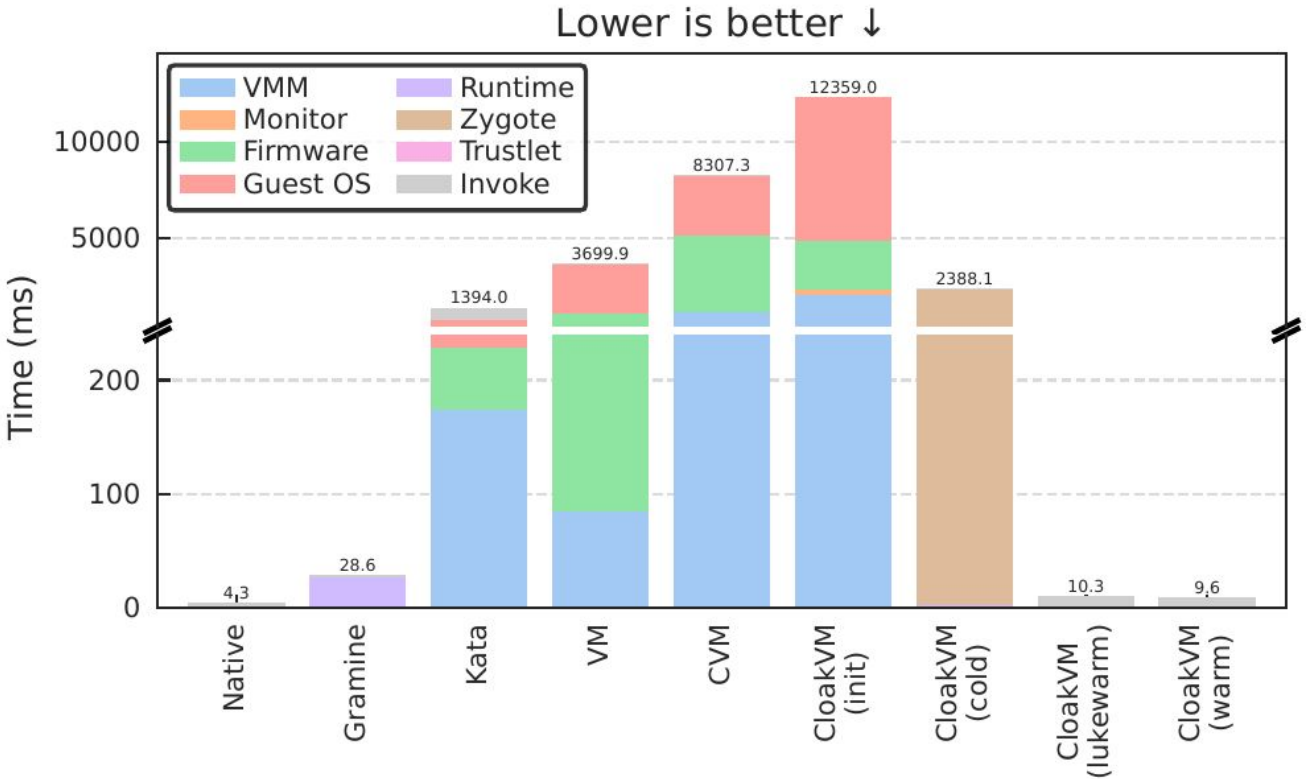
Evaluation

Comparison between:

- Native
- Gramine
- Kata Containers
- Virtual machine
- Confidential virtual machine
- CloakVM
  - Cold start
  - Lukewarm start
  - Warm start

