# Secure Big Data Processing with Apache Spark + SGX

**Imperial College London**
**LSDS resarch group**

Christian Priebe, Luke Granger-Brown, Dan O'Keeffe,Pierre-Louis Aublin, Florian Kelbert, Josh Lind, Divya Muthukumaran, Peter Pietzuch

Imperial College London

LSDS
Large-Scale Distributed Systems Group

SecureCloud
Secure Big Data Processing in Untrusted Clouds

# Motivation

- SecureCloud = Secure Big Data Processing in Untrusted Clouds

- Idea

  → Run big data processing tasks inside TEE

  → Apache Spark + SGX

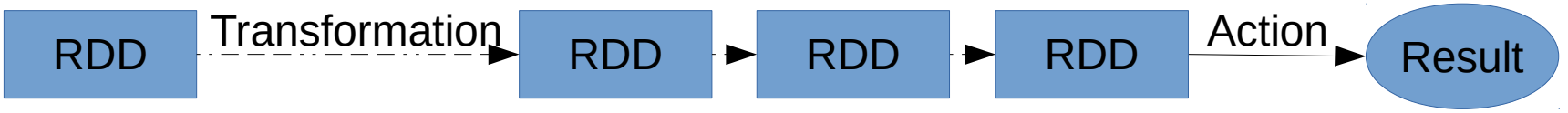
# Apache Spark

- Cluster-computing framework
- Data parallelism and fault tolerance

- Addresses limitations of MapReduce

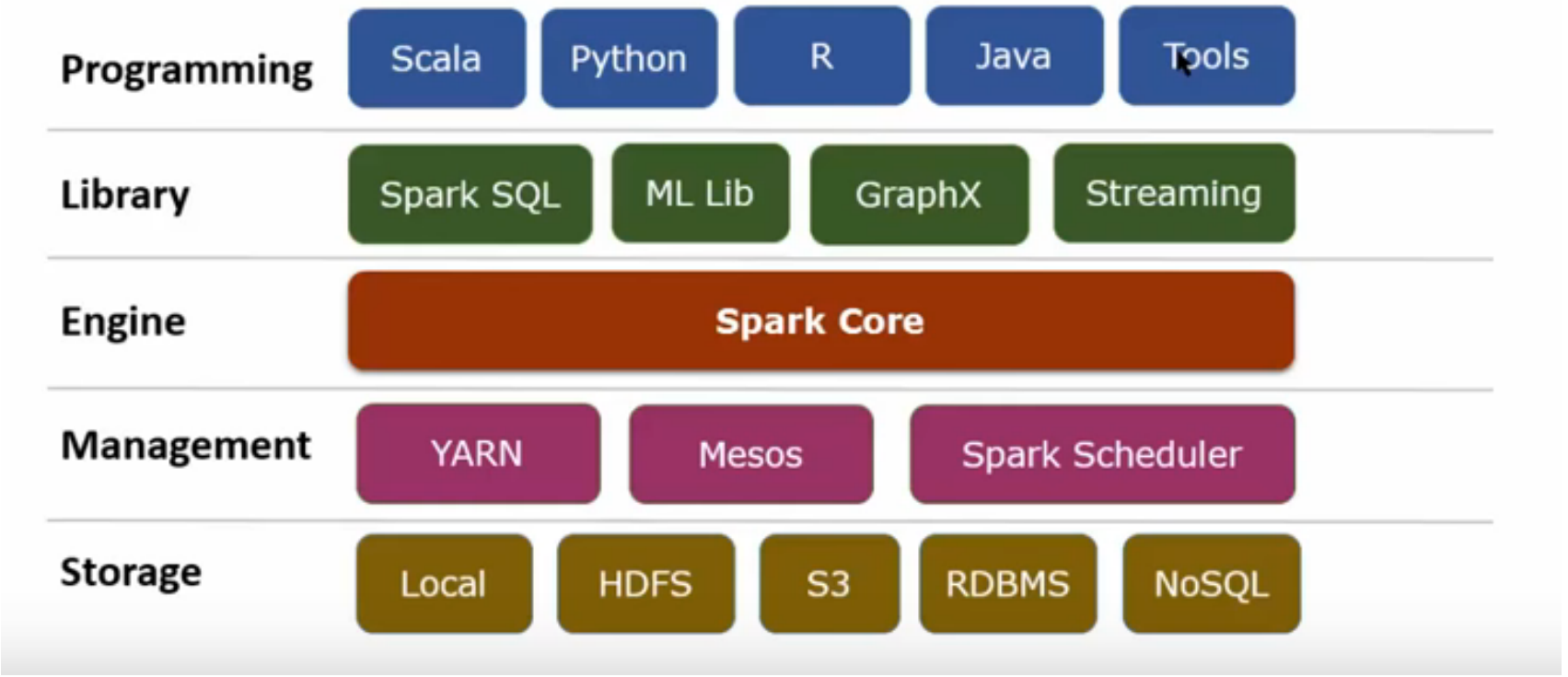
# Apache Spark

- Provides API on the basis of RDD (resilient distributed dataset) data structure
  - RDD = collection of objects
    - Split up and transformed on different nodes in parallel

