Applying Homomorphic Encryption in the Cloud

Jesús Antonio Soto Velázquez

Universidad Autónoma de Nuevo León

23 de septiembre de 2015

Overview

1. Introduction
   - Problem Definition
   - Motivation
   - Hyphotesis
   - Objectives
   - Case Study
2. Second Section

Introduction

These days, it has become more common to exchange information with our peers remotely. An issue arises when the information is considered to be *sensitive*, and thus, the confidentiality of it must be protected.

Cryptography is the study of techniques that enable secret communication, such as ciphers, that is, encryption and decryption algorithms to be used on sensitive data.

The issue at hand becomes even more interesting when the safe containing the private information does not go directly to the intended party, but is rather stored somewhere in the cloud, i.e. the Internet.

Problem Definition

An approach to secure data on the cloud consists in encrypting the data before storing it; therefore, assuring its confidentiality. However, it is inconvenient to modify the data if this approach is followed.

Homomorphic encryption is an advanced technique used to modify the already encrypted data without compromising its confidentiality.

Even though there are many homomorphic encryption schemes that have been created to allow for computations on encrypted data, so far, they are not considered fast enough to build efficient secure cloud computing solutions.

Motivation

There are many areas in which homomorphic encryption could be used, such as the medical, marketing, and financial fields. Until now, there was no way to make a concrete implementation of a solution related to these areas, since available schemes were either too limited or too slow.

By showing a compelling example of how homomorphic encryption can be applied in a simple scenario, cloud service providers and developers might start considering how to apply homomorphic encryption in other ways and mediums, and thus, expanding on software that makes use of it.

Hyphotesis

Building a client-server based solution using the homomorphic encryption functionalities provided by HElib is feasible in terms of processing time.

Objectives

Develop a client-server based solution using HElib to perform homomorphic evaluations on encrypted data.

Specific Objectives:

1. Establish a client-server architecture where homomorphic encryption can be applied.
2. Identify which factors pose a challenge to deem applications of homomorphic encryption as inefficient.
3. Show the use of HElib to setup, encrypt, and decrypt in simple terms.
4. Collect performance data on the use of homomorphic encryption.

Case Study

Consider a household that has a pattern of activity, i.e. empty during the day and non-empty at night, so that the resident seeks to ascertain the number of people inside at any point in time during the day.

Assuming the resident has put in place certain sensors around the building so that it detects and counts who comes in and out, he would like to learn the value of the counter remotely. As the resident chooses to store the value in the cloud, he quickly realizes he does not want others to learn of this value, not even the cloud service itself, as to prevent potential burglars to break in when the household is empty.

Bullet Points

- Lorem ipsum dolor sit amet, consectetur adipiscing elit
- Aliquam blandit faucibus nisi, sit amet dapibus enim tempus eu
- Nulla commodo, erat quis gravida posuere, elit lacus lobortis est, quis porttitor odio mauris at libero
- Nam cursus est eget velit posuere pellentesque
- Vestibulum faucibus velit a augue condimentum quis convallis nulla gravida

Blocks of Highlighted Text

Block 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer lectus nisl, ultricies in feugiat rutrum, porttitor sit amet augue. Aliquam ut tortor mauris. Sed volutpat ante purus, quis accumsan dolor.

Block 2

Pellentesque sed tellus purus. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Vestibulum quis magna at risus dictum tempor eu vitae velit.

Block 3

Suspendisse tincidunt sagittis gravida. Curabitur condimentum, enim sed venenatis rutrum, ipsum neque consectetur orci, sed blandit justo nisi ac lacus.

Multiple Columns

Heading

1. Statement
2. Explanation
3. Example

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer lectus nisl, ultricies in feugiat rutrum, porttitor sit amet augue. Aliquam ut tortor mauris. Sed volutpat ante purus, quis accumsan dolor.

Table

Treatments	**Response 1**	**Response 2**
Treatment 1	0.0003262	0.562
Treatment 2	0.0015681	0.910
Treatment 3	0.0009271	0.296

Table 1 : Table caption

Theorem

Theorem (Mass–energy equivalence)

$E = mc^2$

Verbatim

Example (Theorem Slide Code)

```
\begin{frame}
\frametitle{Theorem}
\begin{theorem}[Mass--energy equivalence]
$E = mc^2$
\end{theorem}
\end{frame}
```

Figure

Uncomment the code on this slide to include your own image from the same directory as the template .TeX file.

Citation

An example of the `\cite` command to cite within the presentation:

This statement requires citation [Smith, 2012].

References

John Smith (2012)
Title of the publication
Journal Name 12(3), 45 – 678.

The End