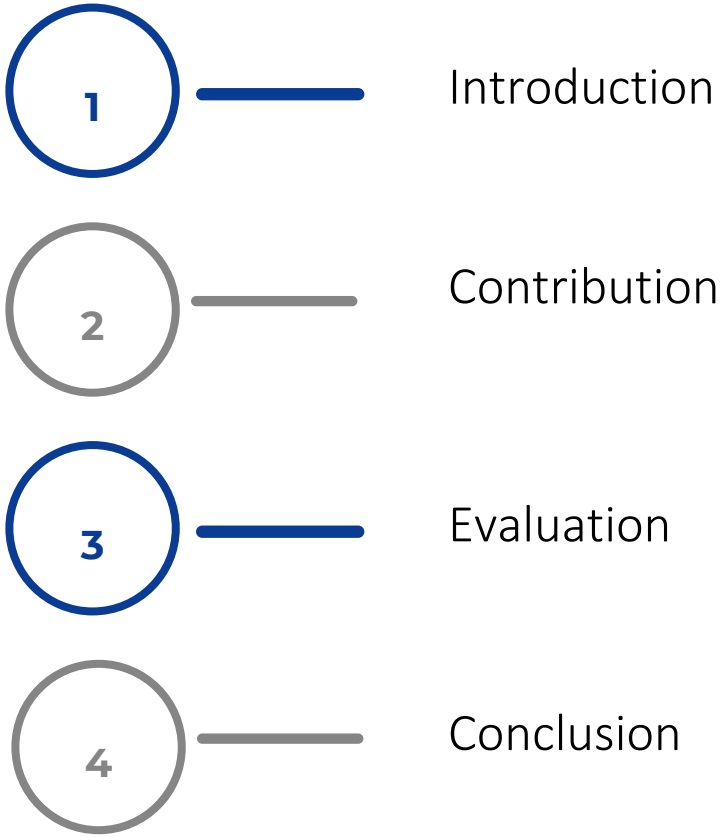
MOHAMMED VI POLYTECHNIC UNIVERSITY | College of Computing

Decentralized SGX-based Cloud Key Management

Yunusa Simpa Abdulsalam, **Jaouhara Bouamama**, Yahya Benkaouz, and Mustapha Hedabou

NSS 2023: 17th International Conference on Network and System Security

Outline

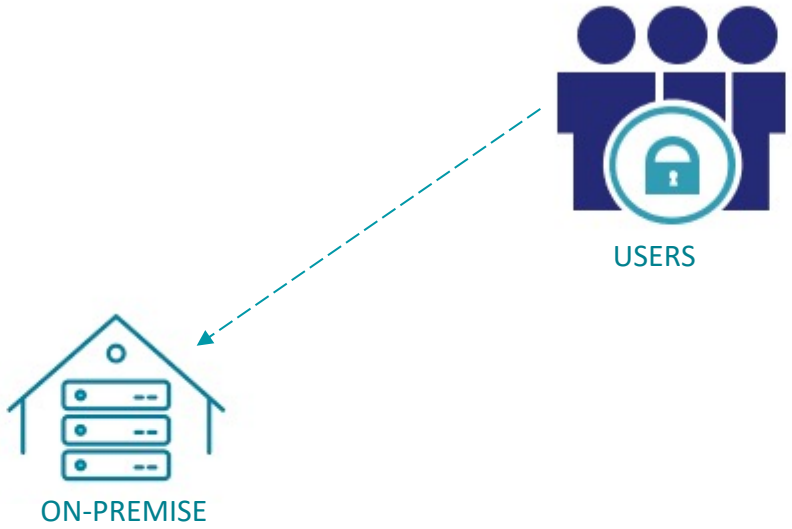


Introduction

- Sensitive data has resided on local servers where encryption keys were required to secure this data.

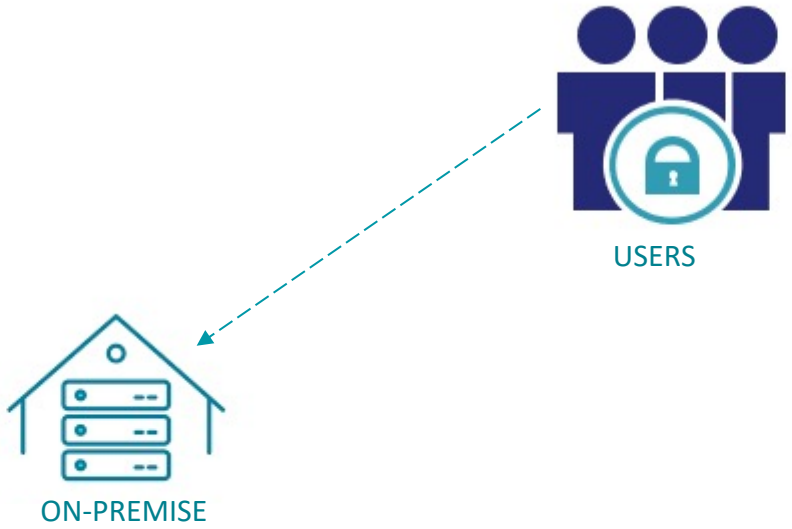
Introduction

- Sensitive data has resided on local servers where encryption keys were required to secure this data.



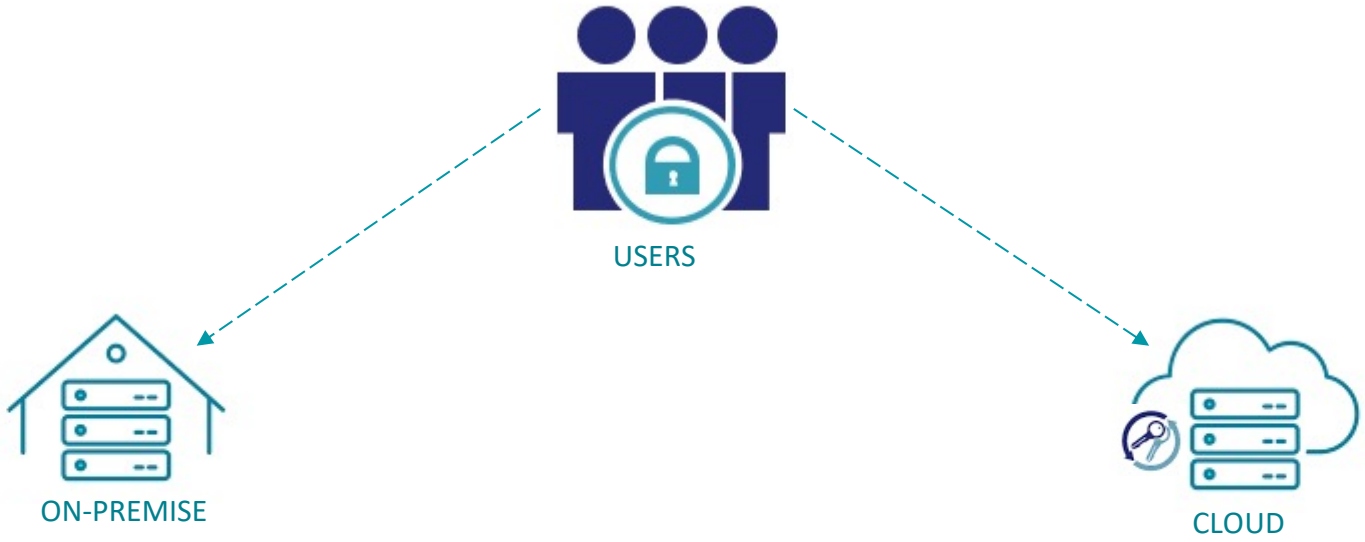
Introduction

- Sensitive data has resided on local servers where encryption keys were required to secure this data.
- To improve the scalability and availability of applications, enterprises are now moving Infrastructure and applications to the cloud



Introduction

- Sensitive data has resided on local servers where encryption keys were required to secure this data.
- To improve the scalability and availability of applications, enterprises are now moving Infrastructure and applications to the cloud



Introduction

businesswire
A BERKSHIRE HATHAWAY COMPANY

HOME SERVICES NEWS EDUCATION ABOUT US

Search

Report Finds 90% of IT Professionals Have Experienced a Cybersecurity Breach

Global research from Skyhigh Security spotlights cloud data security challenges across key industries, indicating the need for stronger security controls

April 10, 2023 08:00 AM Eastern Daylight Time

SAN JOSE, Calif.--(BUSINESS WIRE)--Skyhigh Security today released *The Data Dilemma: Cloud Adoption and Risk Report*, focusing on the prevailing problem of how to protect data that is used, shared and stored in today's hybrid and cloud-first enterprise environments. The report finds that, on average, organizations store 61% of their sensitive data in the cloud, and most have experienced at least one cybersecurity breach (90%), threat (89%) and/or theft of data (80%), with three quarters (75%) experiencing all three. Overall, the report underscores the need to address data security gaps by investing in comprehensive data protection that provides remote workforces with a secure and productive user experience.

"Today, data is everywhere, traversing devices, cloud applications, the web and infrastructure, so it comes as no surprise that one of the biggest challenges organizations face is securing their vital data"

Tweet this

"Today, data is everywhere, traversing devices, cloud applications, the web and infrastructure, so it comes as no surprise that one of the biggest challenges organizations face is securing their vital data," said Rodman Ramezanian, global cloud threat lead, Skyhigh Security. "The problem is compounded by the increasing use of private and public cloud services, practices like Shadow IT and even economic factors. With so many variables, it begs the question: Are organizations trying to solve new problems with old methods? Our report findings reinforce the importance of a converged platform across data, web and cloud protection capabilities to cater for the needs of security teams today."

Cloud Security Market is Set to Grow at a CAGR of 13.9% Leading to a Revenue of US$ 144.3 Billion by 2031 | Get In-Depth Studies by Transparency Market Research

Friday, March 31, 2023 4:34 AM

Topic: Company Update Share this Article

WILMINGTON, DE / ACCESSWIRE / March 31, 2023 / Transparency Market Research Inc. - According to TMR, the global

Gartner Report: Select the Right Key Management as a Service to Mitigate Data Security and Privacy Risks in the Cloud

"According to Gartner, by 2024, the increasing impact of international data residency and privacy requirements will result in more than 40% of organizations adopting multicloud KMaaS over native cloud service provider KMaaS, up from less than 10% today."

Introduction

businesswire
A BERKSHIRE HATHAWAY COMPANY

HOME SERVICES NEWS EDUCATION ABOUT US

Search

Report Finds 90% of IT Professionals Have Experienced a Cybersecurity E

Global research from Skyhigh Security spotlights cloud da
indicating the need for stronge

April 10, 2023 08:00 AM Eastern Daylight Time

SAN JOSE, Calif.--(BUSINESS WIRE)--Skyhigh Security today released 7
focusing on the prevailing problem of how to protect data that is used, sh
enterprise environments. The report finds that, on average, organizations
have experienced at least one cybersecurity breach (90%), threat (89%) a
experiencing all three. Overall, the report underscores the need to addres
data protection that provides remote workforces with a secure and produ

"Today, data is everywhere, traversing devices, cloud applications, the web and infrastructure, so it comes as no surprise that one of the biggest challenges organizations face is securing their vital data"

Tweet this

"Today, data is eve
web and infrastruc
challenges organiz
Ramezanian, global cloud threat lead, Skyhigh Security. "The problem is compounded by the increasing use of private and public cloud services, practices like Shadow IT and even economic factors. With so many variables, it begs the question: Are organizations trying to solve new problems with old methods? Our report findings reinforce the importance of a converged platform across data, web and cloud protection capabilities to cater for the needs of security teams today."

