Enabling Efficient Verifiable Fuzzy Keyword Search Over Encrypted Data in Cloud Computing

Laura Mambrilla Moreno

Grado en Ingeniería Informática de la Universidad de Alcalá
laura.mambrilla@edu.uah.es

Resumen. El cifrado de búsqueda puede ayudar al usuario de datos a recuperar de forma selectiva los documentos cifrados a través de datos cifrados en la nube mediante una búsqueda basada en palabras clave. La mayoría de los esquemas de cifrado de búsqueda existentes solo se centran en la búsqueda de palabras clave exactas, por lo que, cuando se cometen errores ortográficos, no devuelven el resultado de interés. Para abordar estos problemas, se propone un nuevo esquema de búsqueda de palabras clave difusas verificables sobre datos encriptados en la nube. Para conseguirlo, se propone un esquema de búsqueda de palabras clave exactas verificables (VEKS), que se ampliará posteriormente con uno de palabras clave difusas verificables (VFKS). Tras el análisis de seguridad y la evaluación de experimentos, se demuestra que los esquemas propuestos son seguros y eficientes.

Keywords: Computación en la nube, cifrado de búsqueda, búsqueda de palabras clave exactas verificables, búsqueda de palabras clave difusas verificables.

1 Introducción

Debido a la conveniencia y flexibilidad de la computación en la nube, cada vez más propietarios de datos prefieren almacenarlos en el servidor de la nube para reducir el espacio de almacenamiento y ahorrar la sobrecarga de administración en las máquinas locales.

Pero usuarios no autorizados pueden tener acceso a ellos, por lo que es de importancia inminente proteger la privacidad de los datos en la nube. Por ello, el propietario de los datos los encripta antes de cargarlos en el servidor de la nube. Para obtenerlos de vuelta, el usuario proporciona la clave de descifrado y la palabra clave a consultar al servidor de la nube. El servidor descifra los datos cifrados y realiza una operación de búsqueda sobre el texto sin formato.

Los esquemas de cifrado de búsqueda permiten al usuario de datos recuperar selectivamente documentos cifrados almacenados en el servidor de la nube mediante una búsqueda basada en palabras clave.

2 Resultados

Se propone un esquema de búsqueda de palabras clave exactas verificables (VEKS), que logra la operación de búsqueda en una ronda de comunicación. Para detectar el comportamiento malicioso del servidor en la nube, se genera una etiqueta de autenticación para cada palabra clave. Una vez que el servidor en la nube devuelve el resultado de la búsqueda, el usuario de datos puede verificar la validez del resultado de la búsqueda según la etiqueta de autenticación. Con este método se puede detectar si los documentos devueltos desde el servidor en la nube han sido modificados o eliminados.

Basado en el esquema VEKS, se propone un esquema de búsqueda de palabras clave difusas verificables (VFKS). En el esquema VFKS, para construir el índice de manera eficiente, se adoptan las listas enlazadas como estructura del índice. Se almacena un conjunto de palabras clave difusas en lugar de una sola palabra clave difusa en un nodo, y solo se genera un vector de índice para cada conjunto en lugar de para cada palabra clave difusa. Este método puede reducir considerablemente el espacio de almacenamiento. Además, no es necesario construir el conjunto de palabras clave difusas para la palabra clave consultada en el diseño, lo que reduce el coste de cálculo y mejora la eficiencia de búsqueda.

A través del análisis de seguridad y la evaluación experimental en un gran conjunto de datos del mundo real, se demuestra que los esquemas propuestos son seguros y eficientes.

3 Conclusión

Se propone en primer lugar un esquema de búsqueda de palabras clave exactas verificables (VEKS) sobre datos encriptados en la nube. Posteriormente se construye un esquema de búsqueda de palabras clave difusas verificables (VFKS) basado en el esquema VEKS. Para mejorar la eficiencia, se emplean listas enlazadas como estructura de índice segura.

En comparación con los esquemas existentes, los esquemas propuestos logran una verificación más eficiente de los resultados de búsqueda. Proporcionan un análisis de seguridad detallado de los esquemas propuestos.

La evaluación exhaustiva de los experimentos indica que son muy eficientes.

4 Bibliografía

X. Ge, J. Yu, C. Hu, H. Zhang and R. Hao, "Enabling Efficient Verifiable Fuzzy Keyword Search Over Encrypted Data in Cloud Computing", *IEEE Access*, vol. 6, pp. 45725-45739, August 2018.