UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO
ESCUELA DE POST GRADO
MAESTRÍA EN CIENCIAS MENCIÓN INFORMÁTICA

TESIS

CONSULTAS DE DISYUNCION SOBRE DATOS CIFRADOS HOMOMORFICAMENTE EN BASE DE DATOS RELACIONALES

PARA OBTENER EL GRADO ACADÉMICO DE:
MAESTRO EN CIENCIAS MENCIÓN INFORMÁTICA

PRESENTADO POR:
BR. RAUL HUILLCA HUALLPARIMACHI
ASESOR:
MGT. JAVIER ARTURO ROZAS HUACHO

CUSCO – PERÚ
2020

Resumen

Podemos afirmar, que toda la información almacenada en las diferentes bases de datos se encuentran expuesto a agentes internos e externos, los mismos, con frecuencia no tienen las mismas intenciones que los administradores i/o propietarios de dicha información, mucho mas aun cuando esta base de datos se encuentra tercerizada. En este sentido, los responsables de la administración de dichos gestores hacen uso de herramientas de hardware y software para poder resguardar sus datos,es con este propósito entonces que los administradores, dentro de un mecanismo de seguridad, hacen uso del cifrado de toda o parte de la información contenida en una base de datos para cumplir sus objetivos de confidencialidad.

Por otra parte, tanto una base de datos cifrada al igual que una base de datos de texto en claro(sin cifrar), tienen que garantizar la ejecución exitosa de consultas cotidianas y frecuentes a la misma, esto para no comprometer los datos, y dentro de estas podemos mencionar consultas de selección, comparación, procesos aritméticos etc, aclarando que todos estos procesos se tienen que realizar sobre datos cifrados y no sobre datos sin cifrar como es el caso cotidiano. En este sentido, nos trazamos el objetivo de como realizar este tipo de procedimiento para las consultas de disyuncion los cuales se pueden realizar con naturalidad cuando la consultas se realiza en texto claro.

Por las consideraciones anteriores,se expone la existencia de los sistemas de cifrado homomorfico, los mismos que nos permiten realizar diferentes operaciones sobre datos cifrados sin comprometer el cifrado original. En este sentido, un esquema de cifrado homomorfico conserva la estructura y operaciones para los diferentes procesos, cuyos resultados de estas operaciones son equivalente ya sea que se realicen en datos cifrados o en texto plano.

Un cifrado asimétrico hace uso de la clave publica del receptor para el envió seguro de mensajes y es la persona que recibe el mensaje la única que conoce la clave privada. Las consultas de disyuncion conocidas también como “or” no presentan complejidad alguna en su comprensión y ejecución en texto plano, el mismo se hace presente cuando lo realizamos en una base de datos cifrada mas aun cuando deseamos hacer el proceso de descifrado una sola vez. Hecha esta observación, este objetivo se logra haciendo uso de las estructuras algebraicas de homomorfismo de anillos, el cual nos permite generar un dominio de números especiales y posteriormente hacer un cifrado asimétrico de estos, para así con este conjunto de datos poder operar sobre datos encriptados y ya al resultado final hacer el proceso de descifrado con la clave privada. En este orden de ideas se resume, que los resultados obtenidos son equivalentes y semejantes a los que se realizan sobre datos en texto claro.