

# Securing Data While in Use with Azure Confidential Compute

---



**Reza Salehi**

CLOUD CONSULTANT

@zaalion [linkedin.com/in/rezasalehi2008](https://www.linkedin.com/in/rezasalehi2008)



# Overview



**Securing data, in transit, at rest, and while in use**

**Understanding confidential computing**

- Trusted Execution Environments (TEEs), Enclaves
- TEE types (hardware and software backed)

**A few confidential compute use cases**

**Introducing Azure Confidential Compute**

- DC-series virtual machine

**Demo: Working with Azure Confidential Compute using Open Enclave SDK**



# Securing Data

## In transit

SSL/TLS

## At rest

Always Encrypted,  
Storage Service  
Encryption

## In use (processing)

How to protect code  
and data while being  
processed in memory?



# High Privileged, Unauthorized Entities



OS administrators



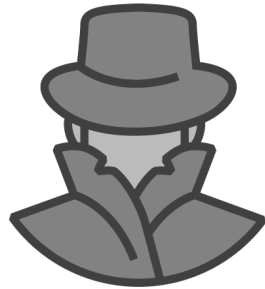
DB administrators



Business partners



Third-party  
contractors

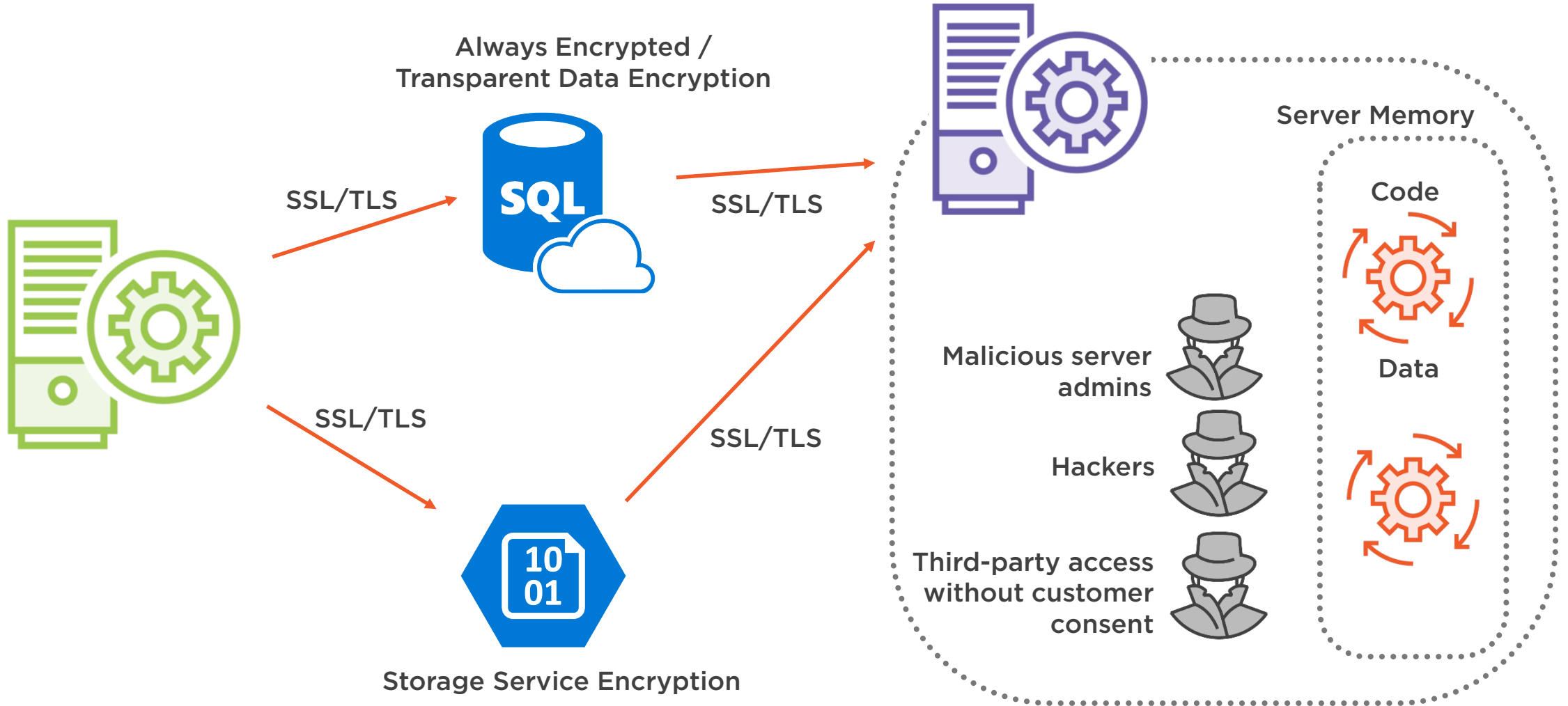


Hackers

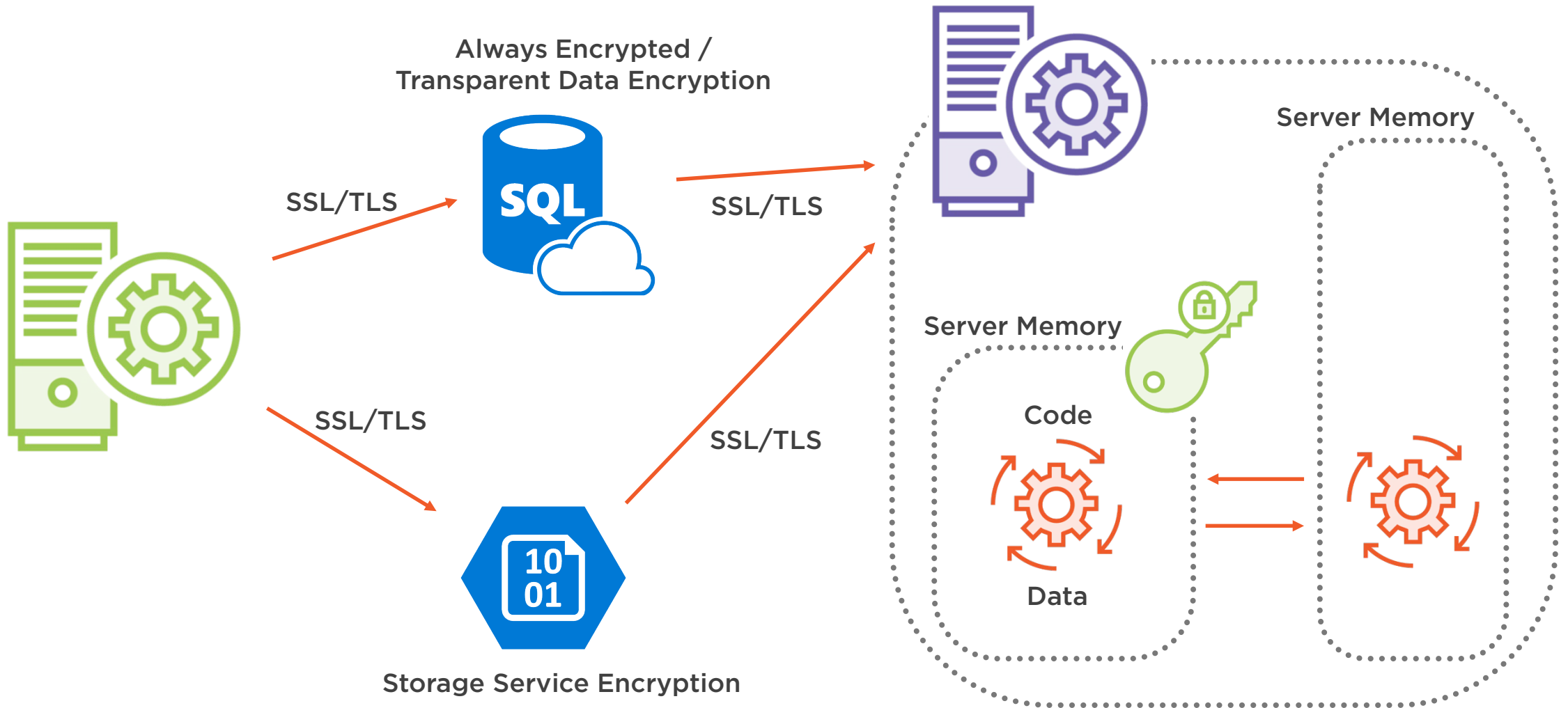


Malicious processes

# Data in Use



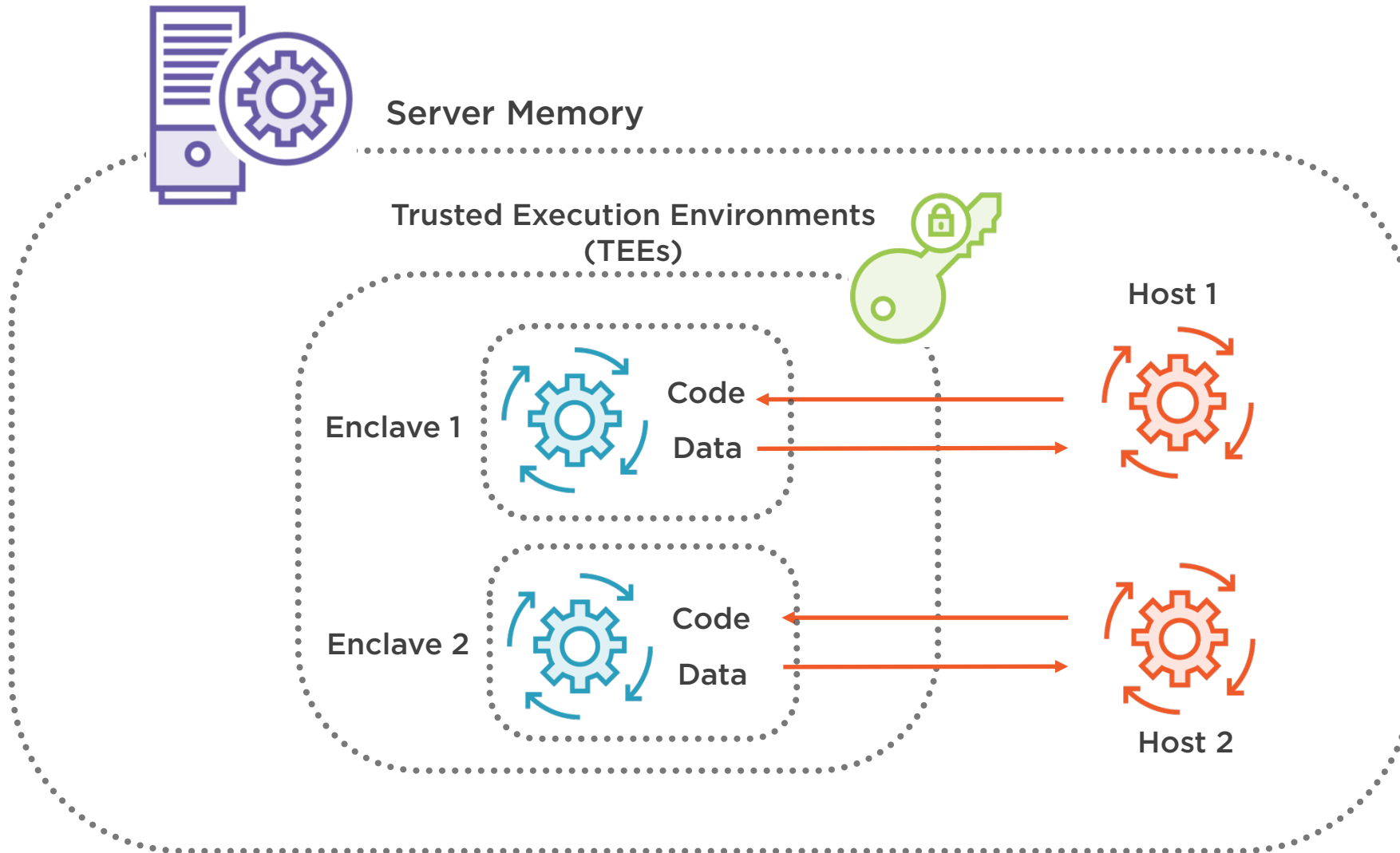
# Data in Use



Confidential computing  
protects the confidentiality  
and integrity of your data  
and code while it's  
processed, using TEEs.