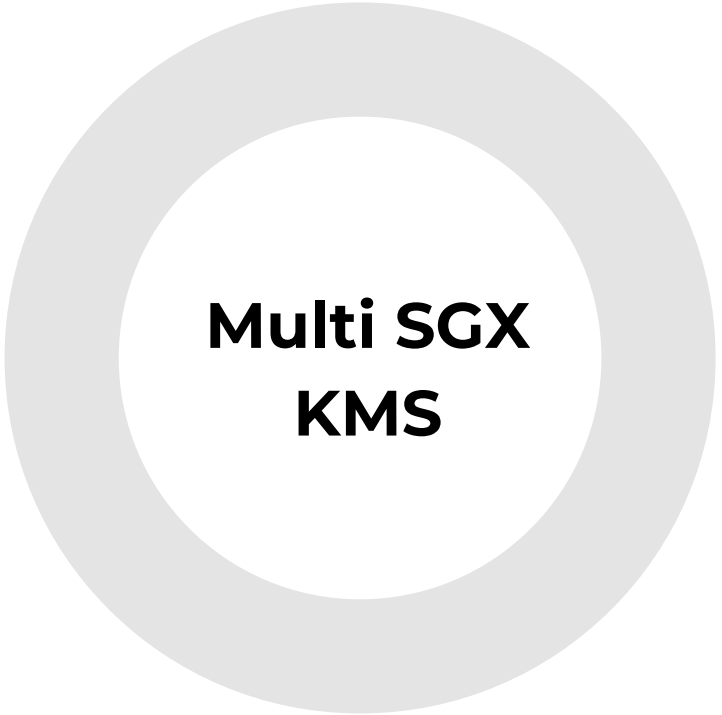
Cloud Security Market is Set to Grow at a CAGR of 13.9% Leading to a Revenue of US$ 144.3 Billion by 2031 | Get In-Depth Studies by Transparency Market Research

/ Transparency Market Research Inc. - According to TMR, the global c

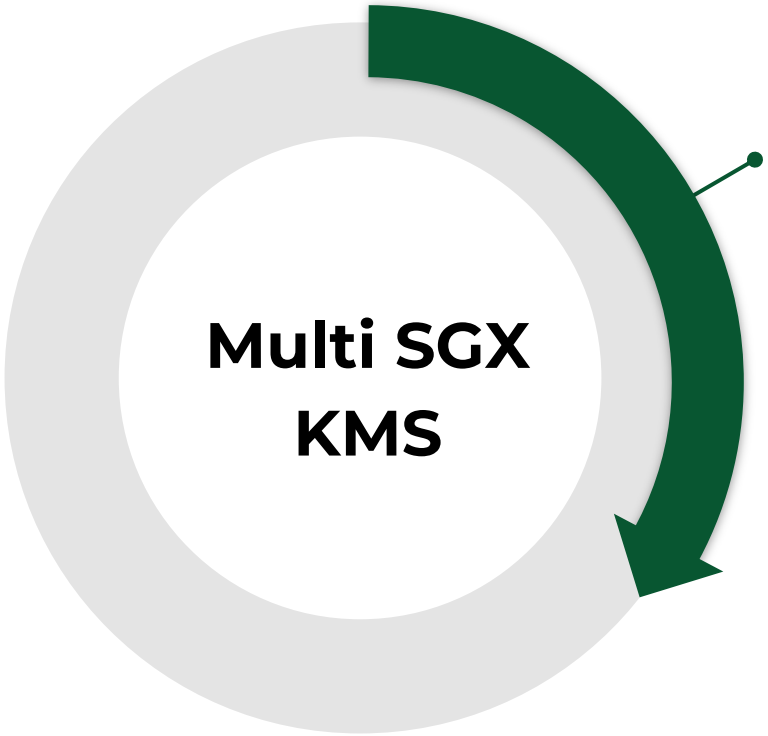
Select the Right nt as a Service to ecurity and Privacy ud

"According to Gartner, by 2024, the increasing impact of international data residency and privacy requirements will result in more than 40% of organizations adopting multicloud KMaaS over native cloud service provider KMaaS, up from less than 10% today."

Introduction

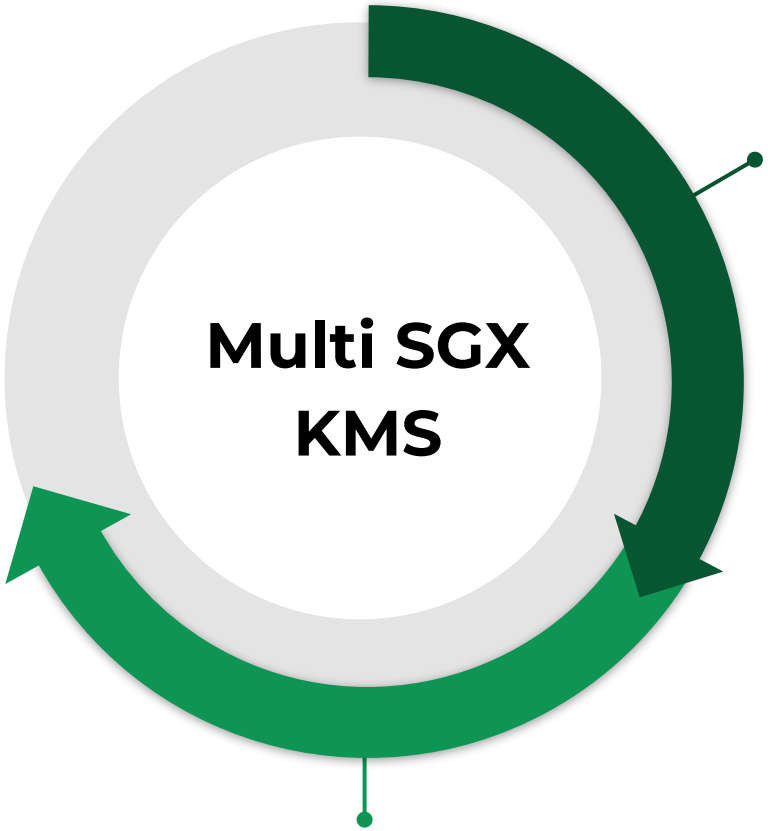


Introduction



A scalable cloud based key management system

Introduction

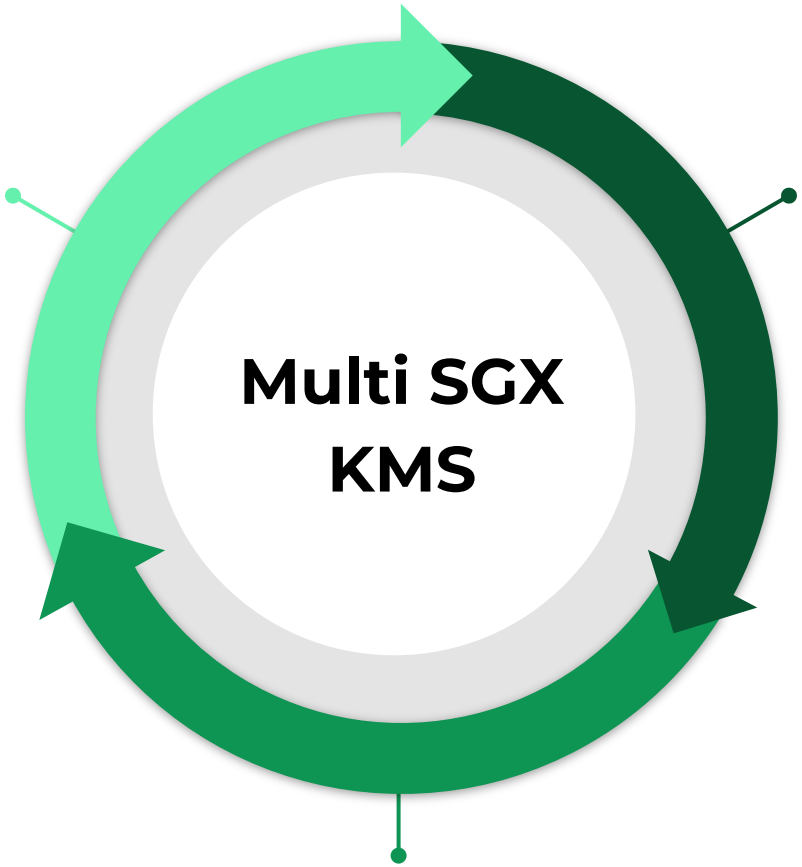


A scalable cloud based key management system

A secure scheme in the random oracle model

Introduction

Efficiency through implementation



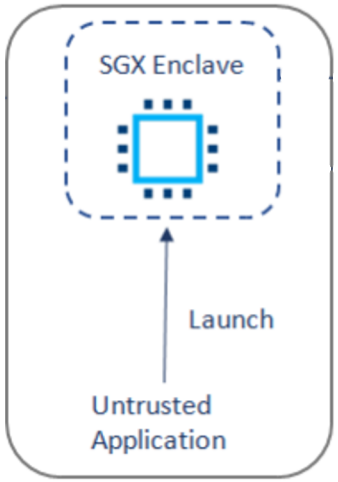
A scalable cloud based key management system

A secure scheme in the random oracle model

Literature Review

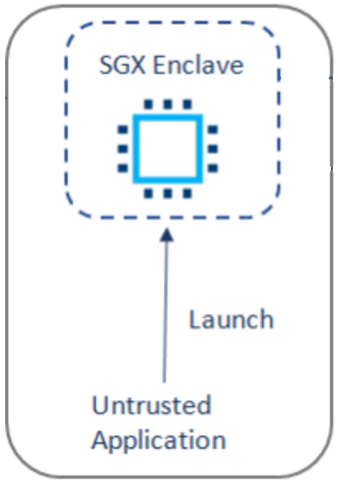
	Confidentiality	Integrity	Authentication	Single point of failure	Scalability
KMSGX	✗	✓	✓	✗	✗
EnclaveDB	✓	✓	✓	✗	✗
RansomClave	✓	✓	✓	✗	✗
MultiSGX-KMS	✓	✓	✓	✓	✓

Preliminaries



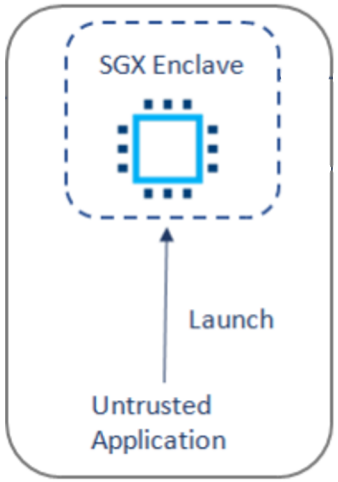
- Intel SGX is a technology that enables high-level protection of secrets against all non-authorized access.

Preliminaries



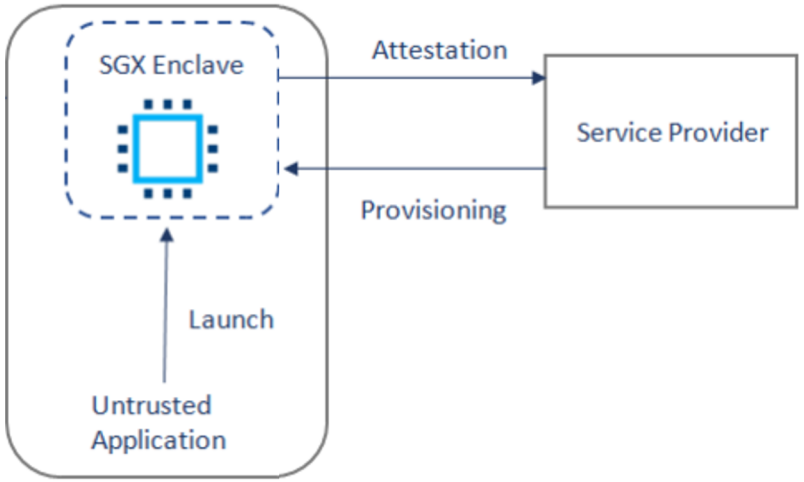
- Intel SGX is a technology that enables high-level protection of secrets against all non-authorized access.
- SGX uses enclave to allocate hardware-protected memory where data and code reside.

