HOMOMORPHIC CRYPTOGRAPHY

APPLICATION TO CLOUD SECURITY

Υπεύθυνος καθηγητής: Κ.Α. Δραζιώτης
παρουσίαση: Τσιροζίδης Ιωάννης

INTRO

- TODAY'S DATA USAGE
- CLOUD SERVICES/ CLOUD COMPUTING
- CLOUD SECURITY/ CLOUD CRYPTO

HOMOMORPHIC CRYPTOGRAPHY IN **CLOUD** SECURITY

- DEFINITION, BRIEF HISTORY
- INSTANCES OF USE, COMPANIES' ADAPTATIONS

DISCLAIMER

All shapes, diagrams and sketches used in this presentation are drawn by hand and do not fall under any copyright.

INTRO

TODAY’S DATA USAGE

CLOUD SERVICES/ CLOUD COMPUTING

CLOUD SECURITY/ CLOUD CRYPTO

INTRO

TODAY’S DATA USAGE

Our private information and data are being shared more widely than ever before. And often, we're the ones sharing it. We share our data in exchange for convenience and improved services.

And for most, giving up our personal information is required to interact in the digital world — both at work, and to utilize basic everyday social needs—.

So how do we know our data is safe?

INTRO

TODAY'S DATA USAGE

IN FACT out of all the data
a business can LEGALLY collect about you:

79.49%	68.23%
46.15%	23.08%

statistics presented are referring to data analytics observed in the timestamp of Mar. 2021 - Sep.2021

INTRO

TODAY’S DATA USAGE

Well, most of the sensitive data we share is encrypted. Encrypted data is useless to hackers and thieves, as it's translated into complex code, or CIPHERTEXT, that is illegible by humans. That's a good thing.

But while encryption safeguards our data as it's being stored or transferred, the data must be decrypted—or translated back into a clear text— to be processed.

This provides a window of opportunity where your data is exposed, making it vulnerable to cyber criminals, privacy violations, and other misuse.

INTRO

TODAY’S DATA USAGE

SO, WHAT HAPPENS WHEN WE DO A SEARCH?

The Internet search engine, **search the Internet based on important words**. They go through the remote database and categorize results based on the given key-words. They keep an index of the words they find, and where they find them.

The search results tend to be optimized depending on the user’s habits, interests and older searches.

INTRO

TODAY'S DATA USAGE

“ The search results tend to be optimized depending on the user's habits, interests and older searches. ”

The data provided get stored in companies remote databases.

And same goes for Cloud Computing.

INTRO

CLOUD SERVICES/
CLOUD COMPUTING

CLOUD COMPUTING is a model for enabling

- convenient,
- on-demand network access

to a shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

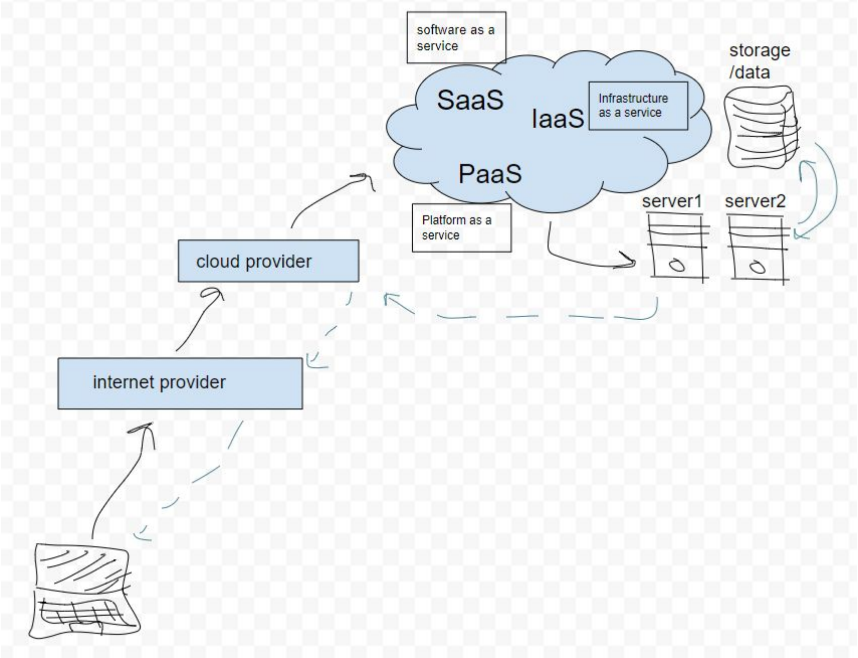
INTRO

CLOUD SERVICES/
CLOUD COMPUTING

SaaS

PaaS

IaaS



representation of how Cloud Services work

INTRO

CLOUD SERVICES/
CLOUD COMPUTING

(SaaS) Software as a Service, also known as cloud application services, represents the most commonly utilized option for businesses in the cloud market.