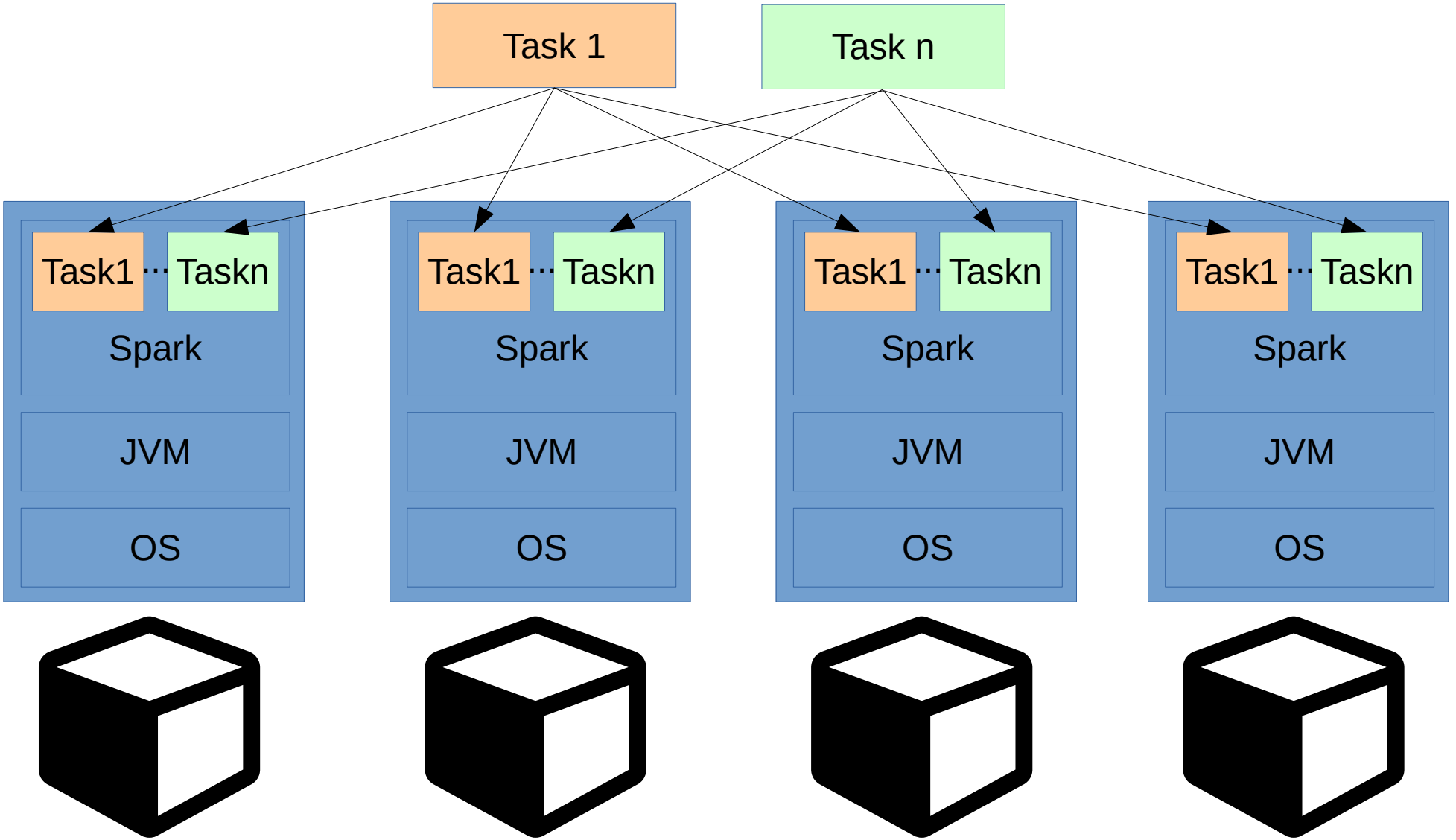



  - Example transformations
    - filter, map, union, intersection
  - Example actions
    - count, first, take

# Apache Spark



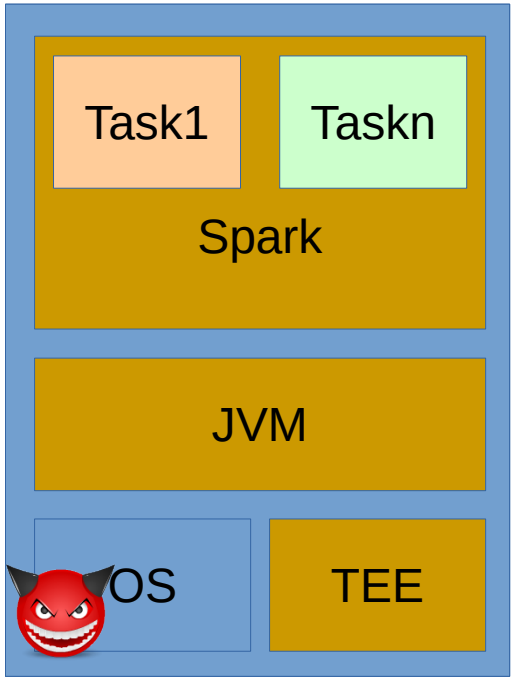
