

Abonnieren Sie DeepL Pro, um dieses Dokument zu bearbeiten.  
Weitere Informationen finden Sie auf [www.DeepL.com/pro](https://www.deepl.com/pro?cta=edit-document)

HealthID - Informationssicherheit

Einleitung:

Die Speicherung personenbezogener Daten in der Blockchain ist aus mehreren Gründen nicht sicher. Die Blockchain ist so konzipiert, dass sie unveränderlich ist, was bedeutet, dass Daten, die einmal in ihr gespeichert sind, nicht mehr geändert oder gelöscht werden können. Dies ist ein grundlegendes Merkmal für die Gewährleistung der Integrität von Aufzeichnungen. Wenn personenbezogene Daten jedoch unwiderruflich gespeichert werden, kann ein Fehler oder eine Verletzung der Privatsphäre nicht korrigiert werden.

Anstatt personenbezogene Daten direkt auf der Blockchain zu speichern, ist es sicherer, sie zu nutzen, um Zugriffsberechtigungen zu verwalten und die gemeinsame Nutzung personenbezogener Daten zu kontrollieren, die sicher auf externen Systemen gespeichert sind, wobei strenge Datenschutzvorschriften eingehalten werden. Dies trägt dazu bei, die Privatsphäre des Einzelnen zu schützen und gleichzeitig die Vorteile der Technologie zu nutzen.

In unserem Projekt befassen wir uns mit den medizinischen Daten des Benutzers, daher müssen wir diese Informationen behandeln und die Privatsphäre des Benutzers garantieren, und erst dann ihre medizinischen Daten in die Datenbank eingeben.

1. die Identifizierung sensibler Daten:

In der Anwendung lädt der Nutzer seine medizinische Untersuchung hoch. Nach dem Hochladen muss die Datei in Text umgewandelt werden, und OCR (Optical Character Recognition) wird verwendet, um sensible Informationen zu analysieren und zu suchen (nur nicht sensible Daten oder pseudonymisierte Informationen sollten auf der Blockchain gespeichert werden). Personenbezogene Informationen, die für den Zweck der Transaktion auf der Blockchain (Freigabe des Zugriffs auf medizinische Daten) nicht wesentlich sind, werden entfernt und mit Hilfe von Anonymisierungstechniken zentral gespeichert.

2. Physische Trennung der Daten:

Eine Möglichkeit, die Daten zu trennen, besteht darin, verschiedene Arten von Datensätzen oder Datenstrukturen zu erstellen, z. B.: **Metadatensatz,** dieser Datensatz enthält Kontrollinformationen und Metadaten über die Datei, wie eindeutige Kennungen, Erstellungsdaten, Dokumenttypen und alle anderen nicht sensiblen Informationen, die nützlich sind, und **Inhaltsdatensatz,** dieser Datensatz enthält den eigentlichen Inhalt der Dokumente, wobei die sensiblen Daten jedoch anonymisiert werden. Dies bedeutet, dass personenbezogene Informationen wie Namen und Identifikationsnummern durch Pseudonyme ersetzt werden.

3. Querverweis:

Um sicherzustellen, dass der Metadatensatz und der Inhaltsdatensatz miteinander verbunden sind, können Sie einen eindeutigen Bezeichner (z. B. einen Hash-Code oder eine ID) verwenden, der diese Datensätze miteinander verknüpft. Auf diese Weise können Sie bei Bedarf sensible Daten abrufen, allerdings nur, wenn die entsprechende Berechtigung erteilt wurde.

4. Zugangskontrolle:

Wir implementieren ein Zugangskontrollsystem mit intelligenten Verträgen, um sicherzustellen, dass nur autorisierte Parteien auf sensible Daten zugreifen können. So können Sie detaillierte Berechtigungen festlegen, wer diese Daten sehen oder nutzen darf.

5. Auditing und Rückverfolgbarkeit:

Wir zeichnen alle Transaktionen und Aktivitäten im Zusammenhang mit dem Datenzugriff und der Datennutzung auf, einschließlich der erteilten und widerrufenen Genehmigungen. Dies ermöglicht die Rückverfolgbarkeit und eine vollständige Historie der Interaktionen mit sensiblen Daten.

6. Einhaltung von Vorschriften:

Alle Praktiken der Anonymisierung, Pseudonymisierung und Datenspeicherung müssen den Datenschutzbestimmungen entsprechen, wie z. B. der GDPR in der Europäischen Union.

7. Benutzerschulung:

Die Nutzer müssen darüber aufgeklärt werden, wie ihre Daten geschützt sind und wie sie den Zugang zu diesen Informationen kontrollieren können, was in regelmäßigen Abständen geschehen kann.