SaaS utilizes the internet to deliver applications to its users, which are managed by a third-party vendors.

A majority of SaaS applications run directly through your web browser, which means they do not require any downloads or installations on the client side.

common Examples

Google Workspace, Dropbox, Cisco WebEx, Concur, GoToMeeting

INTRO

CLOUD SERVICES/
CLOUD COMPUTING

(PaaS) Platform as a Service, also known as Cloud platform services, provide cloud components to certain software while being used mainly for applications.

PaaS delivers a framework for developers that they can build upon and use to create customized applications.

All servers, storage, and networking can be managed by the enterprise or a third-party provider while the developers can maintain management of the applications.

common Examples

Windows Azure, Heroku, Google App Engine, Apache Stratos, OpenShift

INTRO

CLOUD SERVICES/
CLOUD COMPUTING

(IaaS) Infrastructure as a Service, known as Cloud infrastructure services, are made of highly scalable and automated compute resources.

IaaS is fully self-service for accessing and monitoring computers, networking, storage, and other services.

IaaS allows businesses to purchase resources on-demand and as-needed instead of having to buy hardware outright.

common Examples

DigitalOcean, Linode, Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE)

INTRO

CLOUD SERVICES/ CLOUD COMPUTING

🪛 Service Type that You are Responsible of Managing

☁ Service Type Others manage on your behalf

Service Type	IaaS	PaaS	SaaS
Applications	🪛	🪛	☁
Data	🪛	🪛	☁
Runtime	🪛	☁	☁
Middleware	🪛	☁	☁
O/S	🪛	☁	☁
virtualization	☁	☁	☁
servers	☁	☁	☁
storage	☁	☁	☁
networking	☁	☁	☁

CLOUD SECURITY

Cloud Security is a shared responsibility between the user and the cloud provider.

Prevent data leakage

Strong authentication

Data encryption

Visibility and threat detection

Continuous compliance

Integrated security

CLOUD CRYPTOGRAPHY

There are two primary types of cloud cryptography an organization should include in cybersecurity plans:

- DATA in TRANSIT

and

- DATA at REST

CLOUD CRYPTOGRAPHY

DATA in TRANSIT

Data-in-transit is data that is moving between endpoints.

A common form of data-in-transit cloud encryption is HTTPS and HTTP protocols that secure the information channel you use when visiting different sites across the web. They do this with an SSL, “Secure Socket Layer,” which is a layer of encryption around the secure channel.

CLOUD CRYPTOGRAPHY

DATA at REST

Data-at-rest is sensitive data you store in corporate IT structures such as servers, disks, or cloud storage services.

Encrypting data while it is stored allows you to enforce access control by only giving decryption credentials to those employees with authorization.

HOMOMORPHIC CRYPTOGRAPHY

DEFINITION, BRIEF HISTORY

INSTANCES OF USE, COMPANIES’ ADAPTATIONS

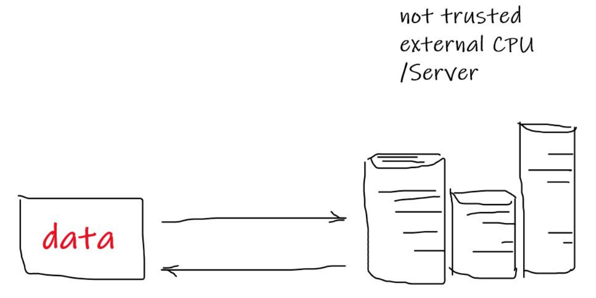
GRID-BASED CRYPTOGRAPHY, LWE-homomorphic cryptosystem

HOMOMORPHIC CRYPTOGRAPHY

DEFINITION, BRIEF HISTORY

Homomorphic encryption makes it possible to perform calculations on encrypted data.

This means that data processing can be outsourced to a third party without the need to trust the third party to properly secure the data. Without the proper decryption key, the original data can't be accessed.



Partially Homomorphic Encryption

Somewhat Homomorphic Encryption

Fully Homomorphic Encryption

Partially Homomorphic Encryption

Partially homomorphic encryption algorithms allow a certain operation to be performed an infinite number of times.

more details next slide

For example, a particular algorithm may be additively homomorphic, meaning that adding two cipher together produces the same result as encrypting the sum of the two plaintexts.