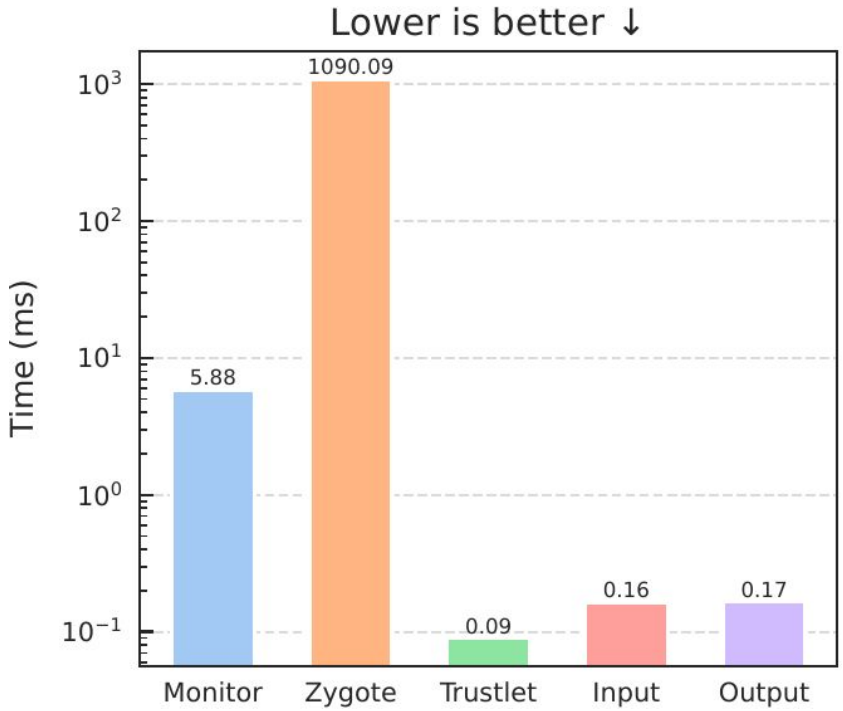


Evaluation: Startup Time



CloakVM warm and lukewarm starts are very fast;
approach Native speed

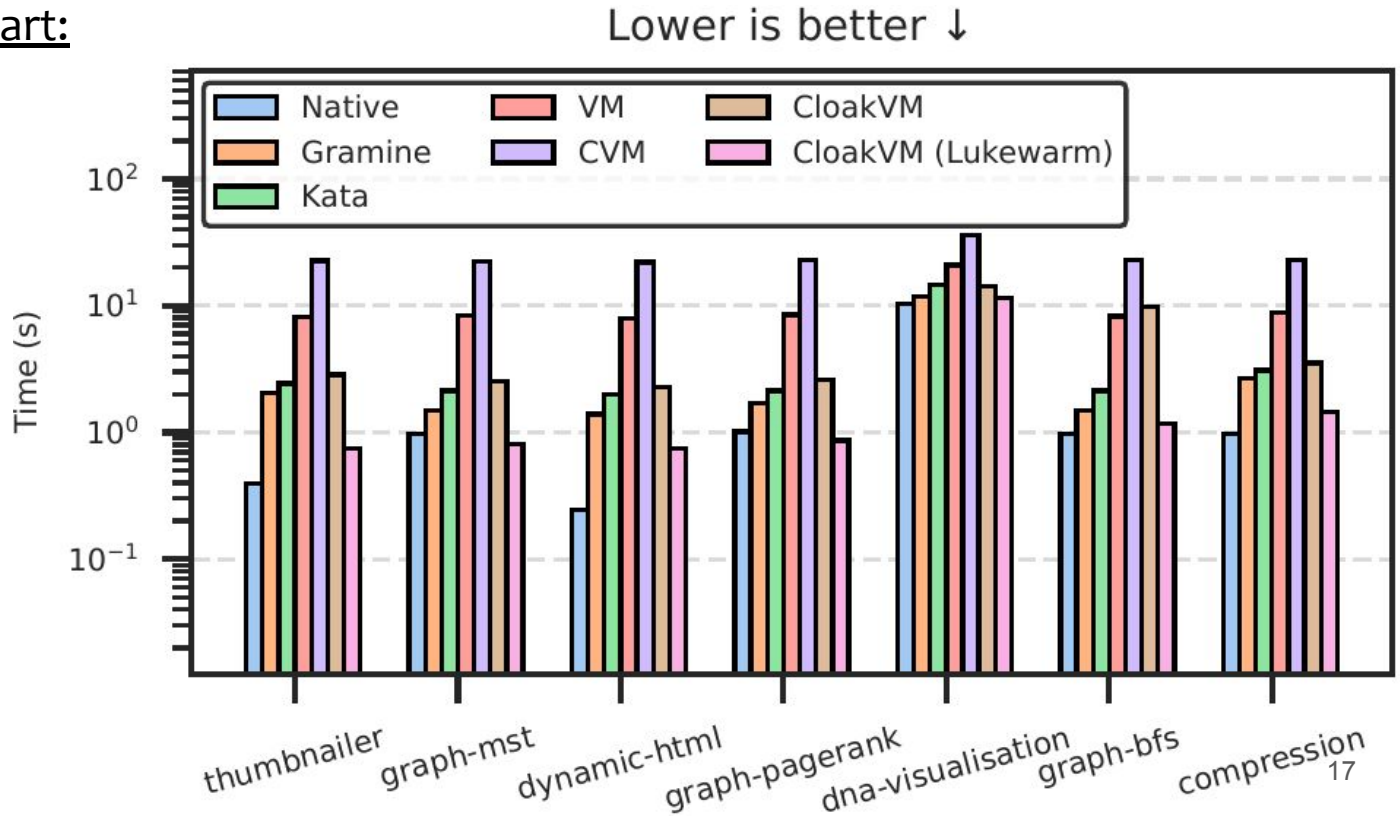
Evaluation: Measurement Cost



CloakVM's incremental attestation is very effective for large Zygotes

Evaluation: Application-level Benchmarks (end-to-end latency)

Cold and lukewarm start:

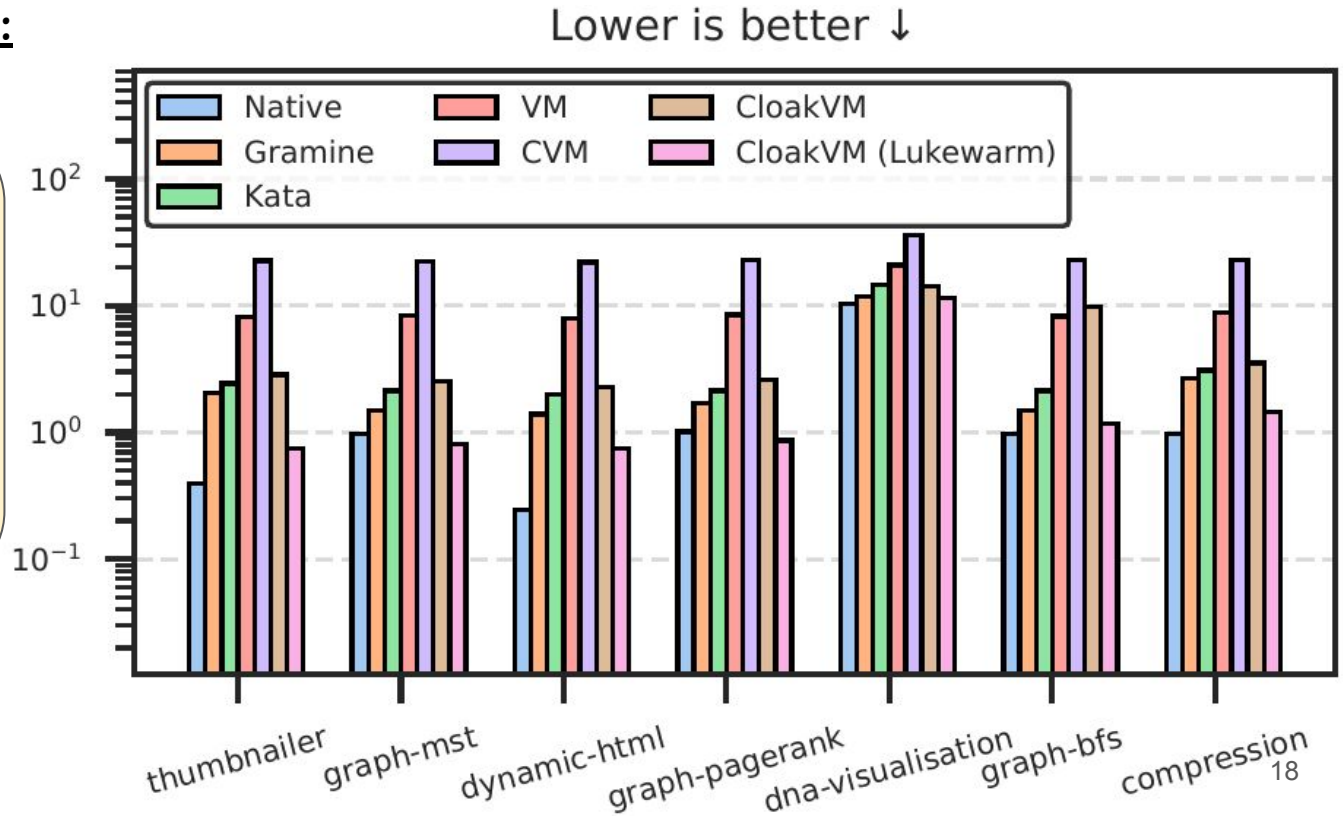


Evaluation: Application-level Benchmarks (end-to-end latency)

Cold and lukewarm start:

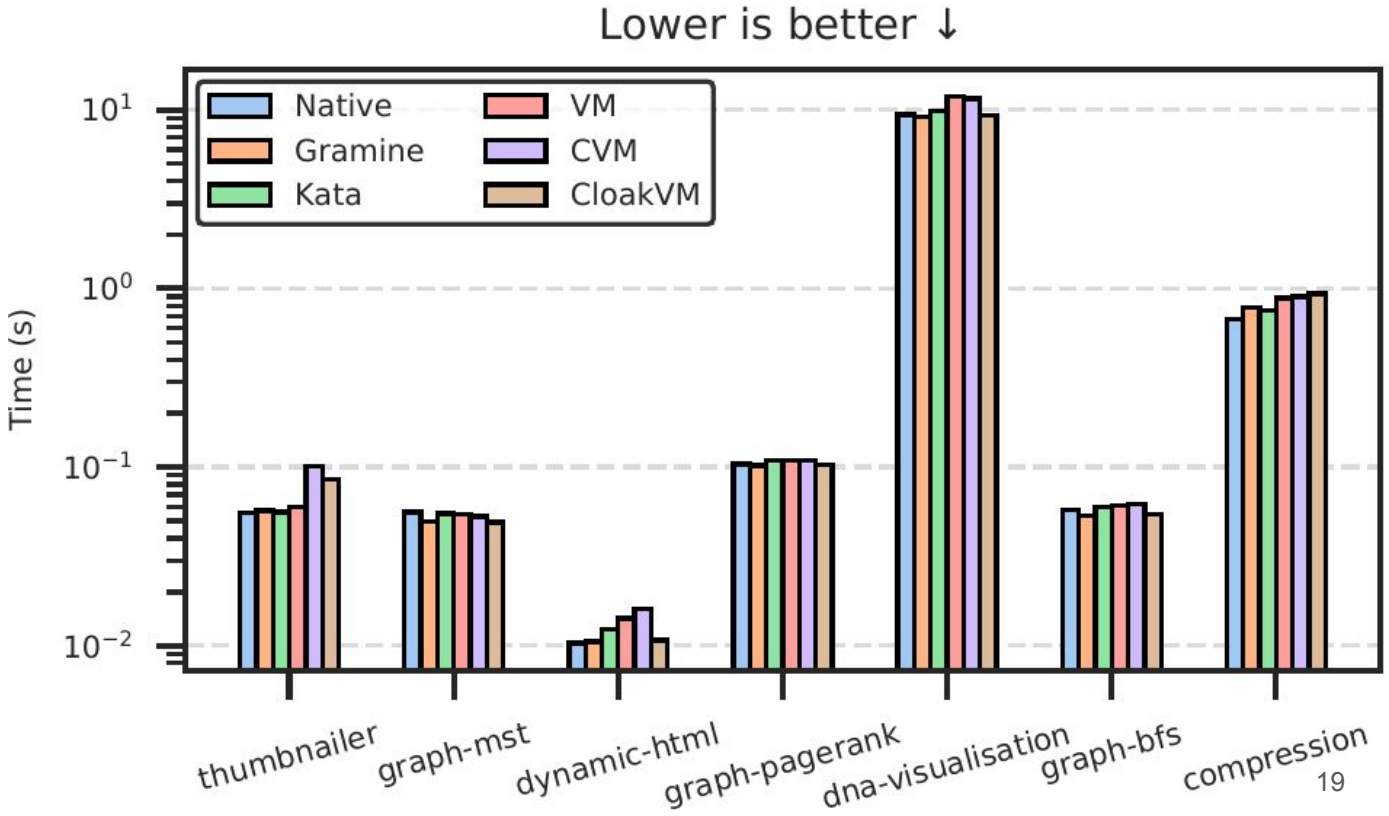
Faster than CVMs:
83 % for cold starts,
94 % for lukewarm starts

