const jwt = require("jsonwebtoken");

const User = require("../models/signup"); // Import the User model

const authenticateToken = async (req, res, next) => {

    console.log("🔗 Authenticating token...");

    // Get token from cookies or Authorization header

    const token = req.cookies.token || req.headers.authorization?.split(" ")[1];

    console.log("🔑 Token:", token);

    if (!token) {

        console.log("❌ No token provided.");

        return res.status(401).json({ message: "Access denied. No token provided." });

    }

    try {

        console.log("🔍 Verifying token...");

        const decoded = jwt.verify(token, process.env.JWT\_SECRET);

        console.log("✅ Token verified successfully.");

        console.log("👤 Decoded user data:", decoded);

        // Fetch the user from the database to get additional fields (e.g., yourname)

        const user = await User.findById(decoded.userId);

        if (!user) {

            console.log("❌ User not found in the database.");

            return res.status(403).json({ message: "User not found." });

        }

        console.log("👤 User data from database:", user);

        // Attach user data to the request object

        req.user = {

            userId: user.\_id,

            email: user.email,

            yourname: user.yourname, // Add the user's name

            role: user.role

        };

        next();

    } catch (error) {

        console.error("❌ Token verification failed:", error.message);

        res.status(403).json({ message: "Invalid or expired token." });

    }

};

module.exports = { authenticateToken };