SOLUTION BRIEF

SafeLiShare: Bringing Security to Dataflows

Data Vulnerability

Today, data is most vulnerable when it is accessed and processed by applications. Data itself cannot differentiate between safe or unsafe applications; all applications that present acceptable credentials are granted access.

Vulnerabilities may manifest themselves in multiple ways:

1 Compromised or erroneous new versions of applications may damage data or act maliciously.

2 If the account credentials are compromised, data may be accessed by unauthorized and unknown applications.

3 If the machine or infrastructure where the data is being processed is compromised, an application may access the contents of memory where data resides while being processed.

Data vulnerability is further increased when applications run in network domains not under control of the data owner such as in cloud contexts where the data owner does not control physical access to the network or computer processing the data.

Furthermore, an application's intellectual property (IP) is vulnerable when an application runs in a network not controlled by the application owner.

SafeLiShare Solution

SafeLiShare uses secure enclaves based on confidential computing technology to manage data and application vulnerabilities by introducing **Policy Driven Access to Applications and Data** (PDAAD).

With PDAAD technology:

1. Data and applications remain encrypted whenever protection is required.

2. Data is only accessible inside a secure enclave.

3. Only pre-identified applications running in secure enclaves may be allowed to access data.

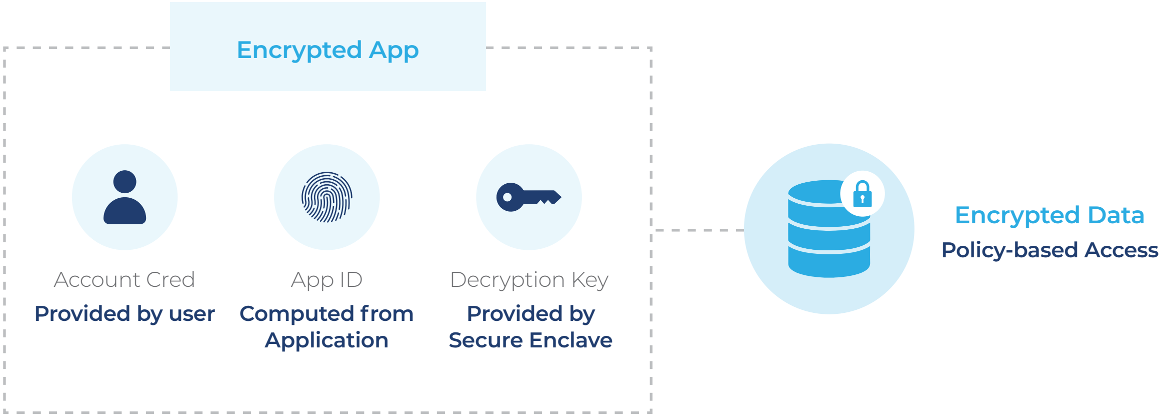
4. The keys to decrypt data are only available inside a secure enclave.

5. The decryption keys provided to an application running inside a secure enclave are protected by the confidential computing hardware that created the secure enclave, hence the secure enclave is the only and single source of trust.

6. An application running in a secure enclave may be assigned a unique and unforgeable identity.

7. Any application accessing data from inside a secure enclave is auditable such that its unique identity is available and verifiable through audit logs.

8. Data and applications have designated ownership; usage of data or application is only allowed by its owner, or someone granted permission by the owner.



Benefits of Policy Driven Access to Applications and Data (PDAAD)

Security:
Data is only made accessible within a secure enclave and always remains encrypted when outside a secure enclave.

Trackability:
All access by applications is logged and available for audit.

Accessibility:
Only pre-identified applications may access the data.

Auditability:
All accesses are verifiable using audit logs.

Compliance:
Privacy regulations satisfied by proving that all data entering and exiting secure enclaves was encrypted.

Usability:
Data and applications are usable within and across data domains and organizational boundaries.

How SafeLiShare Uses Confidential Computing

Confidential computing technology allows the creation of run-time environments, called secure enclaves, that assign encrypted memory space to user applications. Confidential computing hardware protects the keys used to decrypt the encrypted memory space assigned to applications.

An application running in a secure enclave is isolated because no other application can access its decrypted memory space. Data being processed by an application running in a secure enclave, and the code of the application, is protected from other applications that may be running on the same computer.

SafeLiShare uses computer programs, called policy servers, running in secure enclaves to generate encryption keys that may be used by data and application owners to encrypt their data and applications. The corresponding decryption keys are only made available by the policy server to applications inside a secure enclave.

Before providing a data decryption key to an application, the secure enclave (in which the application is running), is required to “attest” itself to the satisfaction of the policy server. Attestation services are provided by the hardware manufacturer and, more recently, by infrastructure providers.

SafeLiShare allows encrypted data and encrypted applications to be “stitched” together and presented for execution inside a secure enclave. The execution needs keys for decrypting the application and the data from the policy server which are only provided if the respective identities of the application (and account credentials of the data and application owners) are verifiable.

The identities and credentials involved in the execution are recorded in logs that are generated by a known logging process that itself runs in a secure enclave.