# Esquema de Cifrado de Datos con Capacidades de Búsqueda[1]

Melissa Brigitthe Hinojosa Cabello

Cinvestav - Unidad Tamaulipas

## 1. Introducción

El almacenamiento en la nube es un modelo de servicio en el cual se almacenan, gestionan y respaldan datos de forma remota en servidores externos administrados por un proveedor de servicios. El modelo simple del almacenamiento en la nube contempla tres actores:

- El **propietario de los datos**, que externaliza una colección de documentos hacia un servidor de almacenamiento en la nube.
- El **proveedor del servicio de almacenamiento**, que es responsable de almacenar los datos de los propietarios y hacerlos disponibles a los usuarios autorizados.
- El **consumidor de los datos**, el cual realiza operaciones de consulta sobre los datos del propietario, usando para ello un servicio de búsqueda del proveedor.

## 2. Antecendentes

**1) Searchable Encryption (SE):**
Es una técnica criptográfica que permite al propietario almacenar datos cifrados en servidores externos poco confiables y garantizar a aquellos usuarios autorizados la posibilidad de realizar operaciones de búsqueda [1].

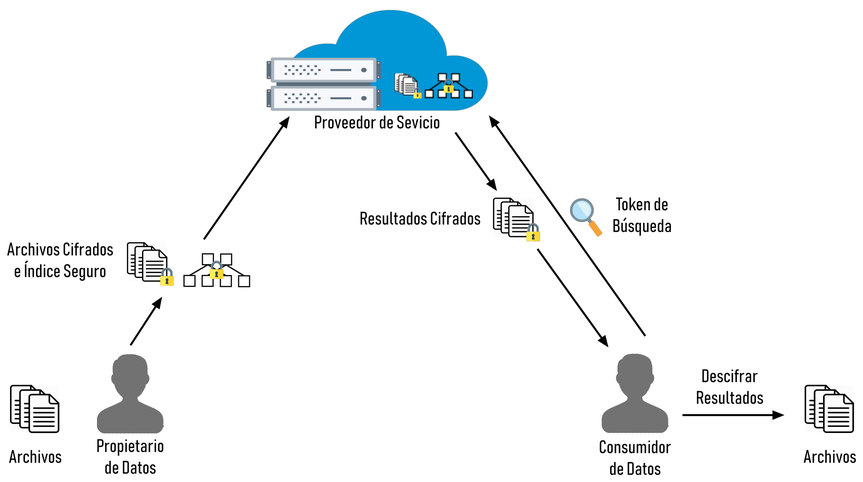


Figura 1: Modelo básico de operación SE.

**2) Attribute-Based Searchable Encryption (ABSE):**
Es un esquema fundamentado en el Cifrado Basado en Atributos (ABE), por lo que es posible lograr autenticación, autorización y transmisión seguras que garantizan la privacidad de la información en entornos complejos como el cómputo en la nube [2].

## 3. Problemática

Si bien en la literatura existen algunos esquemas SE propuestos, también es cierto que éstos no han sido completamente estudiados ni evaluados para ser usados en escenarios reales.

Aunque de forma teórica ABSE cumple con los requerimientos de seguridad y garantiza las capacidades de búsqueda del proveedor del servicio de almacenamiento en la nube, existen los siguientes inconvenientes:

- Los requerimientos funcionales de ABSE en escenarios de almacenamiento en la nube no se han identificado explícitamente.
- No se cuenta con esquemas ABSE con construcciones que permitan implementar niveles de seguridad mayores a 128-bits.
- No se han identificado construcciones ABSE que se hayan evaluado experimentalmente en escenarios de almacenamiento y compartición de datos en la nube en donde se haya demostrado su eficiencia.

## 4. Objetivo general

Definir y evaluar un esquema de cifrado de datos con capacidades de búsqueda bajo el enfoque ABSE, factible de utilizarse en escenarios de almacenamiento y compartición de datos en la nube.

## 5. Solución propuesta

Diseñar e implementar un esquema ABSE que opere bajo el modelo de ataque semi-honesto pero curioso en escenarios reales de almacenamiento y compartición de datos en la nube, de tal forma que cumpla con los requerimientos funcionales mínimos en dichos entornos y cubra aspectos no funcionales, como nivel de seguridad y eficiencia.

Metodología:

- **Fase 1** – Definición de los requerimientos esenciales de un esquema ABSE.
- **Fase 2** – Construcción del esquema propuesto.
- **Fase 3** – Diseño de pruebas y evaluación del rendimiento del esquema.