In fact, some common encryption algorithms are partially homomorphic by chance.

Partially Homomorphic Encryption

For example, the RSA algorithm is multiplicatively homomorphic. The reason for this is that encryption in RSA is based on exponentiation: C = (m^x) (mod n), where **m** is the message and **x** is the secret key.

The rules of exponents say that (a^n)(b^n)=(ab)^n. This means that multiplying two ciphertexts encrypted with the same key is equivalent to raising the product of the plaintexts to the power of the secret key.

Therefore, RSA is multiplicatively homomorphic.

But, what do we mean by that?

RSA

$C = m^x \pmod n$

Suppose m_1, m_2 two messages and x the key

Calculate $m_1 \cdot m_2$, using Homomorphism.

-Homomorphism performs calculations on ENCRYPTED data.

Therefore, we send to the server $E(m_1)$ and $E(m_2)$, without it knowing neither m_1 nor m_2, and ask to calculate $E(m_1 \cdot m_2)$, using $E(m_1)$ and $E(m_2)$

$E(m1) = m_1^x \pmod n$

$E(m_2) = m_2^x \pmod n$

$a1 \equiv b1 \pmod n$ and $a2 \equiv b2 \pmod n$

$E(m_1) \cdot E(m_2) = [m_1^x \pmod n] \cdot [m_2^x \pmod n]$

$= [(m_1^x) \cdot (m_2^x)] \pmod n = (m_1 \cdot m_2)^x \pmod n$

$a1\, a2 \equiv b1\, b2 \pmod n$

$= E(m_1 \cdot m_2)$

Somewhat Homomorphic Encryption

The next step up from partially homomorphic encryption is somewhat homomorphic encryption. A somewhat homomorphic encryption algorithm allows a finite number of any operation rather than an *infinite number of a particular operation*.

For example, a somewhat homomorphic encryption algorithm may be able to support any combination of up to **five additions** or **multiplications**. However, a sixth operation of either type would create an invalid result.

Somewhat homomorphic encryption algorithms are an important stepping stone on the way to fully homomorphic encryption.

Fully Homomorphic Encryption

Fully homomorphic encryption is the holy grail of homomorphic encryption.

A fully homomorphic encryption algorithm allows an infinite number of additions or multiplications of ciphertexts while still producing a valid result.

∞

Fully Homomorphic Encryption

The first fully homomorphic cryptographic System was developed by Craig Gentry in 2009, and it used lattices and their properties.

In general Cryptosystems based on lattices, other than their use in Homomorphic Cryptography are candidates for Post Quantum Cryptography as well. We consider them candidates, because in the future there can be an quantic algorithm able to efficiently solve lattices problems.

HOMOMORPHIC CRYPTOGRAPHY

INSTANCES OF USE, COMPANIES' ADAPTATIONS

EVERYDAY EXAMPLES / Companies' Adaptations

Microsoft, has created the SEAL (Simple Encrypted Arithmetic Library), a set of encryption libraries that allows calculations to be performed directly on encrypted data. Using open source uniform encryption technology, the Microsoft team is working with companies to create end-to-end encryption data storage and computing services.

EVERYDAY EXAMPLES / Companies’ Adaptations

Google has also announced its support for uniform encryption, revealing its own open source encryption tool, Private Join and Compute. Google's tool focuses on data analysis in encrypted form, where only the information obtained from the analysis is visible and not the underlying data.

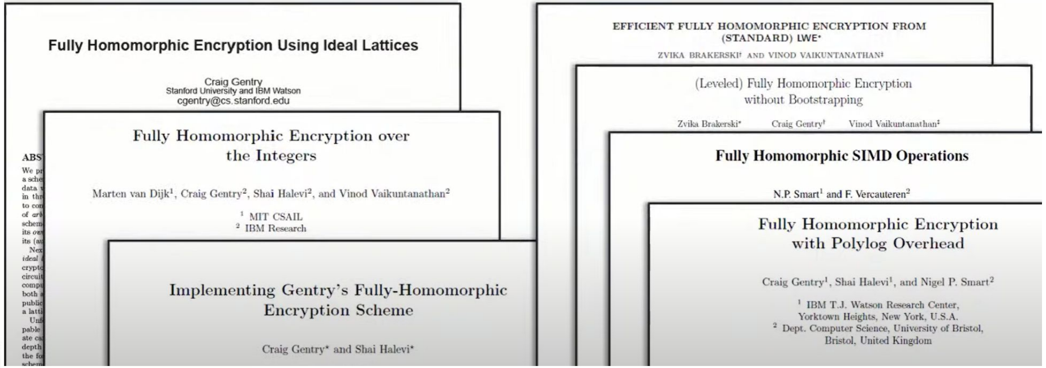
EVERYDAY EXAMPLES / Companies' Adaptations

Finally, in a bid to make homomorphic encryption widespread, IBM released the first edition of the HElib library in 2016, which reportedly "was 100 trillion times slower than plain text operations." Since then, IBM has worked to solve this problem and has come up with a version that is 75 times faster, but still lags behind the corresponding plain text functions.

