3D-Druckplattform: Datensicherheit

1. Generelle Verschlüsselung und Backup

Die Datenströme sind während des Versendens an das Backend mit einem SSL Labs A-Certificate Schlüssel gesichert. Die auf den Amazon Servern gelagerten Dateien sind serverseitig verschlüsselt. Der Zugang zu den Amazon Servern ist mittels Multifactor Authentication gesichert.

Rapid3D vertraut auf die AWS Replikations- und Backup-Systeme. Die eigene SQL-Datenbank erstellt alle 24 Stunden ein Backup. Da Rapid3D sichere Web Frameworks (Django, Spring) benutzt, sind klassische Schwachstellen wie SQL Injection, Cross-Site-Scripting und Cross-Site Request Forgery durch das Design dieser Frameworks nicht möglich und damit ausgeschlossen.

2. Verschlüsselung bei Fileupload

Während der File-Bearbeitung ist die Datei für den User unverschlüsselt. Sobald die Datei auf das Backend hochgeladen wird, ist die Datei mit einem SSL A-Certificate Schlüssel gesichert. Die CAD-Datei befindet sich nun verschlüsselt auf dem EC2-Server. Hier wird sie entsprechend bearbeitet und die Meta-Daten extrahiert. Das CAD-Modell wird verschlüsselt auf dem S3-Server gelagert und die Metadaten auf dem RDS Server gespeichert, die Datensätze sind serverseitig verschlüsselt.

3. Einsicht der 3D-Daten

Der EC2-Server fragt die Rechte des Users (nur Kunde & Rapid3D) zur Einsicht der 3D-Datei ab. Bei berechtigtem Zugriff werden die Metadaten aus dem RDS-Server und das CAD-Modell aus dem S3-Server verschlüsselt über das Backend an den Benutzer weitergeleitet.

4. Download der 3D-Daten

Der EC2-Server fragt die Rechte des Users zum Download der 3D-Datei ab (Kunde, Rapid3D & Druckdienstleister). Bei berechtigtem Zugriff lädt der EC2-Server das verschlüsselte CAD-Modell von dem S3-Server herunter. Nun schickt der EC2-Server das verschlüsselte Modell an den Nutzer.

5. Zusätzliche Aktionen

Die folgende Beschreibung findet Anwendung auf die Fälle: Einen Account anlegen, ein 3D-Projekt kommentieren, eine Anfrage stellen, Statusinformationen updaten. Der Nutzer stellt eine verschlüsselte Anfrage an den EC2-Server. Der EC2-Server greift auf die RDS-Datenbank zu, um die Anfrage zu verarbeiten und eine Antwort zu erstellen.

6. Zugriffe

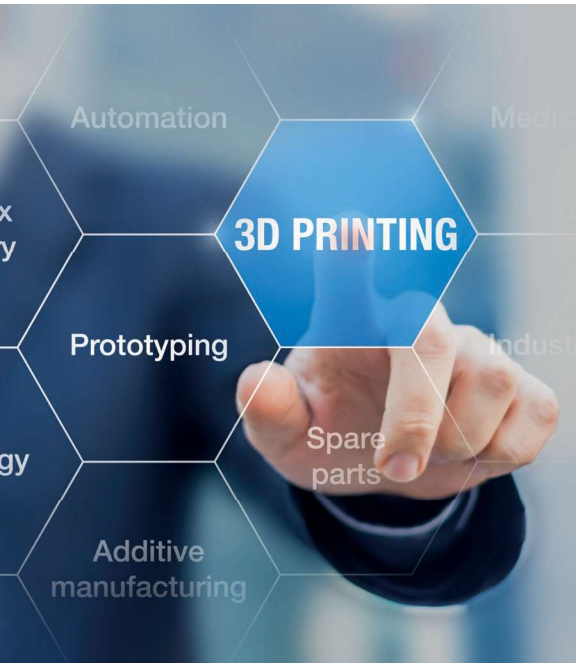
Bei der Erstellung eines Accounts wird auf folgende Daten zugegriffen: E-Mail-Adresse, Passwort, Name und Nachname, Name des Unternehmens, Adresse, Land, Telefonnummer, IP-Adresse. Beim Hochladen eines 3D-Files durch den User wird auf folgende Daten zugegriffen: 3D-Modell, IP-Adresse, Metadaten.

Folgende Informationen werden als Metadaten aus dem CAD-Modell extrahiert: Filename, Filegröße, Dimension, Volumen, Oberfläche, Druckbarkeit, IP-Adresse.

Beim Kommentieren von 3D-Projekten wird auf folgende Daten zugegriffen: User-ID, Kommentar vom User, IP-Adresse. Beim Aufgeben einer Bestellung wird auf folgende Daten zugegriffen: User-ID, 3D-Modell-ID, Lieferanschrift, Rechnungsadresse, Zusätzliche [GF5], [DP6], [DP7] Rechnungsinformationen.

Thomann

Ansprechpartner



Joachim Janz
Telefon: +49 (0) 8382 7058-372
E-Mail: j.janz@thomann.biz

Thomann GmbH
Heuriedweg 34-36
88131 Lindau / Bodensee

Schauen Sie unter **www.thomann.biz** !