Slower than native:
318 % for cold starts,
35 % for lukewarm starts
on average



Evaluation: Application-level Benchmarks (end-to-end latency)

Warm start:

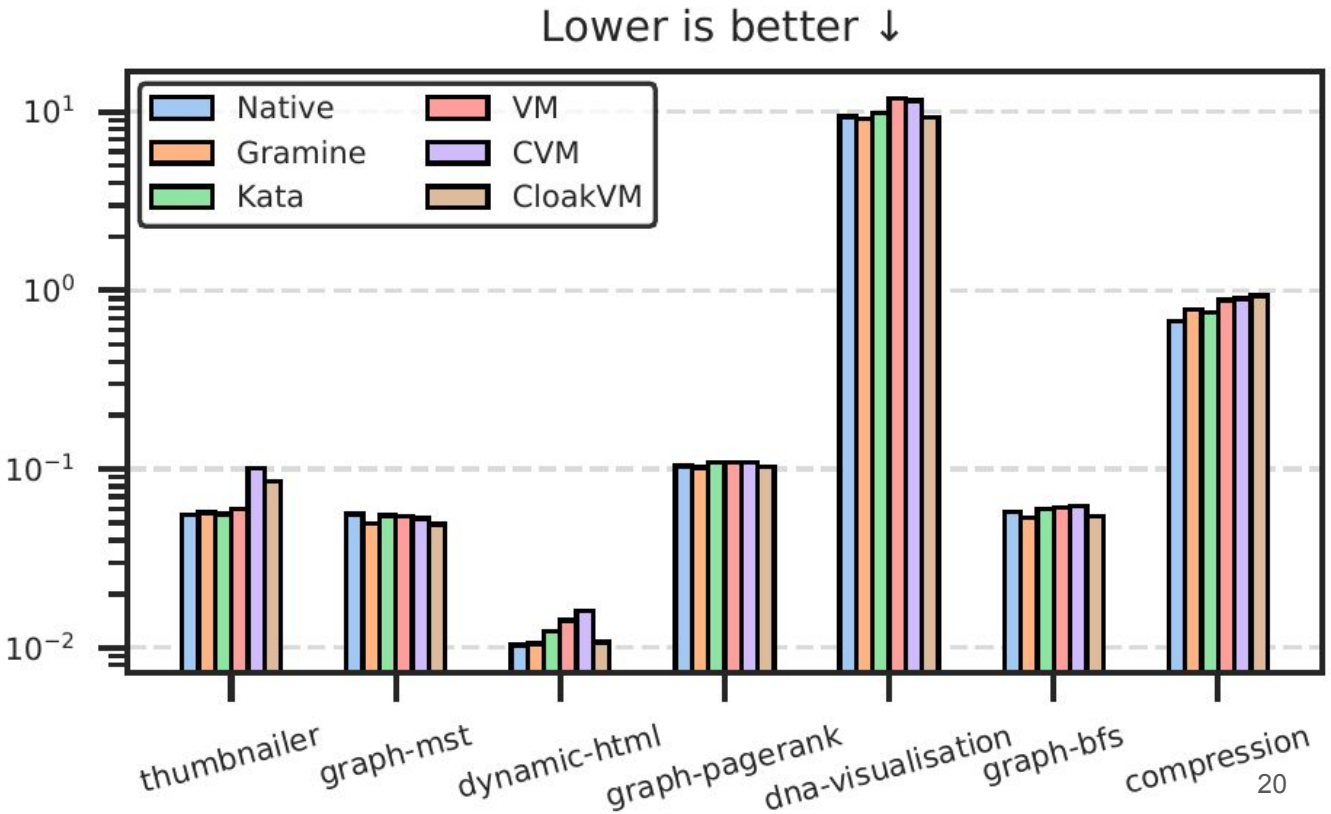


Evaluation: Application-level Benchmarks (end-to-end latency)

Warm start:

Faster than CVMs:
13 % for warm starts

Slower than native:
9 % for warm starts
on average



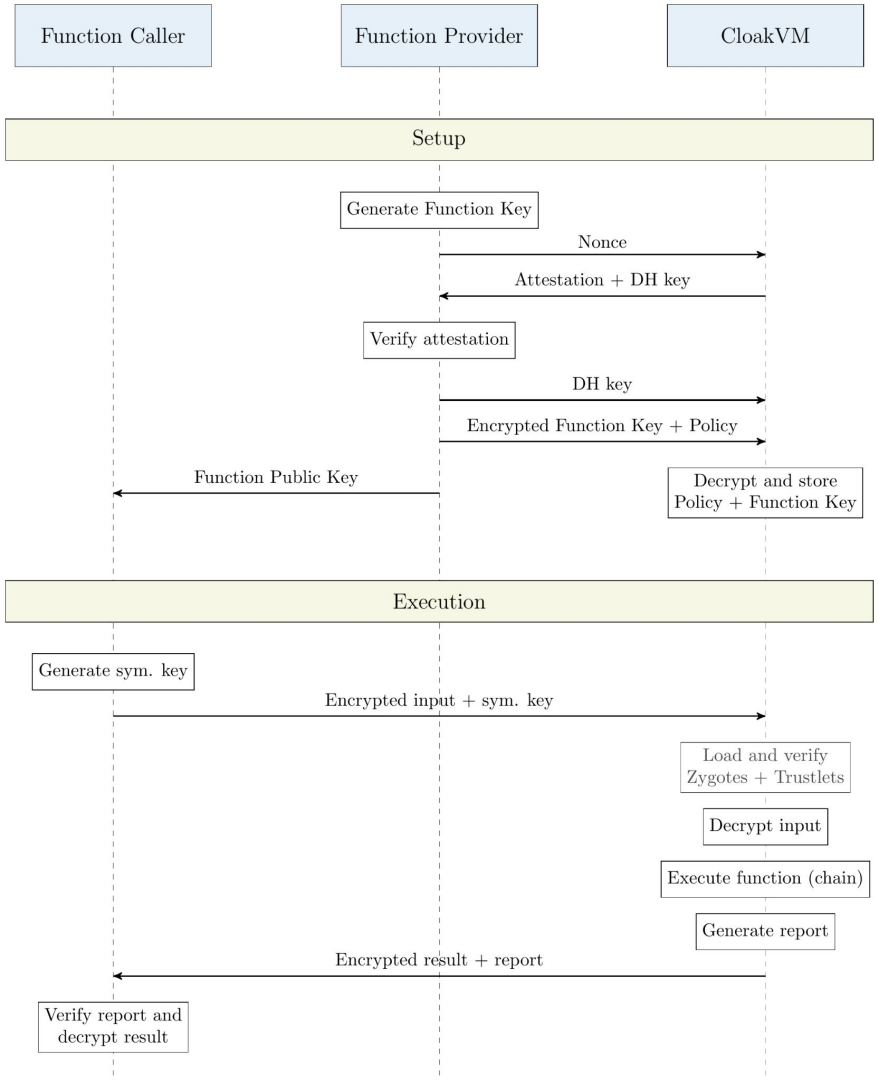
Summary

CloakVM runs confidential serverless functions with

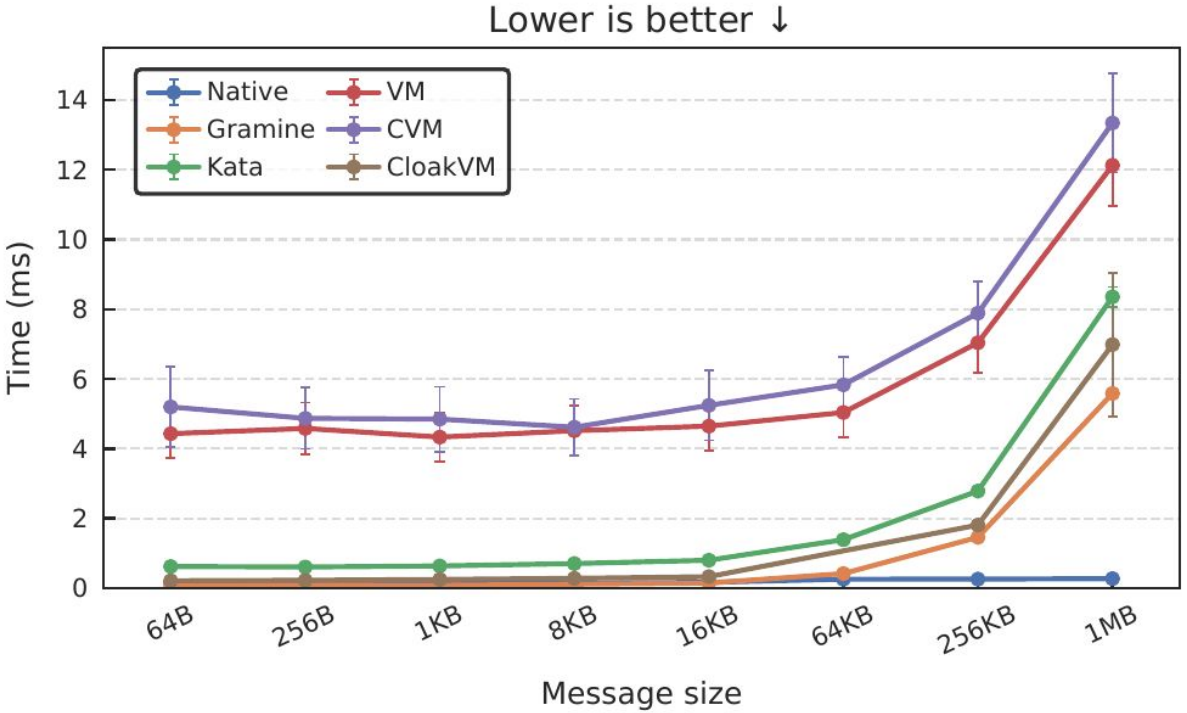
- strong security
  - small TCB
  - attestation
  - isolation
- high performance
  - fast function startup
  - fast chaining

Backup

Sequence Diagram



Evaluation: Communication Cost



CloakVM's shared memory channels are significantly faster than VM/CVM network communication