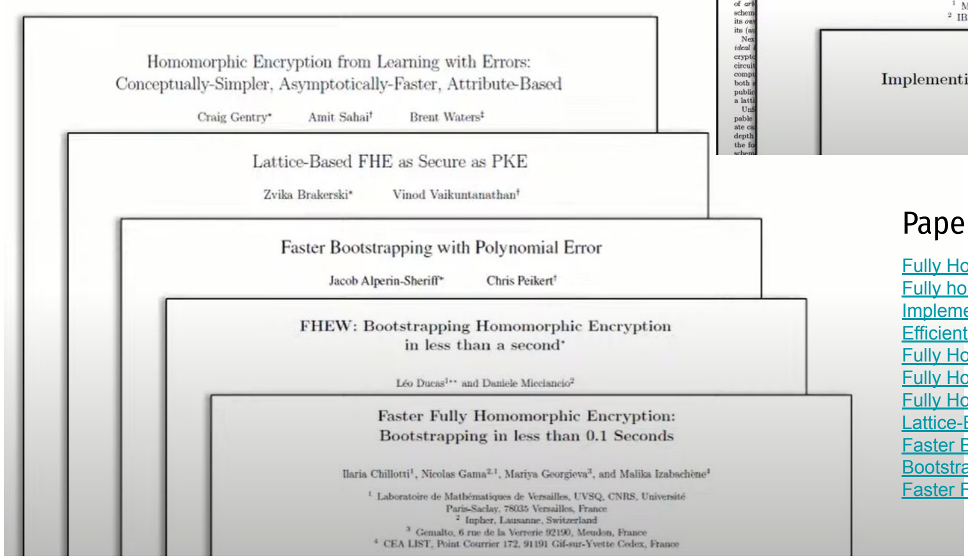
HOMOMORPHIC CRYPTOGRAPHY

EVOLUTION

“ first generation of FHE ”



“ second generation of FHE ”



Paper’s REFERENCES

Fully Homomorphic Encryption using Ideal Lattices
Fully homomorphic encryption over the integers
Implementing Gentry's Fully-Homomorphic Encryption Scheme
Efficient Fully Homomorphic Encryption from (Standard) LWE
Fully Homomorphic Encryption without Bootstrapping
Fully Homomorphic SIMD Operations
Fully Homomorphic Encryption with Polylog Overhead
Lattice-Based FHE as Secure as PKE
Faster Bootstrapping with Polynomial Error
Bootstrapping Homomorphic Encryption in less than a second
Faster Fully Homomorphic Encryption

HOMOMORPHIC CRYPTOGRAPHY

DEFINITION, BRIEF HISTORY

Homomorphic Cryptography, apart from its use in Cloud Security finds applications in various other fields (e.g. Machine Learning, Web Browsers, Clinical Data, …)

This type of Cryptography may be at the moment, at the very first stages of its evolution, but it sure is a promising -and why not say- Revolutionary way of handling our data.

REFERENCES

Σημειώσεις Εισαγωγή στο μάθημα Θεμελιώσεις κρυπτογραφίας Κ.Α.Δραζιώτης

Κ.Α. Δραζιώτης “Εισαγωγή στην Κρυπτογραφία”, ανοικτές ακαδημαϊκές εκδόσεις ΚΆΛΛΙΠΟΣ

https://www.homodigitalis.gr/posts/5200

https://www.ibm.com/topics/cloud-security?cm_mmc=OSocial_Youtube-_-Cloud+and+Data+Platform_Cloud+Platform+Digital-_-WW_WW-_-YTDescription-101-What-is-Cloud-Security-LH-Cloud-Security&cm_mmca1=000016GC&cm_mmca2=10010612

IBM News

https://www.bmc.com/

https://www.ripublication.com/irph/ijict_spl/ijictv4n15spl_05.pdf

https://www.keyfactor.com/blog/what-is-homomorphic-encryption/

THANK YOU FOR YOUR ATTENTION