TRABAJO PRÁCTICO 8

Fundamentos y Desafíos Emergentes en la Seguridad de Bases de Datos

Alumno: Ignacio Figueroa – 45.406.120

Tecnicatura Universitaria en Programación – UTN

Materia: Base de Datos I

Comisión: 8

1. Explorando el Cifrado Homomórfico para la Protección de Datos en Uso

¿Qué es el cifrado homomórfico?

El **cifrado homomórfico** es una técnica de criptografía que permite **realizar operaciones sobre datos cifrados sin necesidad de descifrarlos previamente**. Esto significa que un servidor puede procesar información sin acceder realmente al contenido original, manteniendo la privacidad y seguridad incluso durante el procesamiento.

A diferencia del cifrado tradicional, que solo protege datos en reposo o en tránsito, el cifrado homomórfico protege los **datos en uso**, es decir, mientras están siendo manipulados o analizados en memoria.

Principio fundamental y diferencia con técnicas tradicionales

El principio clave del cifrado homomórfico es que ciertas operaciones matemáticas (como sumas o multiplicaciones) realizadas sobre los datos cifrados producen un resultado que, al ser descifrado, coincide con el que se obtendría si las operaciones se hubieran aplicado directamente sobre los datos sin cifrar.

Tipo de protección	Tradicional	Homomórfico
Datos en reposo	Sí	Sí
Datos en tránsito	Sí	Sí
Datos en uso	No	**Sí**

Esto lo convierte en una herramienta clave para escenarios donde la información sensible debe procesarse sin exponerla.

Ventajas del cifrado homomórfico

1. **Privacidad total durante el procesamiento:** los datos nunca se descifran, reduciendo el riesgo de filtraciones.
2. **Mayor seguridad en entornos de nube:** permite delegar cálculos a terceros sin comprometer información confidencial.

Desafíos y limitaciones

1. **Alto costo computacional:** los algoritmos homomórficos son mucho más lentos que el cifrado tradicional.
2. **Complejidad técnica:** su implementación requiere experiencia avanzada en criptografía y ajustes específicos para bases de datos a gran escala.

Aplicaciones potenciales

1. **Análisis de datos sensibles en la nube:** como información médica o financiera.
2. **Machine learning con privacidad:** permite entrenar modelos con datos cifrados sin acceder a la información real.

2. Técnicas de Auditoría y Monitoreo en Bases de Datos Relacionales

Propósito principal

La auditoría y el monitoreo de bases de datos tienen como objetivo:

- **Detectar actividades sospechosas o no autorizadas.**
- **Registrar eventos para análisis forense.**
- **Garantizar la integridad y disponibilidad de los datos.**
- **Cumplir con normativas legales de protección de datos.**

Actividades que deben ser monitoreadas

1. **Inicios de sesión y accesos:** quién accede, desde dónde y cuándo.
2. **Cambios en el esquema:** modificaciones en tablas, índices o procedimientos almacenados.
3. **Ejecución de consultas sensibles:** operaciones que afecten información crítica, como UPDATE o DELETE masivos.

Uso de herramientas SIEM

Los sistemas SIEM (**Security Information and Event Management**) recopilan y analizan registros de auditoría desde múltiples fuentes. Aplicados a bases de datos, permiten:

- Correlacionar eventos sospechosos.
- Detectar patrones anómalos.
- Disparar alertas tempranas.
- Generar informes automáticos para cumplimiento normativo.

Esto mejora significativamente la detección de incidentes y reduce los tiempos de respuesta.

Cumplimiento legal y normativo

Las auditorías son esenciales para cumplir con:

- **Ley 25.326 (Argentina):** exige proteger datos personales mediante medidas técnicas y organizativas.

- **RGPD (Unión Europea):** requiere trazabilidad y control de acceso sobre información sensible.

El monitoreo permite demostrar que se aplican controles adecuados, asegurando transparencia y responsabilidad en el manejo de datos.

3. Estrategias de Respaldo y Recuperación para la Resiliencia de Bases de Datos

Importancia fundamental

Las estrategias de respaldo y recuperación aseguran:

- **Disponibilidad continua de los datos.**
- **Protección frente a fallos, ataques o corrupción.**
- **Minimización del impacto ante incidentes.**

Sin un plan de respaldo adecuado, una organización puede enfrentar pérdidas irreversibles de información y consecuencias operativas y financieras graves.

Tipos de respaldo

1. Respaldo completo

Copia íntegra de toda la base de datos.
Se aplica cuando: se requiere un punto de restauración sólido.
Desventaja: consume mucho espacio y tiempo.

2. Respaldo diferencial

Almacena solo los cambios desde el último respaldo completo.
Ventaja: más rápido que uno completo.
Desventaja: su tamaño crece hasta el próximo respaldo completo.

3. Respaldo incremental

Guarda los cambios desde el último respaldo de cualquier tipo.
Ventaja: ocupa poco espacio y es rápido.
Desventaja: la restauración es más lenta porque requiere aplicar varios incrementos.

4. Respaldo del registro de transacciones

Conserva cada transacción realizada.
Uso principal: restauraciones punto en el tiempo (PITR).

Regla 3-2-1

La regla 3-2-1 establece:

- **3 copias** de los datos (1 original + 2 copias).
- **2 tipos de almacenamiento diferentes** (por ejemplo: disco y cinta, o SSD y HDD).
- **1 copia fuera del sitio** (offsite o en la nube).

Esto protege contra:

- Fallas físicas.
- Robos.
- Ransomware.
- Desastres naturales.

RPO, RTO y pruebas de recuperación

- **RPO (Recovery Point Objective):** cantidad máxima de datos que una organización puede permitirse perder.
- **RTO (Recovery Time Objective):** tiempo máximo aceptable para restaurar el servicio.

Un plan de respaldo debe estar alineado con ambos objetivos.

Además, es fundamental:

- **Probar periódicamente** los procedimientos de recuperación.
- **Documentar paso a paso** el proceso para evitar errores en momentos críticos.