Preliminaries



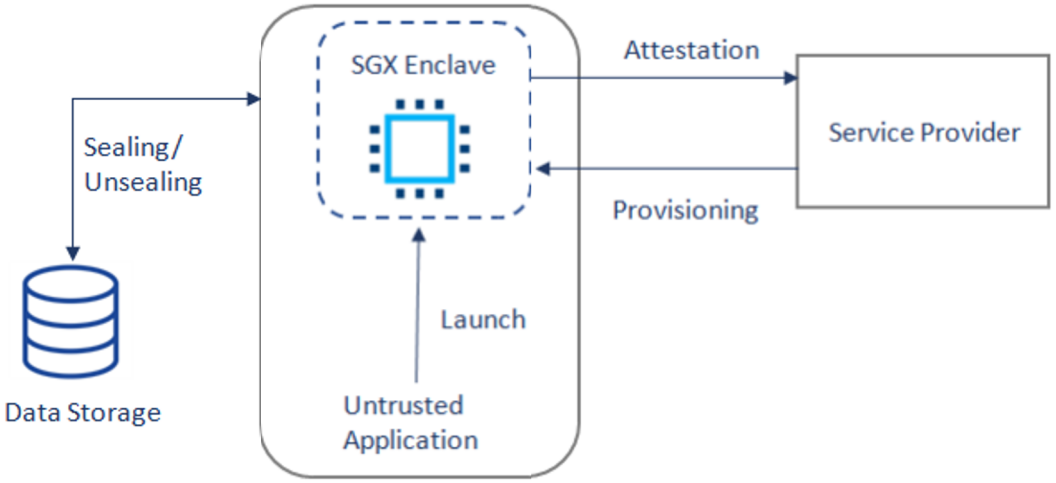
- Intel SGX is a technology that enables high-level protection of secrets against all non-authorized access.
- SGX uses enclave to allocate hardware-protected memory where data and code reside.
- Intel SGX provides dedicated attestation and sealing mechanisms to build a secure model.

Preliminaries



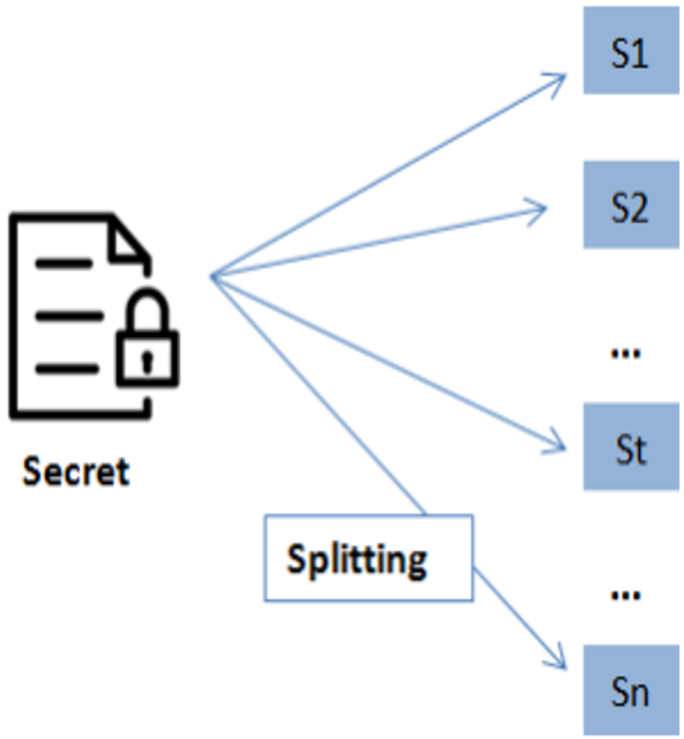
- Intel SGX is a technology that enables high-level protection of secrets against all non-authorized access.
- SGX uses enclave to allocate hardware-protected memory where data and code reside.
- Intel SGX provides dedicated attestation and sealing mechanisms to build a secure model.

Preliminaries



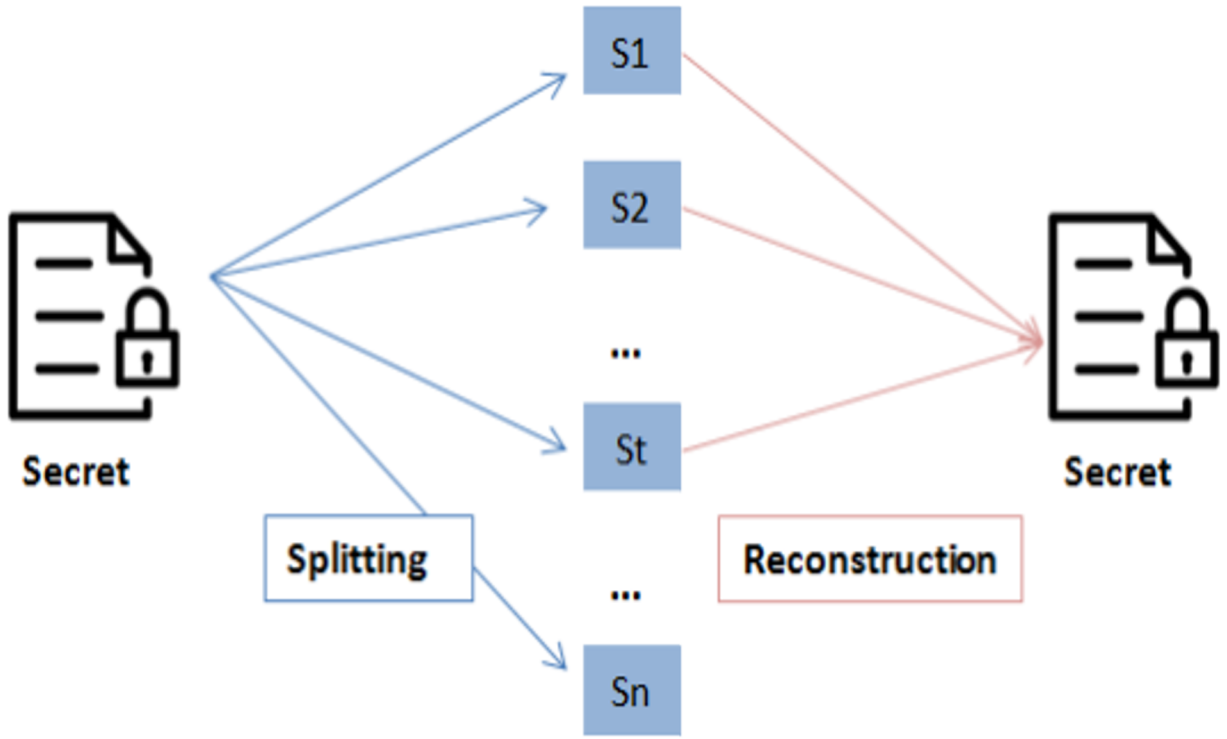
- Intel SGX is a technology that enables high-level protection of secrets against all non-authorized access.
- SGX uses enclave to allocate hardware-protected memory where data and code reside.
- Intel SGX provides dedicated attestation and sealing mechanisms to build a secure model.

Preliminaries



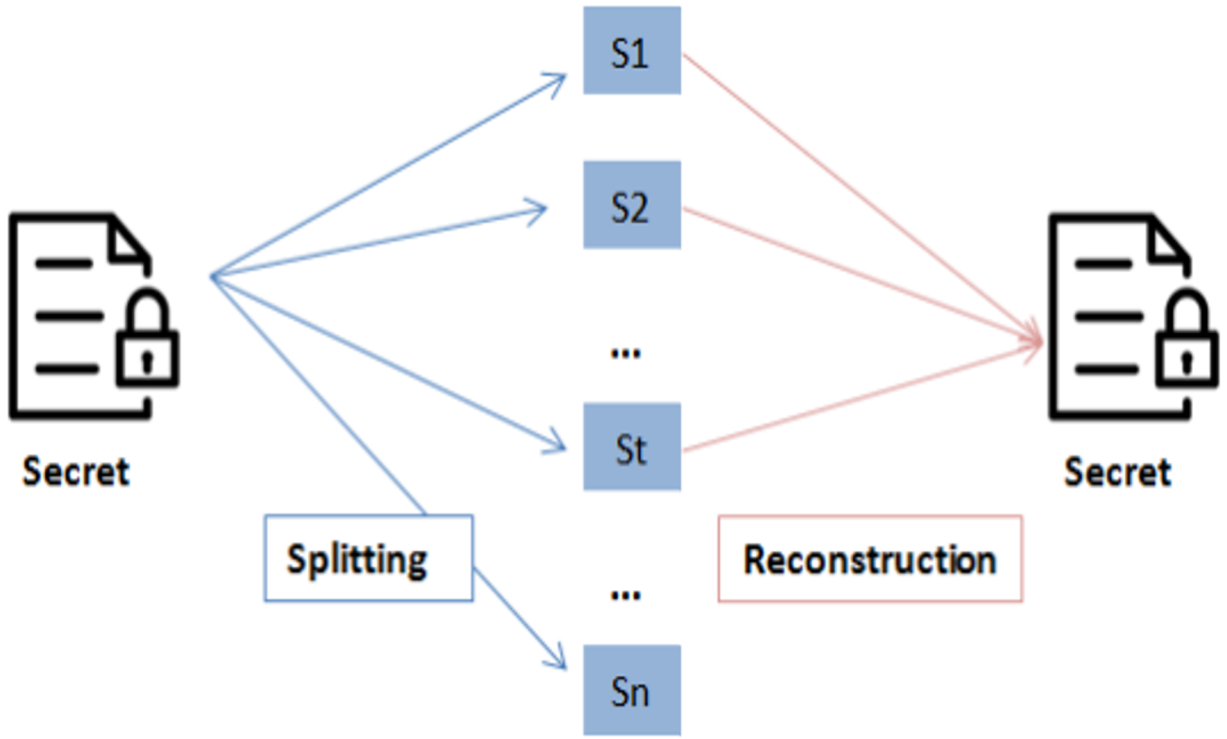
- Secret Sharing Schemes (SSS) refer to methods by which a party divides a secret into multiple shares distributed amongst a group of parties.

Preliminaries



- Secret Sharing Schemes (SSS) refer to methods by which a party divides a secret into multiple shares distributed amongst a group of parties.
- The secret is reconstructed if at least t participants present their shares.

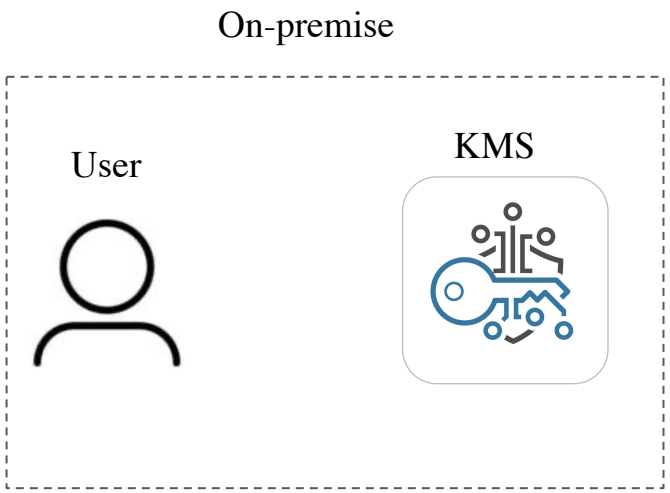
Preliminaries



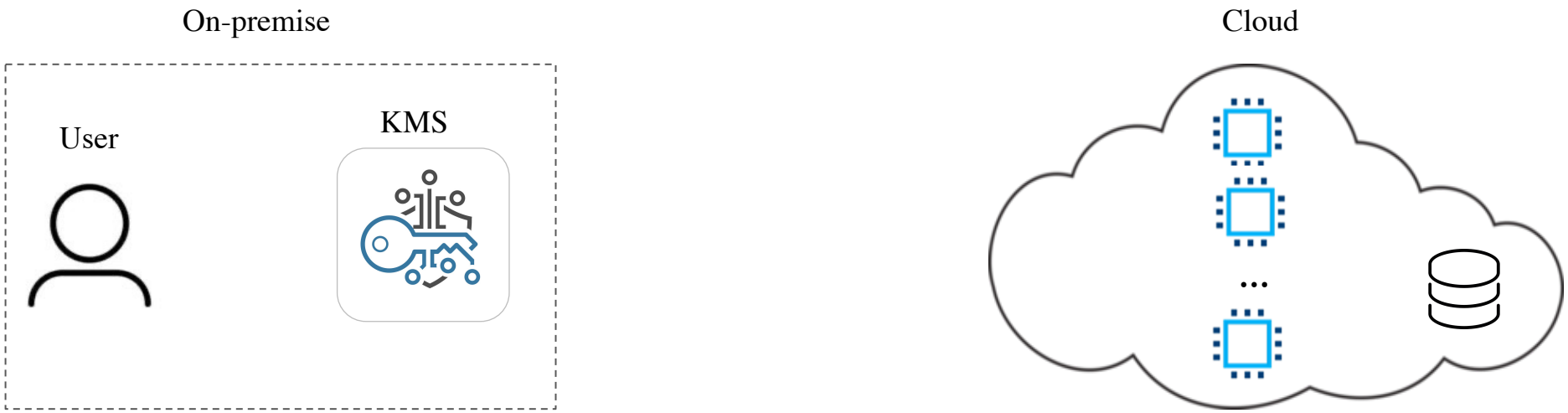
$$f(x) := \sum_{j=1}^{t} y_j l_j(x)$$

$$l_j(x) := \prod_{\substack{1 \le m \le t \\ m \ne j}} \frac{x - x_m}{x_j - x_m}$$