# Apache Spark System Model



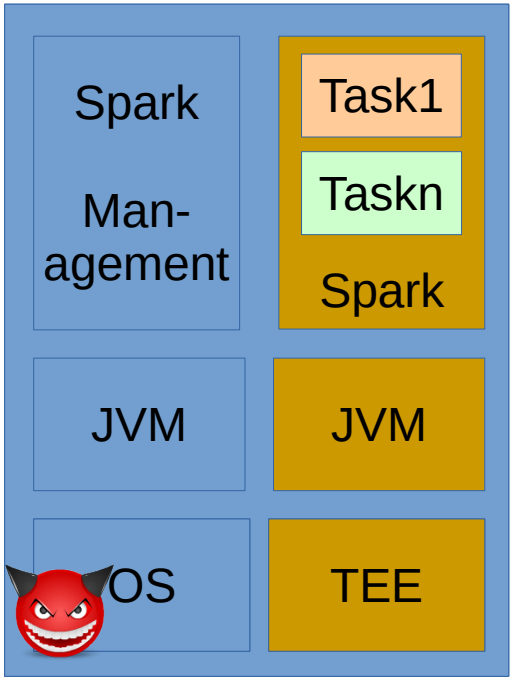
# Our Idea

- Protect task execution using SGX
  - Integrity and confidentiality of tasks and input/output data

