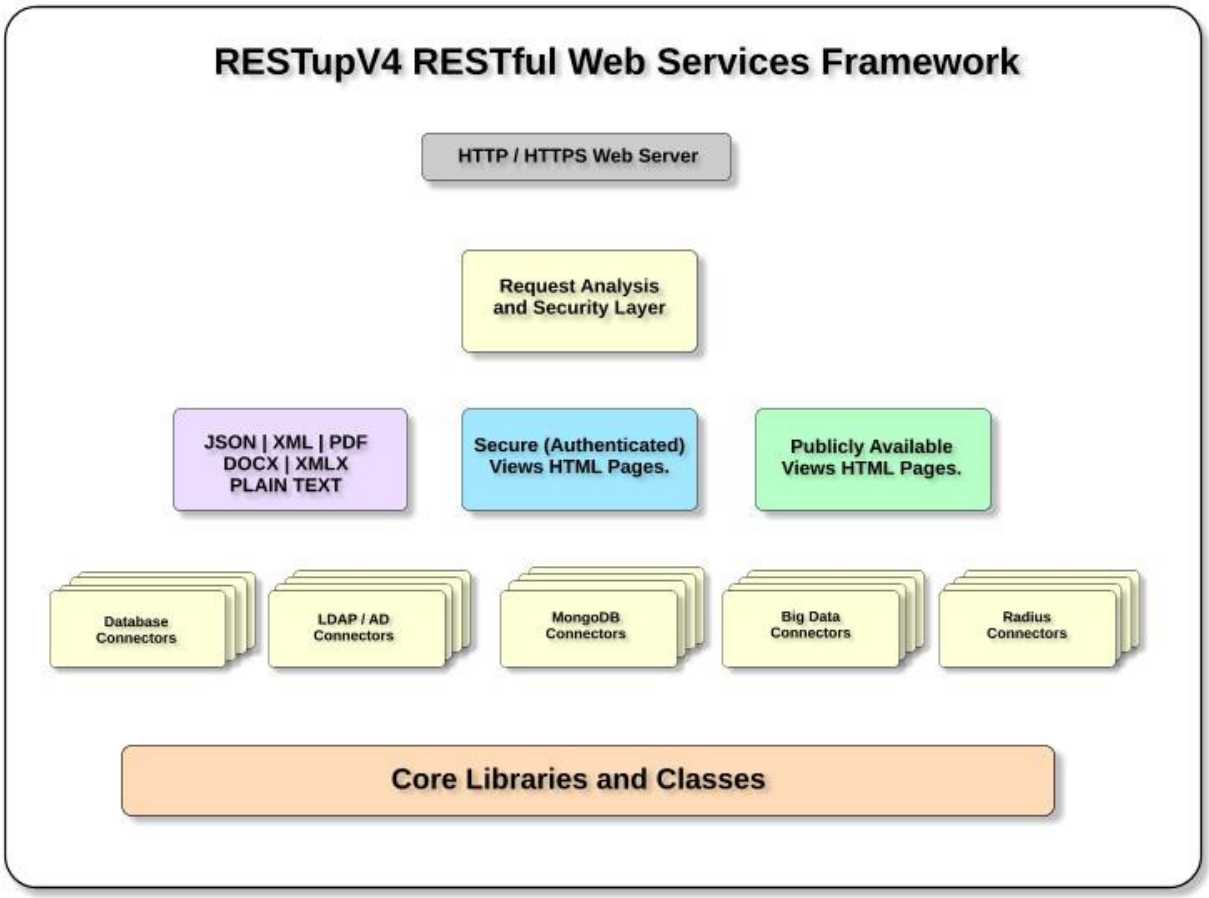
RESTupV4 – Restful Web Services Framework.

The RESTupV4 Web Services Framework is light weight, fast, scalable and highly extensible with pre-built connectivity to all major Databases, Document Data Stores and Big Data (Name / Value Pair) store plus Cloud and Local Server Filesystem storage. The diagram below shows the key components of the RESTupV4 Framework.



In addition to the capabilities listed above, the Framework also utilises several “Best of Breed” open source applications and tools for the efficient production of Web Content including:

- Smarty 3 Template Engine.
- Bootstrap CSS Framework.
- jQuery and Angular.js Javascript frameworks.

The combination of all of these features provides a platform architecture which may be scaled horizontally, reused for multiple different sites concurrently, whilst enabling rapid development and deployment on Linux Server Fabrics including Hybrid Cloud, AWS, OpenStack, Cloud OS, vmWare, Citrix Xen, Rackspace on Debian, RedHat, Centos and Suse distributions.

Configuration and Security within RESTup4:

Granular security is a built-in feature of RESTup4, on a per network, per server, per method, per host and role based levels for authenticated web application users, access may be allowed or denied by setting the appropriate values in the server section of the configuration files.

As an example consider the following excerpt from a serverConf.json main server configuration file:

```
"server":
{
    "hostsAllowed":"*",
    "hostsDenied":[],
    "clientKeys":[],
    "authTokens":["b-9_jy9pfug7BZ2w8WMfW.AF_Mr0lFgx"],
    "requestProtocols":["https","http"],
    "requestMethods":["GET","POST","PUT","DELETE"],
    "debugLevel":0
}
```

The resulting security policy for this server is to allow All hosts and deny no hosts, no specific client keys have been defined and all hosts which send a request header containing the configured authentication token: "authToken:b-9_jy9pfug7BZ2w8WMfW.AF_Mr0lFgx" are allowed to make REST requests without requiring user authentication. This feature enables servers within a corporate network to communicate with other RESTup4 servers without requiring user credential level authentication for each request resulting in transparent trusted connections between servers. The remaining parameters determine which protocols and methods are accepted and may be used to constrain requests to http and/or https, with GET, POST, PUT and DELETE methods. The final parameter here sets the global debugLevel for the server which when 0 turns off debugging, other integer values are used for granular debugging where:

0 - No Debug info.
1 - configuration variables.
2 - variable validation results.
4 - database debug info including SQL executed, timings and results.
8 - ldap debug info including queries executed, timings and results.
16 - radius debug information.
32 - output to screen and debug log.

These integer values may be summed eg: "debugLevel":7 would provide configuration variables, variable validation results and database debug info including SQL executed, timings and results in the debugLog.