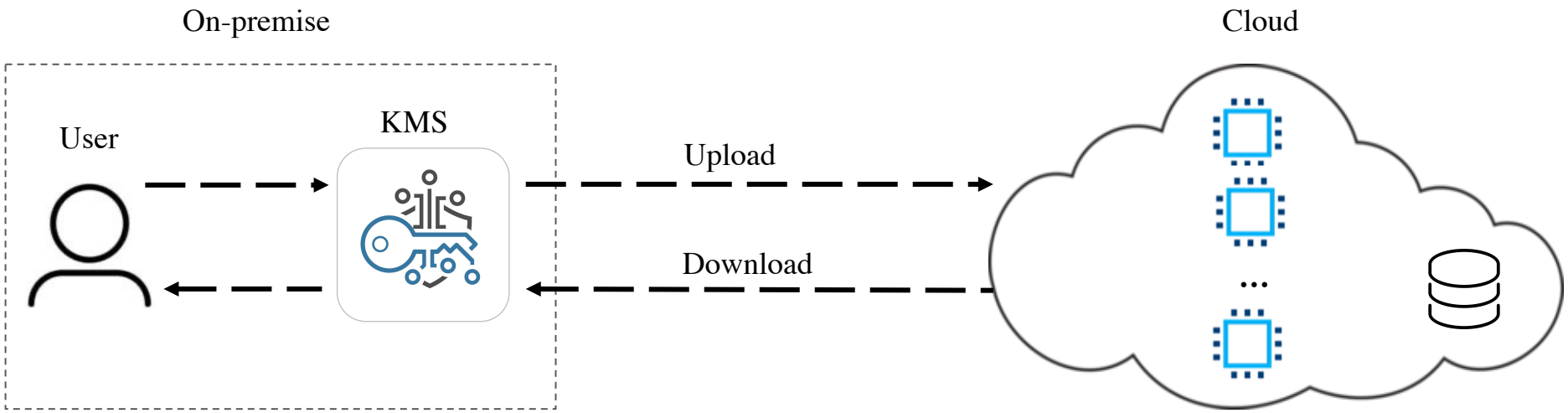
System Model



System Model



System Model

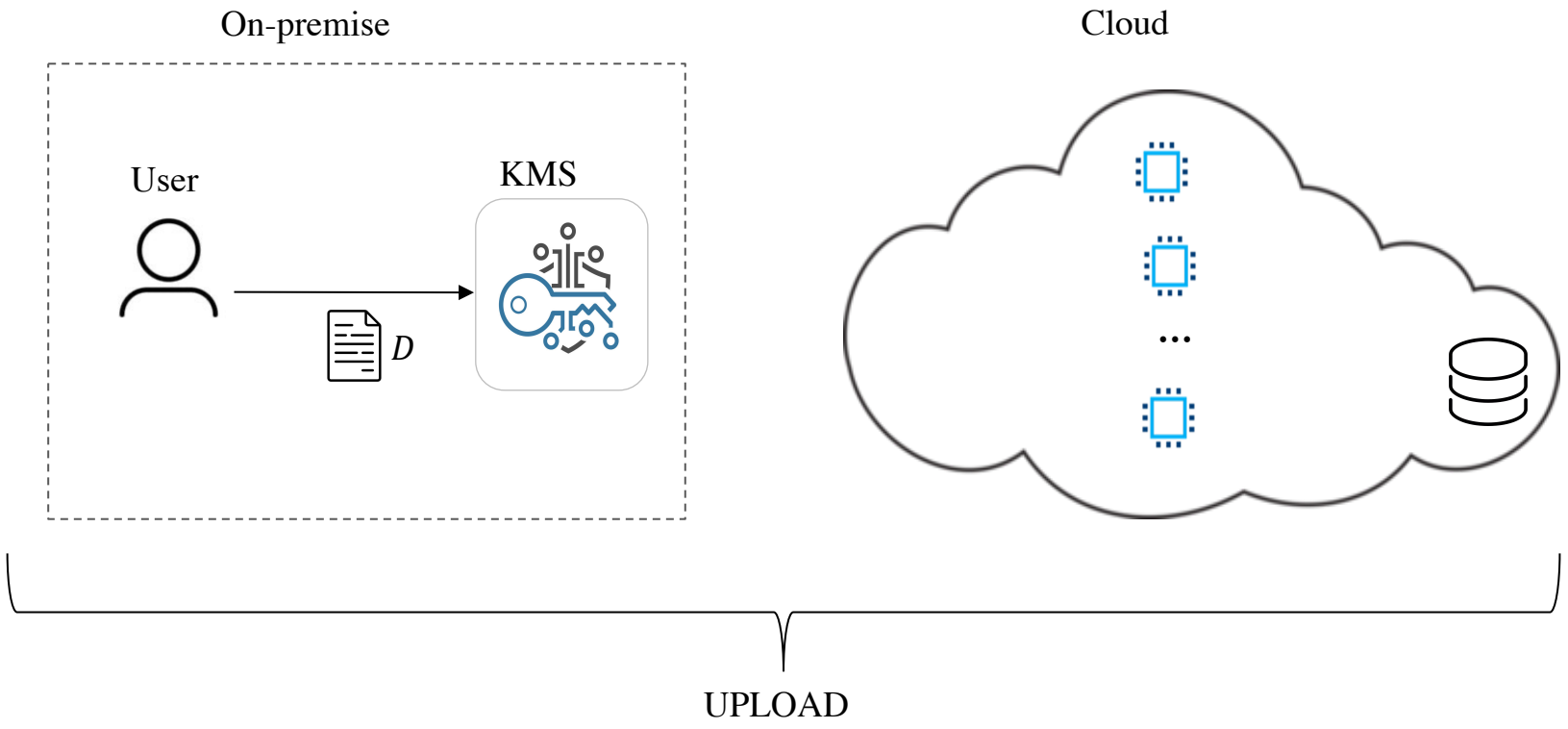


Contribution: Multi-SGX KMS

PHASE 1

KEY GENERATION

All SGX appliances are initialized by the KMS. The KMS generates a master key to protect sensitive data

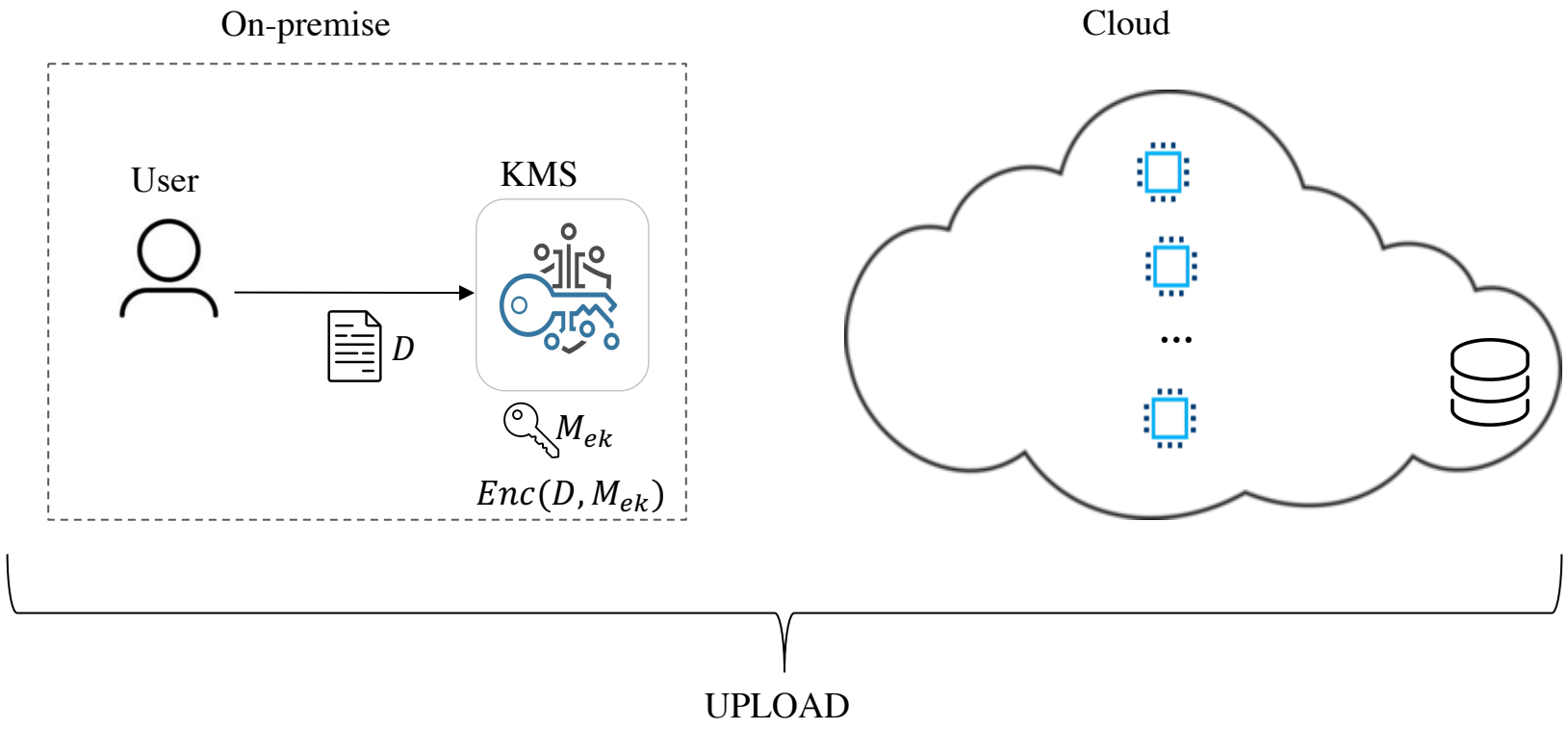


Contribution: Multi-SGX KMS

PHASE 1

KEY GENERATION

All SGX appliances are initialized by the KMS. The KMS generates a master key to protect sensitive data