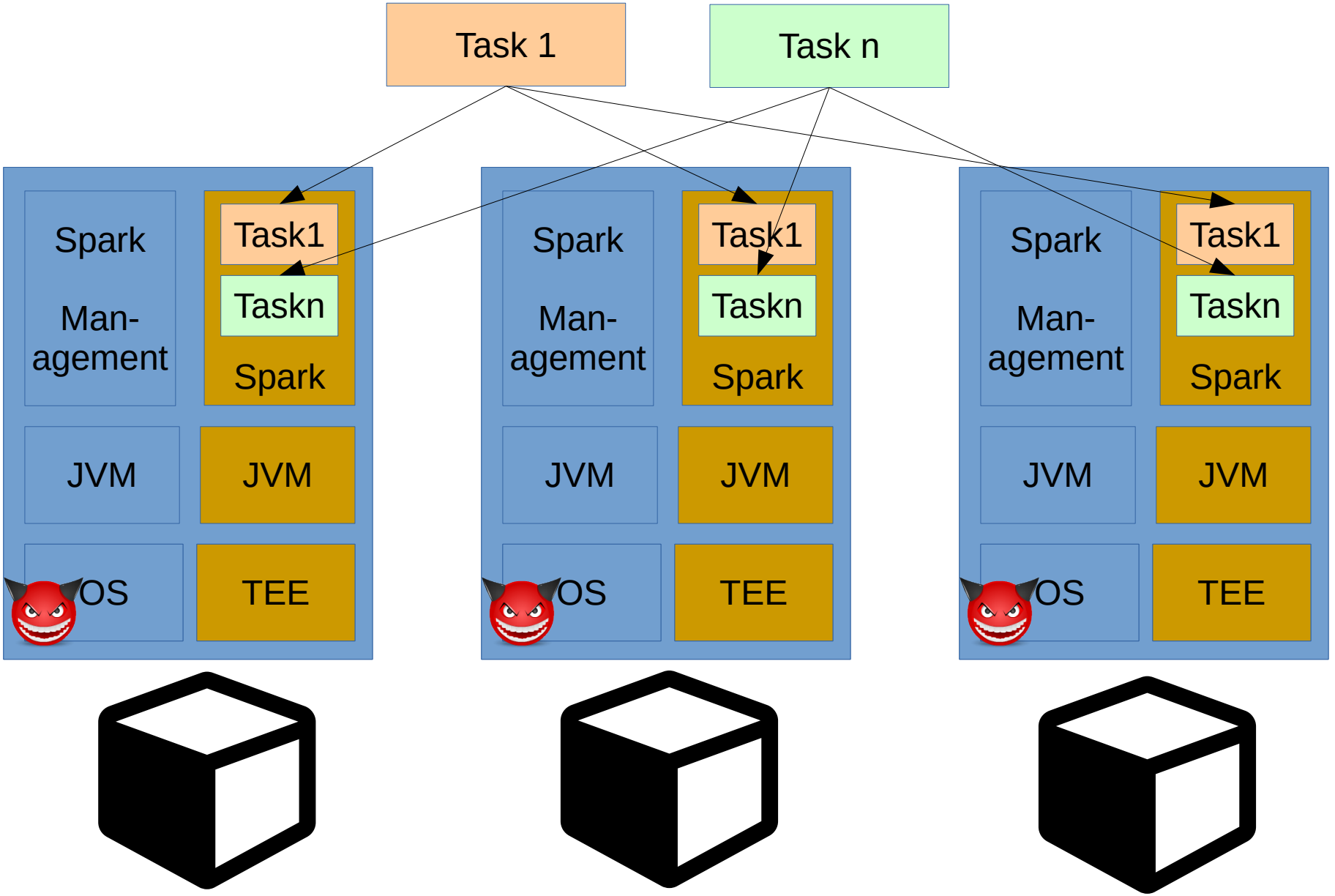
→ Run (parts of) Spark/JVM inside SGX TEE