# Trusted Execution Environments (TEEs)





# Enclaves



Private regions of memory are called enclaves



Their contents are protected and can not be read or saved by any process outside the enclave itself



The enclave is decrypted on the fly within the CPU, only the code and data running from within the enclave can use it



# Using Enclaves in Code

## Enclave SDK

A common cross-platform API consistent across TEEs, so that confidential application is portable

## Attestation

Verifying identity of code running in TEEs to establish trust with that code and release protected data to it



# TEE Types

## Hardware-backed

Virtual machines/servers that run on Intel Software Guard Extensions (SGX) technology (e.g. Azure DC-series)

## Software-backed

Virtualization-based security (VBS) is a software-based TEE implemented by Hyper-V in Windows 10/Server 2016



# Azure Confidential Computing

Thanks to a partnership with Intel, Azure can offer hardware-protected virtual machines that run on Intel Software Guard Extensions (SGX) technology.



# Azure Confidential Computing Use Cases

**Always Encrypted**  
*with secure  
enclaves*

Allows computations on  
plaintext data

**Multi-party Machine  
Learning**

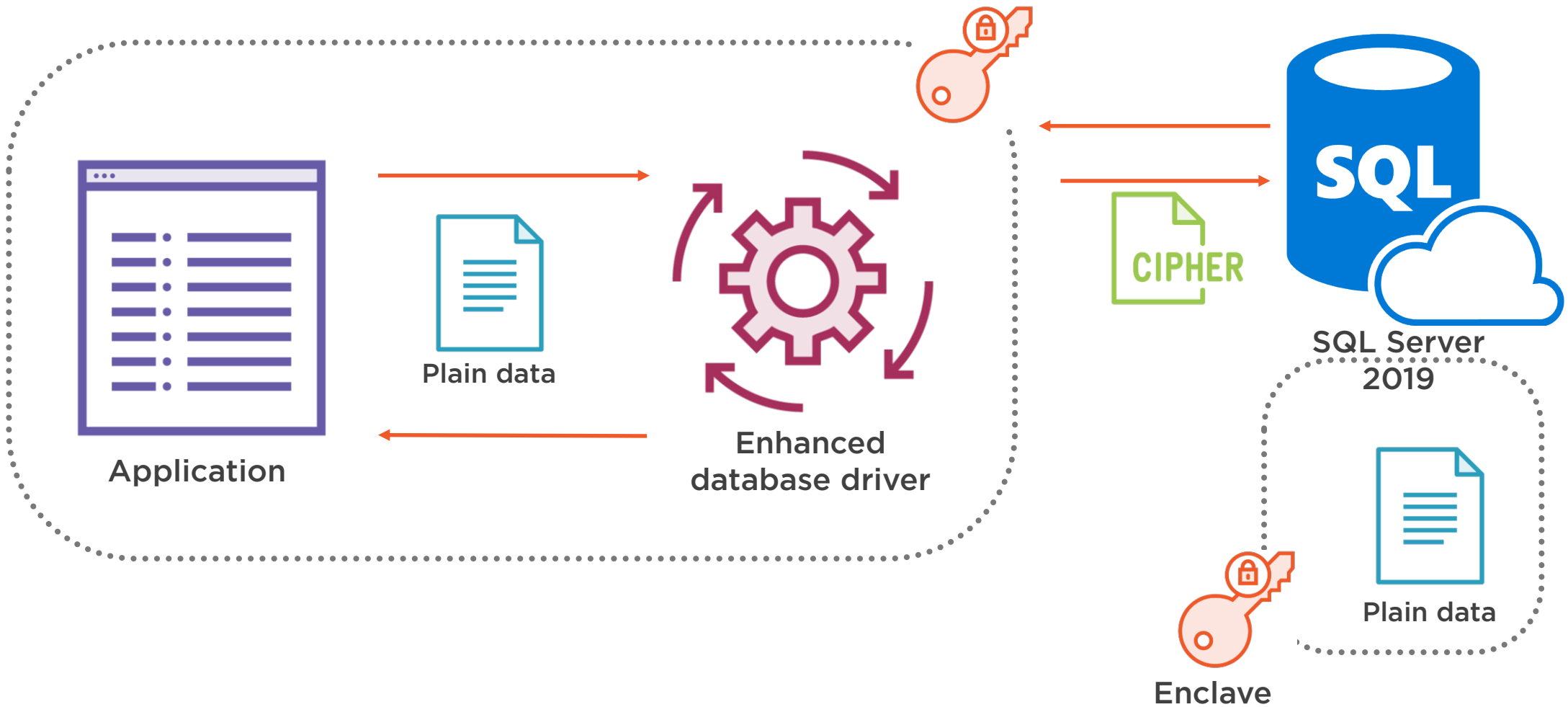
Confidential data from  
multiple parties to  
better train a ML  
algorithm