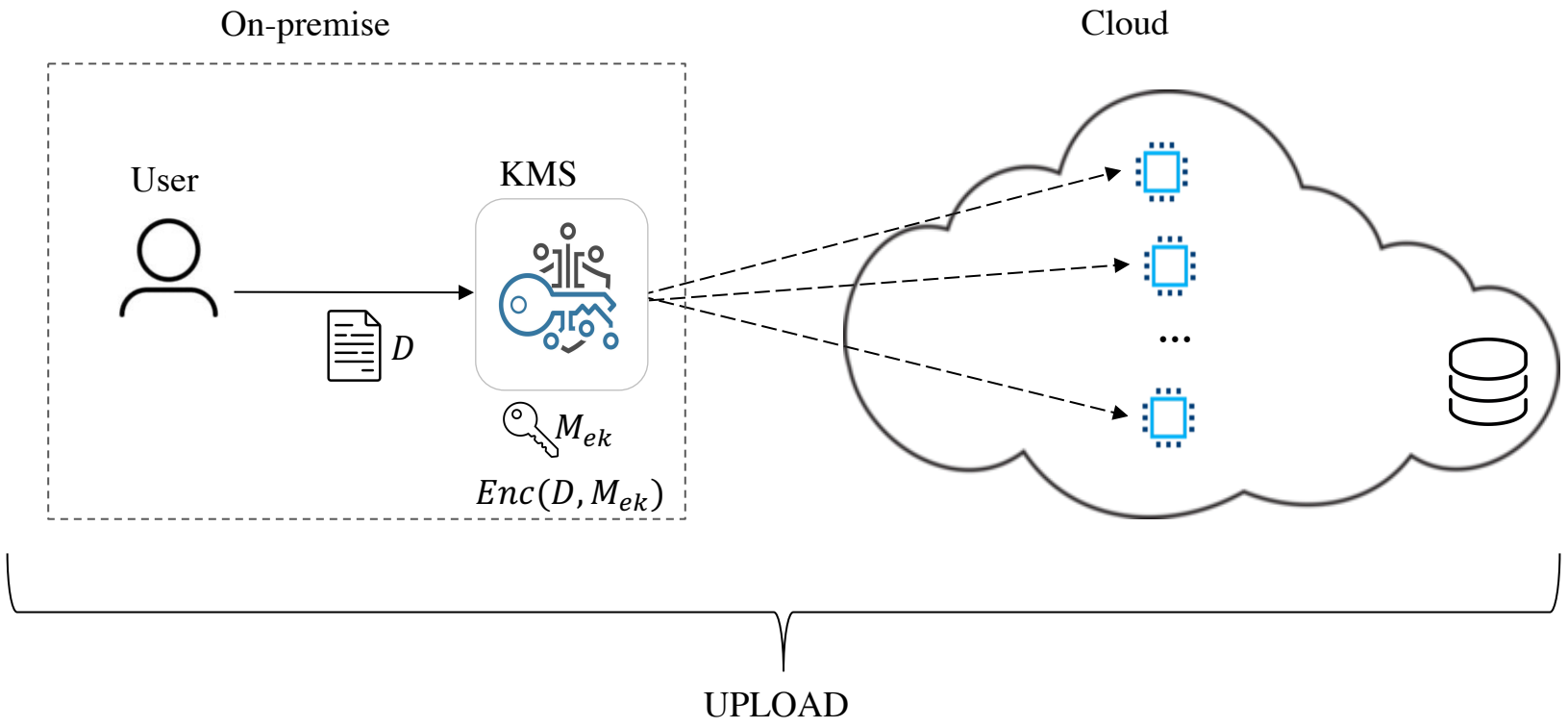


Contribution: Multi-SGX KMS

PHASE 1

KEY GENERATION

All SGX appliances are initialized by the KMS. The KMS generates a master key to protect sensitive data

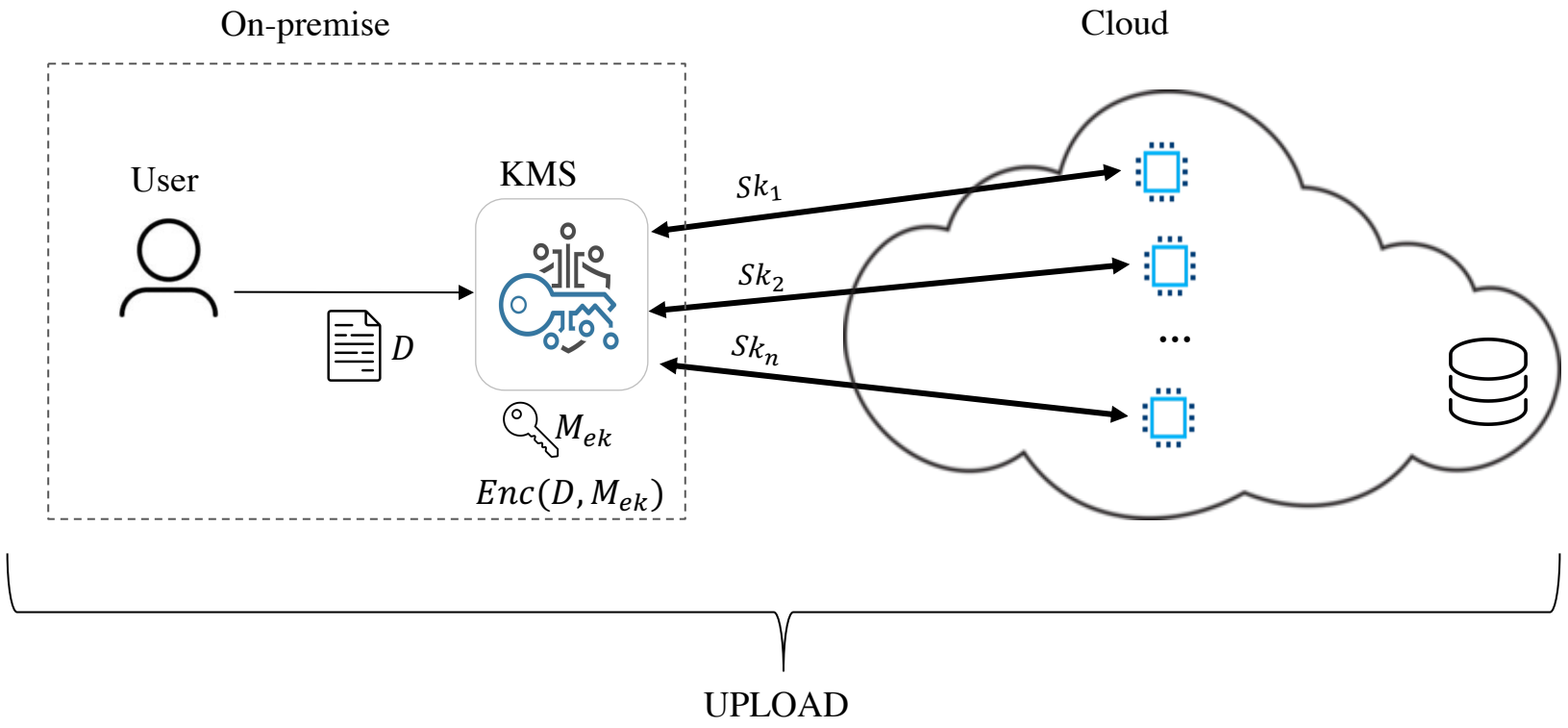


Contribution: Multi-SGX KMS

PHASE 2

Attestation

Each SGX enclave proves its identity using remote attestation, where secure communication channel is set up between the KMS and each SGX

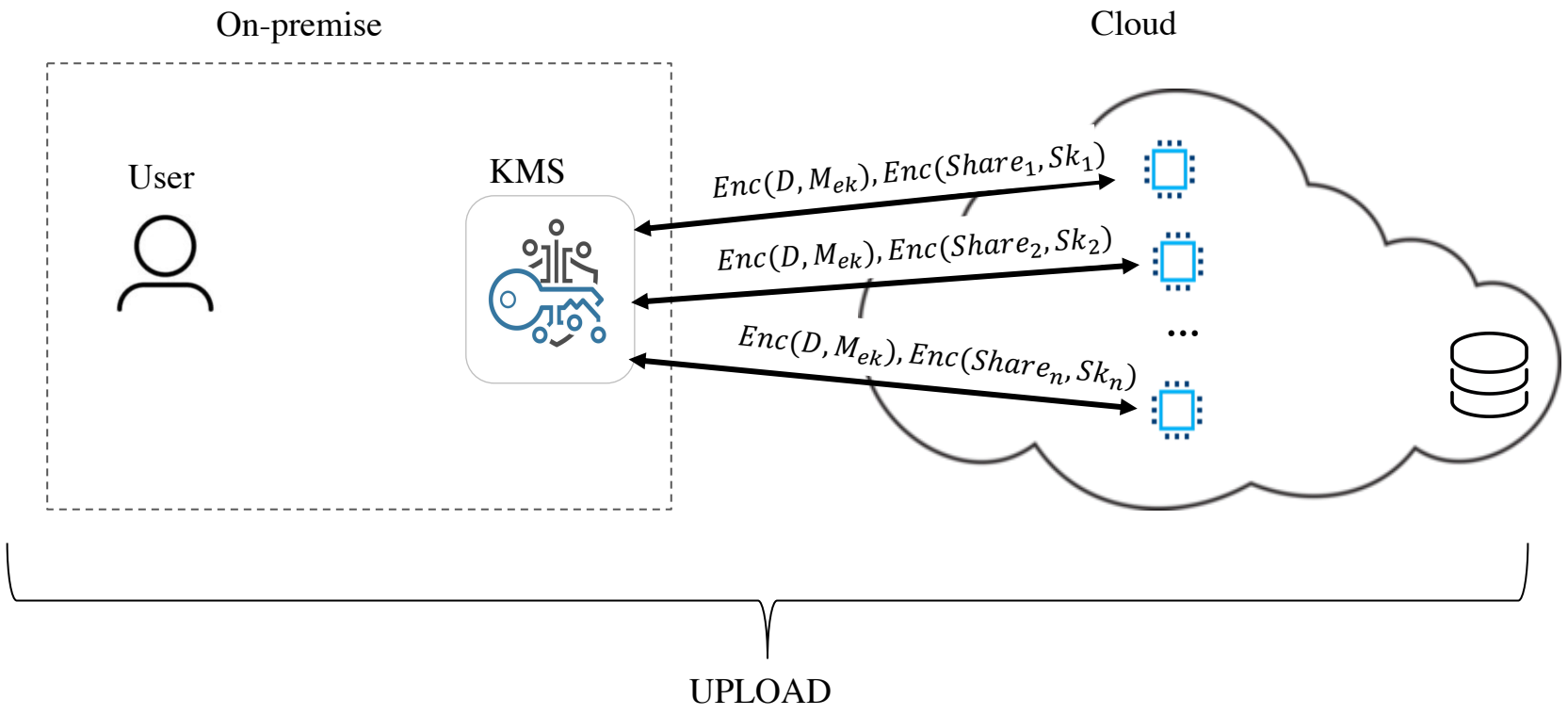


Contribution: Multi-SGX KMS

PHASE 3

KEY SHARING/ SEALING

The master key is split using the threshold secret sharing scheme. Where, each share is encrypted and transmitted to an SGX using its session key. The shares are then decrypted, and are sealed in a data storage

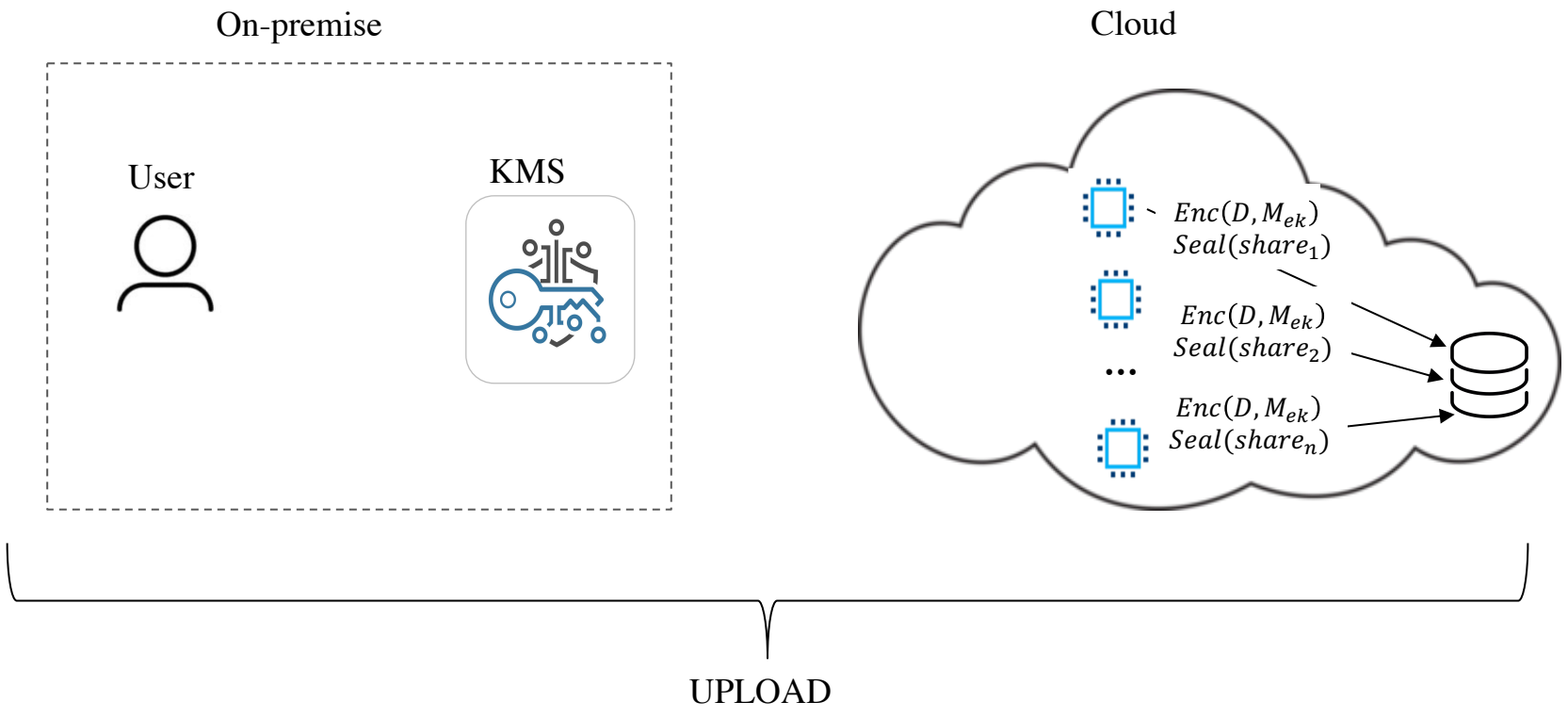


Contribution: Multi-SGX KMS

PHASE 3

KEY SHARING/ SEALING

The master key is split using the threshold secret sharing scheme. Where, each share is encrypted and transmitted to an SGX using its session key. The shares are then decrypted, and are sealed in a data storage

