1)Difference b/w JSON and XML

Feature	JSON	XML
Syntax Simplicity	Uses a straightforward, easy-to-read syntax that resembles JavaScript object literals. It uses curly braces {} for objects and square brackets [] for arrays.	Uses a more complex and verbose syntax with tags to enclose data. Each element has a start tag **<tag>** and an end tag **</tag>**, with attributes contained within tags.
Readability	Generally easier to read and write due to its concise syntax.	Can be harder to read because of the verbose tag structure.
Data Representation	Represents data as key-value pairs, arrays, and nested objects.	Represents data with nested elements, attributes, and text nodes.
Data Types	Supports a limited set of data types: strings, numbers, booleans, arrays, and objects.	Does not inherently support data types. All data is treated as text, and data typing must be handled by schemas (e.g., XSD).
Usage	Commonly used in web applications, particularly with JavaScript and APIs	Widely used in a variety of applications, including web services (SOAP), document storage, and configuration files
Comments	Does not support comments within the data.	Supports comments using the **<!-- comment -->** syntax

Example	{
	"students": {
	"id": 6648,
	"name": "Akshitha",
	"GPA": 8.7
	}
	}
		<student1>
		<id>6648</id>
		<name>Akshitha</name>
		<GPA>8.7</GPA>
		</student1>

2)Difference b/w authentication and authorization?

Aspect	Authentication	Authorization
Definition	The process of verifying the identity of a user or system.	The process of determining the permissions or access levels of an authenticated user or system.
Purpose	To ensure that the user or system is who they claim to be.	To determine what resources and actions the authenticated user or system is allowed to access.
Primary Question	"Who are you?"	"What are you allowed to do?"
Process	Typically involves verifying credentials like username/password, biometric data, or tokens.	Involves checking the permissions associated with the authenticated identity against the requested resources or actions.
When It Occurs	Occurs before authorization.	Occurs after authentication.
Data Used	Usernames, passwords, OTPs, biometric data, security tokens.	Access control lists (ACLs), roles, policies, permissions.
Outcome	Confirms the identity of the user or system.	Grants or denies access to specific resources or actions.
Scope	Identity verification.	Access control and permissions management.
Examples	Logging in with a username and password, fingerprint scan.	Granting access to a file, allowing the user to perform administrative tasks.