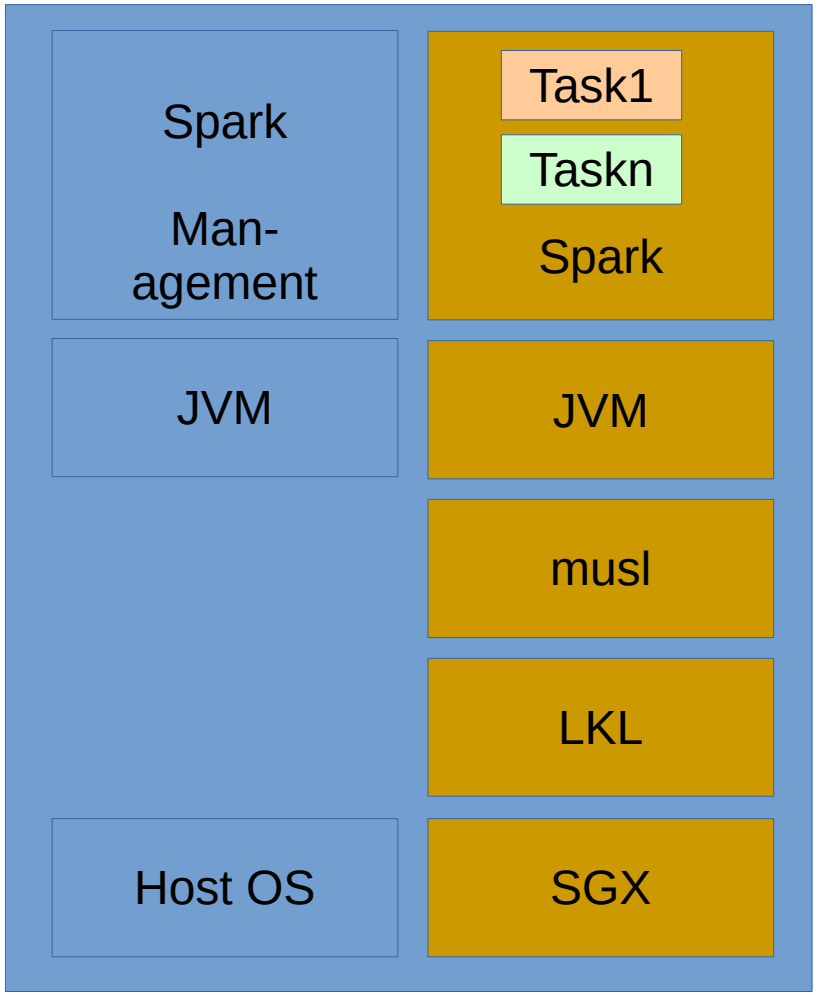

or



# Our Idea


Task 1
Task n
Spark
Man-
agement
Task1
Taskn
Spark
JVM
JVM
OS
TEE
Spark
Man-
agement
Task1
Taskn
Spark
JVM
JVM
OS
TEE
Spark
Man-
agement
Task1
Taskn
Spark
JVM
JVM
OS
TEE

# Our Solution




- Use of LKL and musl
  - LKL (Linux Kernel Library) Kernel code compiled into linkable library
  - musl: libc implementation
- Port LKL and musl to SGX
- Link JVM against LKL/musl
- Run JVM/LKL/musl within SGX
- Load Spark code and tasks into the SGX-protected JVM

# Current Status

```
# MUSL_TAP=tap0 MUSL_HD=${PWD}/miniroot/alpine-rootfs.img MUSL_KERNEL=0 MUSL_VERSION=1 MUSL_ESLEEP=1
MUSL_SSLEEP=4000 MUSL_ESPINS=50000 MUSL_SSPINS=500 MUSL_STHREADS=32 MUSL_ETHREADS=4  obj/sgx-lkl-starter
/usr/bin/java -XX:InitialCodeCacheSize=2000k -XX:ReservedCodeCacheSize=2000K -Xms8000k -Xmx8000k
-XX:MaxPermSize=4000k -XX:CompileThreshold=2000 -XX:+PrintCompilation -Xss228k -classpath /home
HelloWorld
MUSL_ETHREADS: 4
MUSL_STHREADS: 32
MUSL_SLOTS: 256
MUSL_SIGPIPE: 0
MUSL_MMAP32BIT: 0
MUSL_RTPRIO: 0
MUSL_ESPINS: 50000
MUSL_ESLEEP: 1
MUSL_SSPINS: 500
MUSL_SSLEEP: 4000
MUSL_KERNEL: 0
MUSL_HEAP: 83591168
Musl build parameters:
1.1.15Maximum enclave threads (TCS): 8
OpenJDK 64-Bit Server VM warning: Can't detect initial thread stack location - find_vma failed
    202    1 %           java.lang.String::hashCode @ 24 (55 bytes)
    204    2             java.lang.String::indexOf (70 bytes)
    221    3             java.lang.String::hashCode (55 bytes)
Hello world.
```

# Open Challenges / Ideas

- Limited EPC size
  - Deactivate parts of JVM
  - Support only some features of Spark
  - Execute only parts of JVM/Spark inside SGX
- Security considerations
  - Communication between nodes
  - Confidentiality/integrity of data
  - Secure task/data provisioning