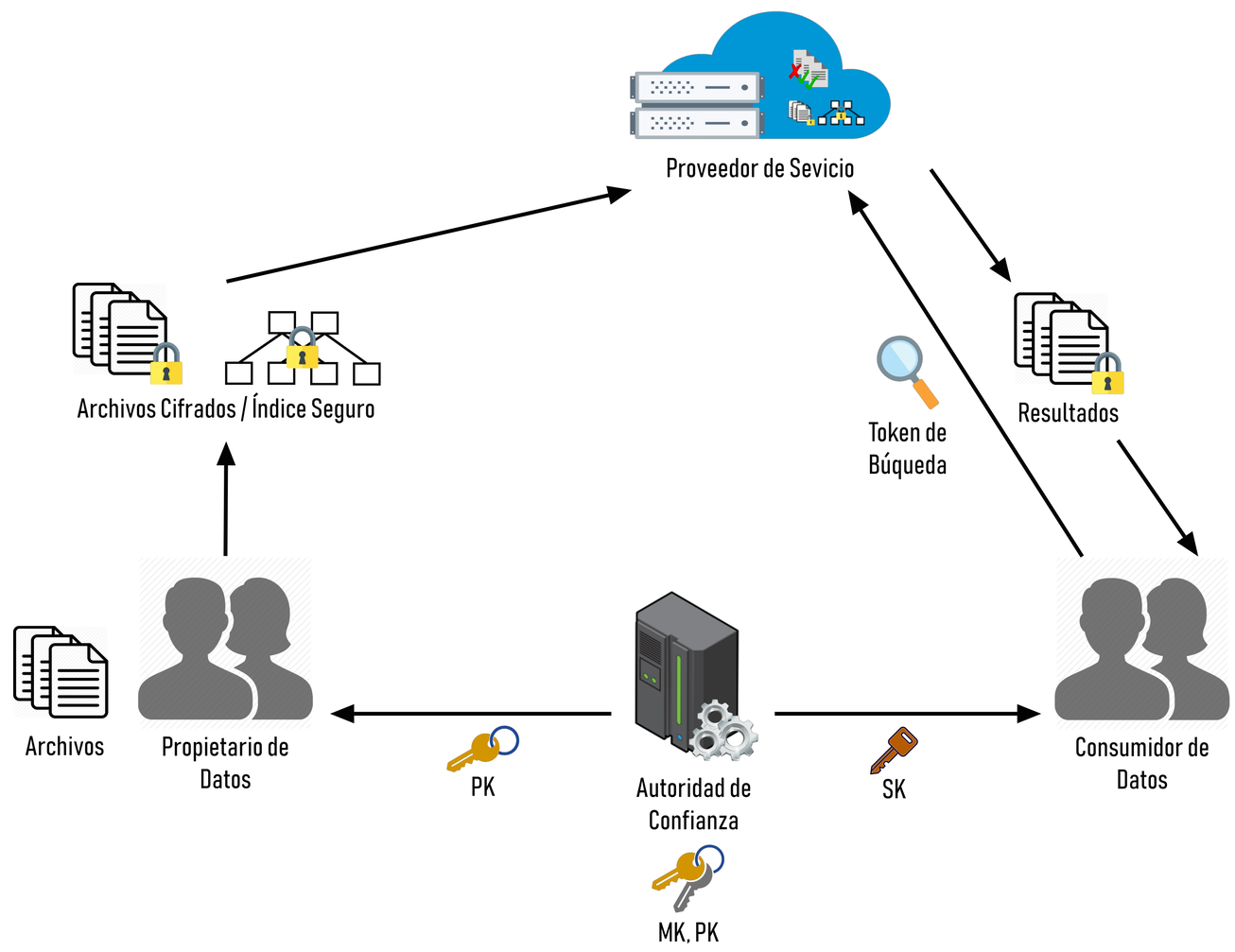


Figura 2: Modelo de operación del esquema de cifrado de datos con capacidades de búsqueda.

## 6. Contribuciones

**Contribución tecnológica**:

- Un nuevo esquema de seguridad que opere en el modelo *semi-honesto pero curioso* utilizando emparejamientos bilineales asimétricos.

**Contribución científica y académica**:

- Evaluación experimental del esquema que demuestre la viabilidad de su uso en entornos reales.
- Prototipo experimental que permita evaluar nuevas técnicas criptográficas y de recuperación de información en el entorno del almacenamiento en la nube.

## Bibliografía

[1] Yunling Wang, Jianfeng Wang, Xiaofeng Chen.
Secure searchable encryption: A survey.
*Communications and Information Networks*, Vol. 1( No. 4):52–65, 12 2016.

[2] P. Praveen Kumar, P. Syam Kumar, and P.J.A. Alphonse.
Attribute based encryption in cloud computing: A survey, gap analysis, and future directions.
*Network and Computer Applications*, 108:37–52, 04 2018.

[1] *Este proyecto de tesis de maestría se realiza en el marco del proyecto 281565 del Fondo de Investigación para la Educación SEP-CONACYT, bajo la dirección del Dr. Miguel Morales Sandoval.*