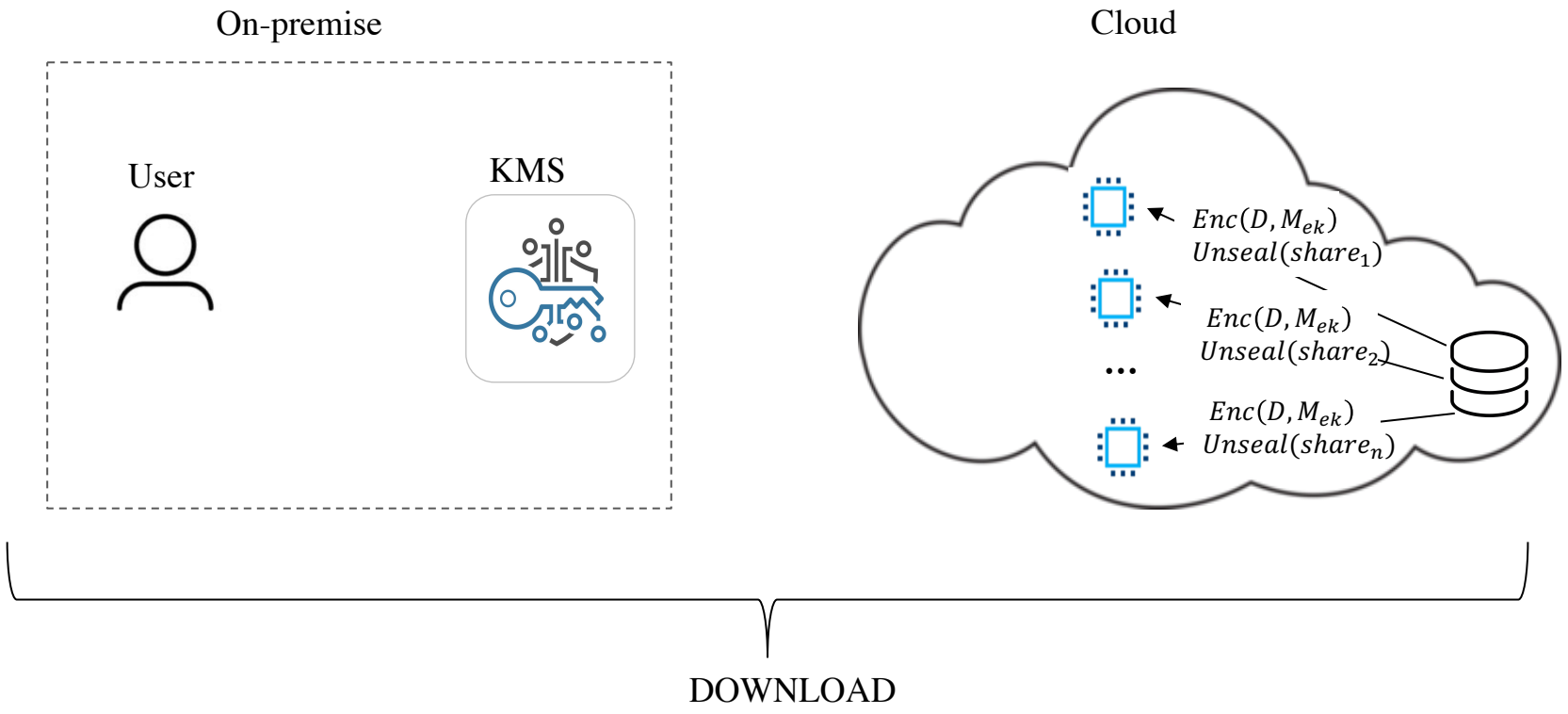


Contribution: Multi-SGX KMS

PHASE 4

UNSEALING / RECONSTRUCTION

The reconstruction requires that at least t SGX appliances to unseal their shares.

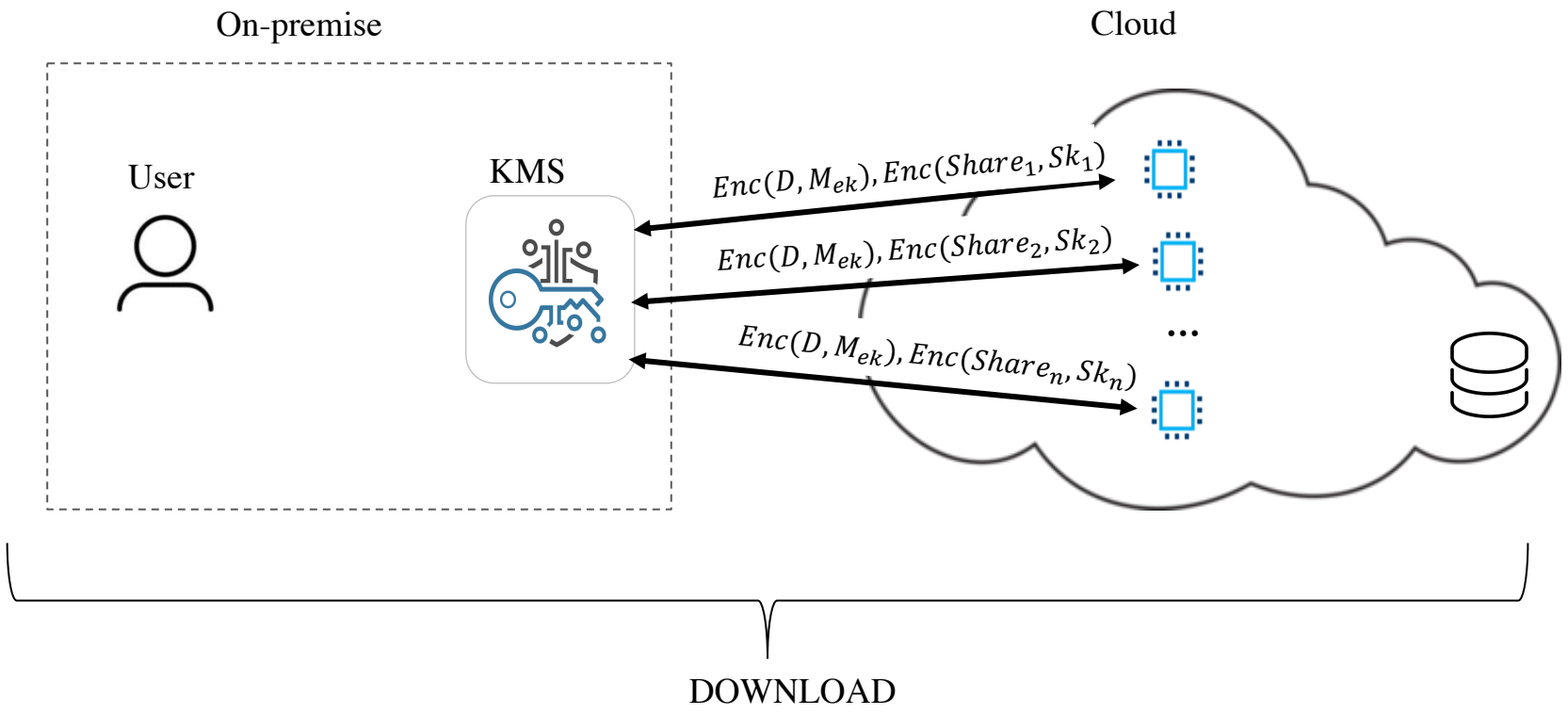


Contribution: Multi-SGX KMS

PHASE 4

UNSEALING / RECONSTRUCTION

The reconstruction requires that at least t SGX appliances to unseal their shares.

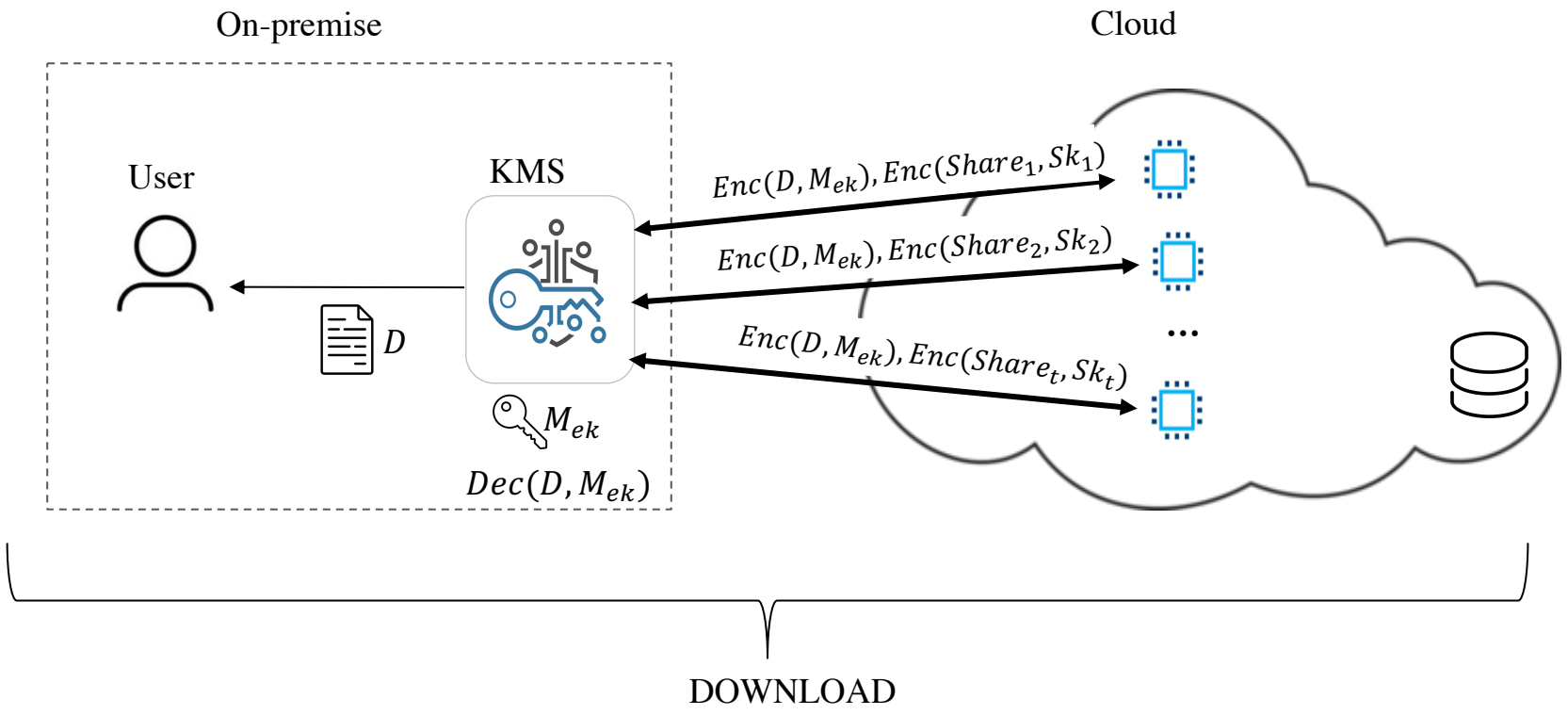


Contribution: Multi-SGX KMS

PHASE 4

UNSEALING / RECONSTRUCTION

The reconstruction requires that at least t SGX appliances to unseal their shares.