**Custom  
Applications**

Using available SDKs  
such as Open Enclave  
SDK by *Microsoft*



# Always Encrypted with Secure Enclaves



# Always Encrypted with Secure Enclaves



The only operations SQL Server (prior to 2019) could perform on encrypted data were equality comparisons



Users needed to move the data outside of the database to perform these operations on the client-side



"Always Encrypted with secure enclaves" allows computations on plaintext data inside a secure enclave on the server side



# Always Encrypted with Secure Enclaves



So far, it is offered for SQL Server 2019, using the software-backed enclaves (VSM)



Azure SQL Database will support this feature later, planned to use hardware-backed enclaves (SGX)

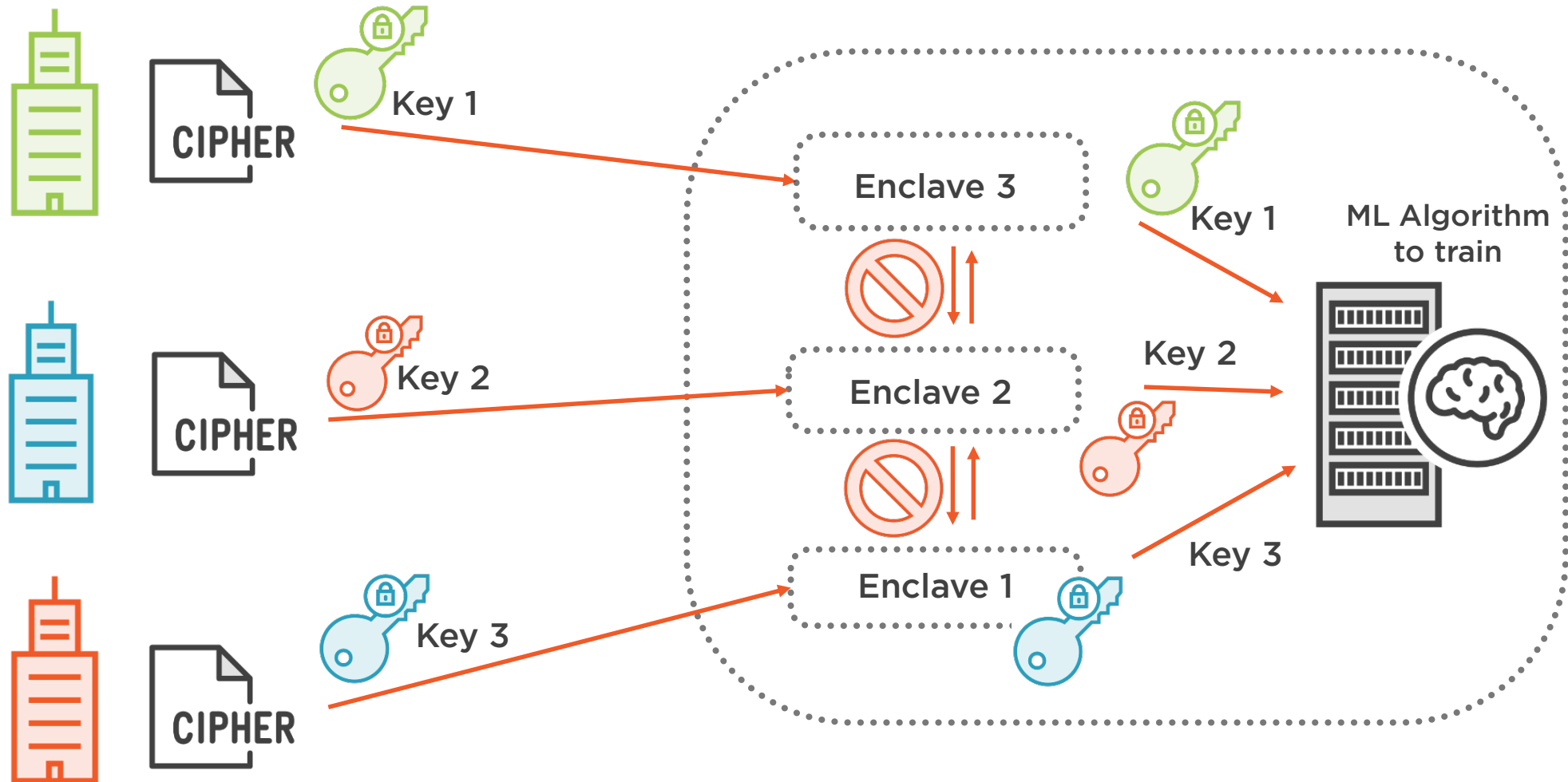


SQL Server delegates rich query processing to the enclave (pattern matching, range comparison, etc.)





# Multi-party Machine Learning



# Multi-party Machine Learning



Individual hospitals establish trust in their TEE and send their encrypted data in



Multi-hospital data is shared with the machine learning service that has access to all individual enclaves



Having more data to train on, allows machine learning algorithms to produce better models



# Develop Custom Applications Using Open Enclave SDK



Open Enclave SDK is an enclaving abstraction for developer to build Trusted Execution Environment (TEEs) based applications



Supports C, C++ on top of Linux. Updates for Windows and other run-times will follow



Supports Intel SGX. Microsoft is working with other hardware vendors (e.g. AMD) to incorporate their implementation



A single application will be divided into 2 sections: the host (not trusted) and enclave (trusted)



# Demo



## Provision a DC-series VM

- Ubuntu Linux

## Working with Open Enclave SDK

- Review a sample C++ code
- Build and run the code within an enclave



# Summary



**Securing data while in use**

**Understanding confidential computing**

- Trusted Execution Environments (TEEs), Enclaves, hardware and software backed TEEs

**Confidential compute use cases**

- Always Encrypted, Multi-party machine learning

**Introduced Azure Confidential Compute**

- DC-series virtual machine

**Demo: Worked with Azure Confidential Compute and Open Enclave SDK**

