| **Feature** | **JSON** | **XML** |
| --- | --- | --- |
| Syntax | Uses key-value pairs and arrays | Uses tags to define elements and attributes |
| Readability | Generally more concise and easier to read | Can be verbose, especially for large datasets |
| Data Types | Supports fewer data types (strings, numbers, Booleans , arrays, objects) | Supports a wider range of data types (text, numbers, dates, custom data structures) |
| Parsing | Faster and easier to parse due to simpler syntax | Can be more resource-intensive to parse, especially for large documents |
| Usage | Widely used in web services, APIs, modern web applications | Historically used in various domains such as web services, configuration files, document markup |
| Schema | No built-in schema, but schemas can be defined using JSON Schema | Supports XML Schema Definition (XSD) for formal schema definitions |

# AUTHORIZATION VS AUTHENTICATION

| **Feature** | **Authentication** | **Authorization** |
| --- | --- | --- |
| Definition | Verifies the identity of a user or entity accessing a system or resource | Determines what actions and resources a user or entity is allowed to access |
| Purpose | Ensures that the user is who they claim to be | Controls access to specific resources or functionalities |
| Process | Verifies credentials (e.g., username/password, token) | Checks permissions against the user's identity or attributes |
| Example | Logging into a website with a username and password | Accessing a file after being granted permission by an admin |
| Scope | Typically focuses on user identity and authentication methods | Concerned with permissions, roles, and access control rules |
| Granularity | Usually binary (authenticated or not authenticated) | Can be granular, specifying different levels of access for different resources or actions |
| Dependency | Precedes authorization; users must authenticate before being authorized | Relies on authentication to determine what resources or actions are available to a user |
| Outcome | Provides access to the system or application | Grants or denies access to specific resources or functionalities |
| Example Technology | Username/password authentication, biometric authentication | Role-based access control (RBAC), access control lists (ACLs) |