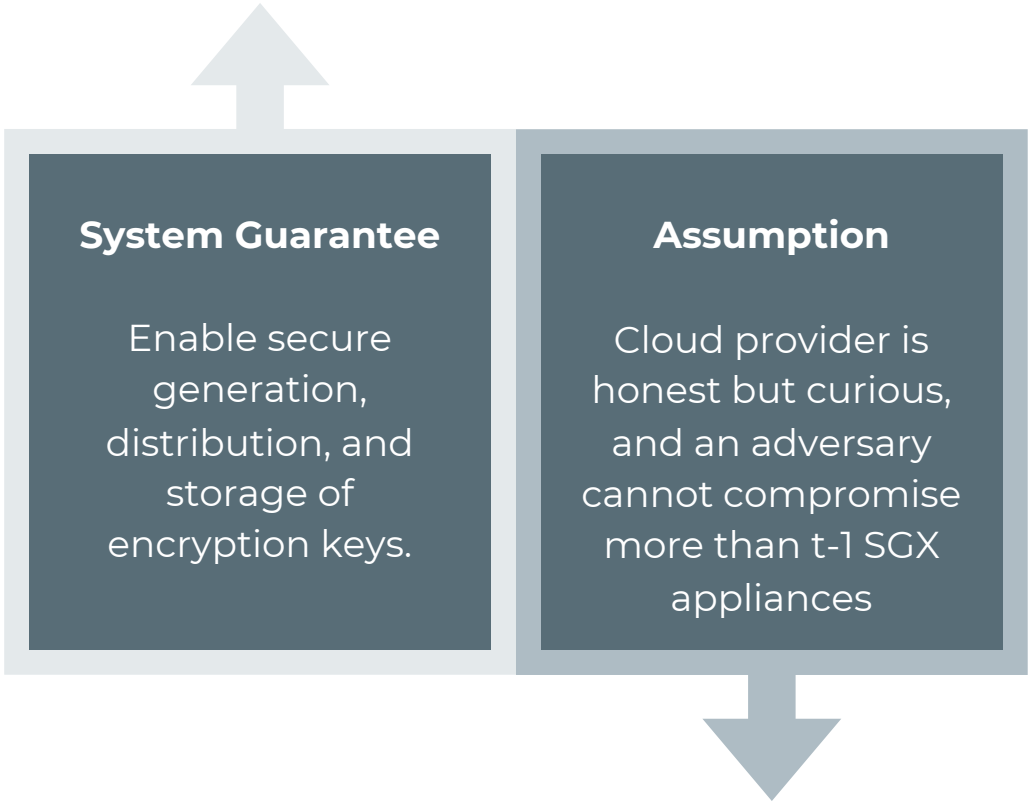


Adversarial Model

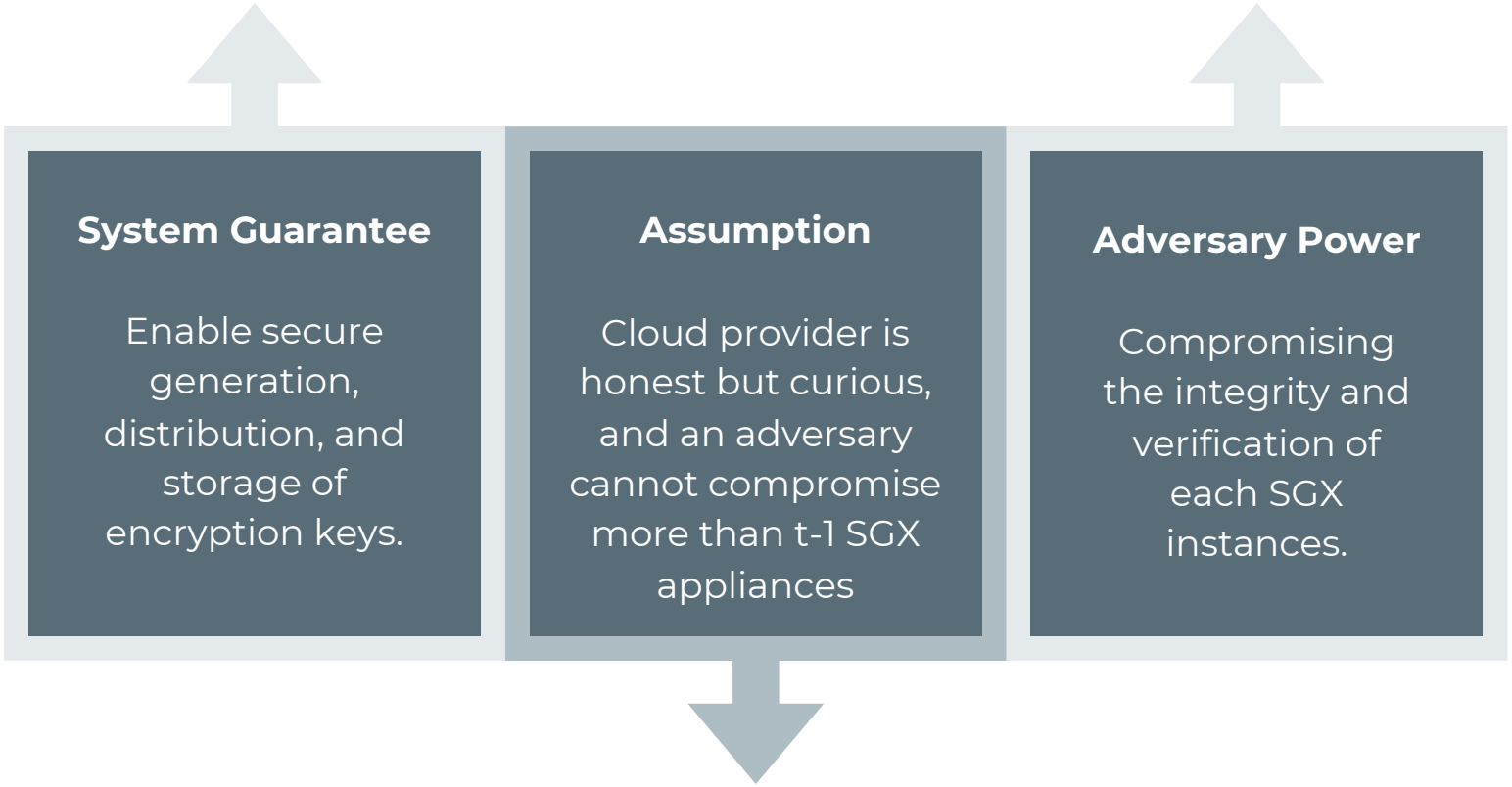
System Guarantee

Enable secure generation, distribution, and storage of encryption keys.

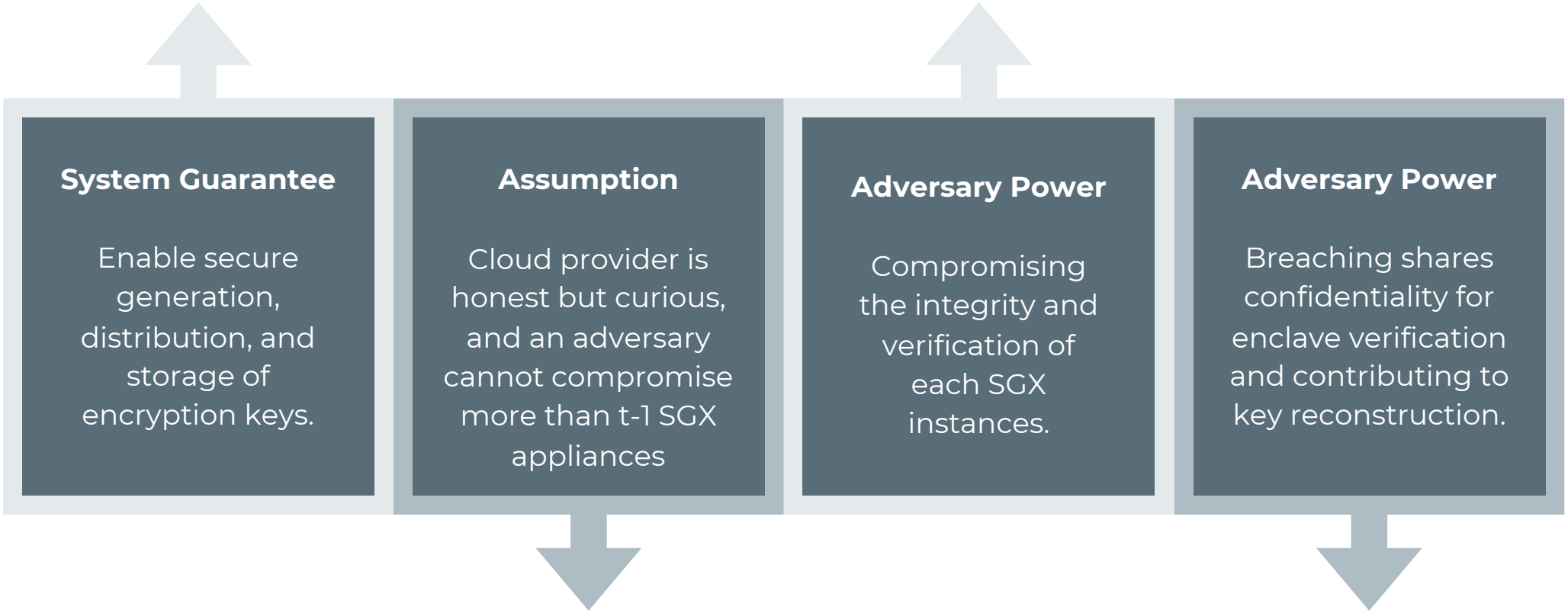
Adversarial Model



Adversarial Model



Adversarial Model



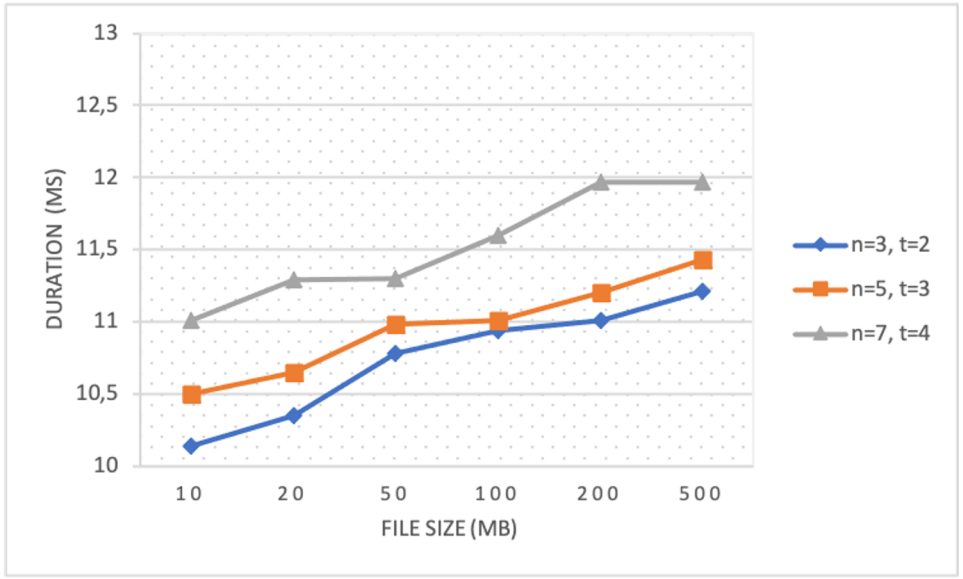
Security Analysis

Theorem 1. *The M_{sKey} cannot be learned with the presence of an adversary $\mathbb{A}$ except with an advantage of $Adv_{SS}[\mathbb{A}, M_{sKey}] < \varepsilon$.*

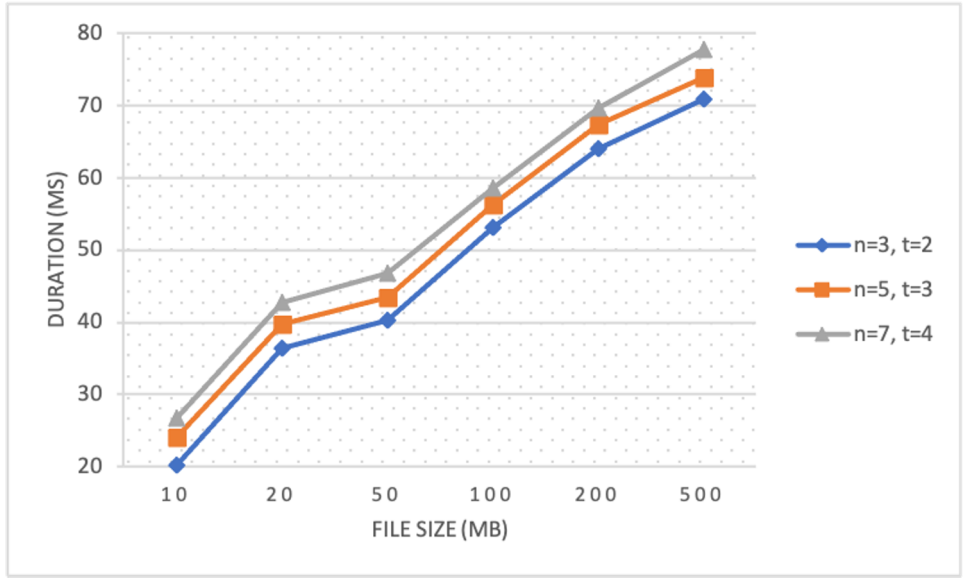
Theorem 2. *The integrity of every verified $SGX_1, SGX_2 \cdots SGX_n$ is without forgery, even in the presence of software impersonation.*

Performance Evaluation - Duration

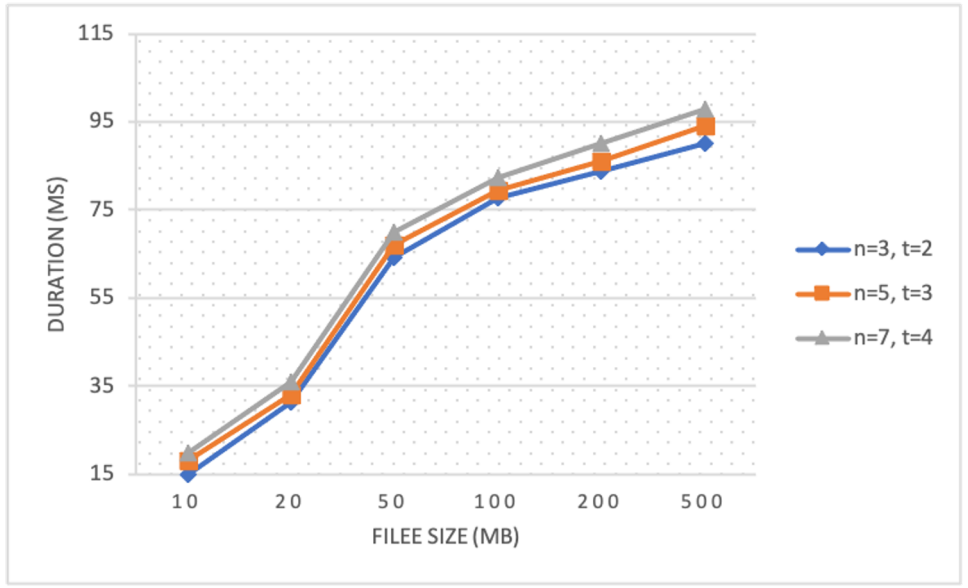
A



B

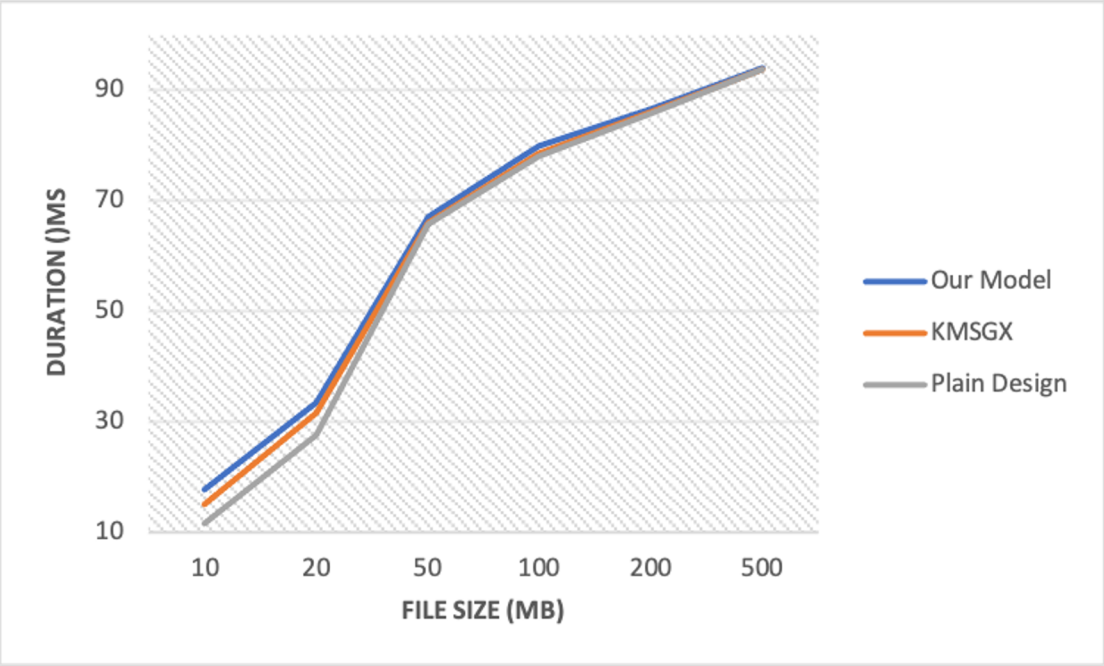


C

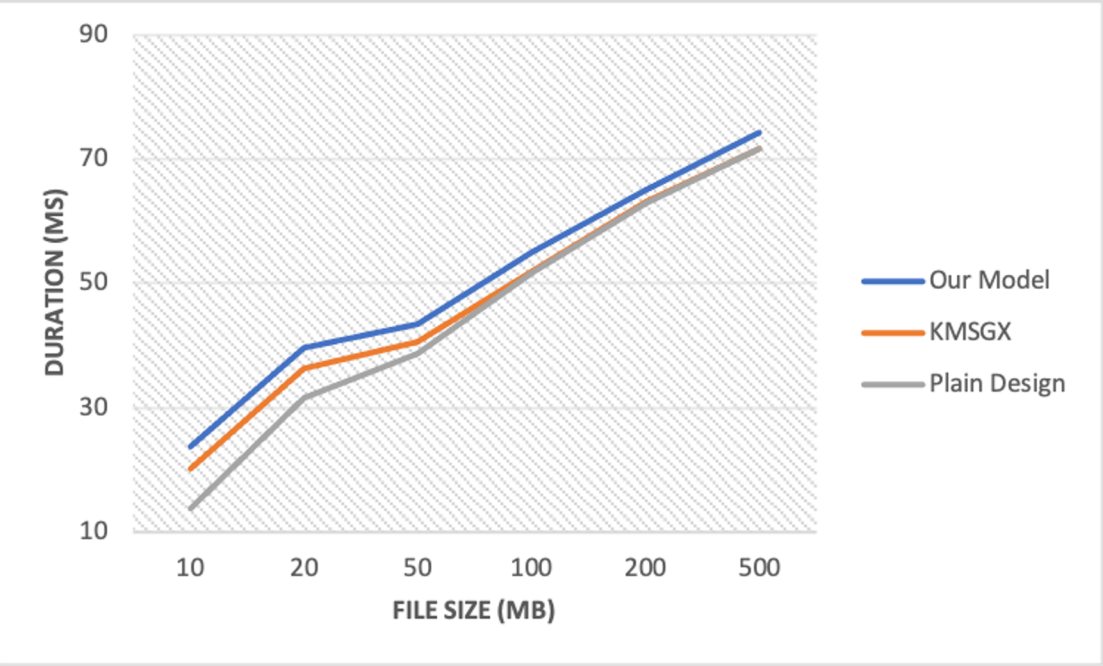


A - Initialization Time
B - Upload Time
C - Download Time

Performance Evaluation - Overhead Computation



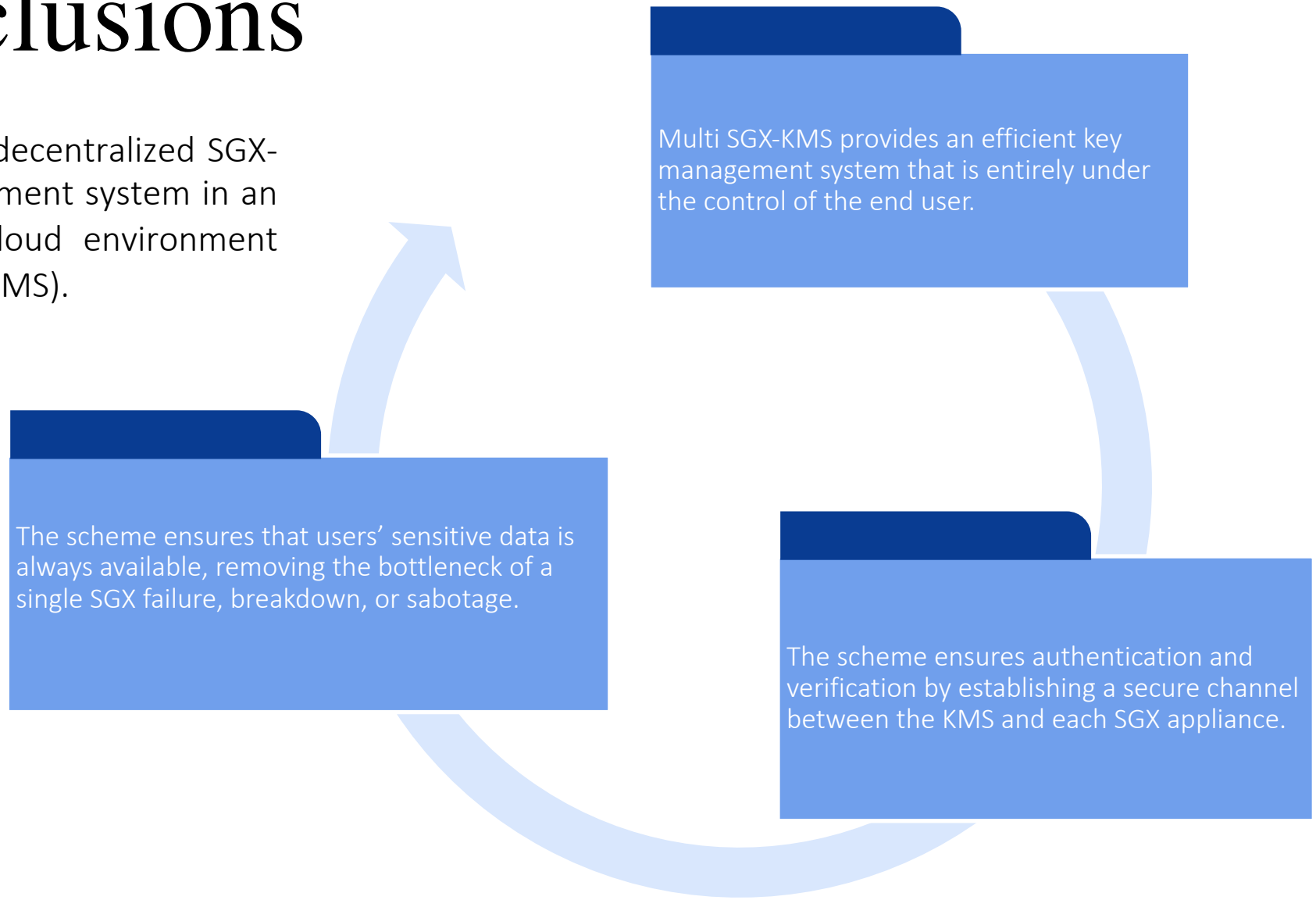
Download Analysis



Upload Analysis

Conclusions

Designed a decentralized SGX-key management system in an untrusted cloud environment (Multi SGX-KMS).



Thank you for your attention!

Questions?