How we secure our parsing data:

1. First of all we do not store any resume on our servers, as soon as the parsing is complete, its deleted. Only the filename and time of parsing is stored.
2. Randomly generated key is provided to each of our client, which is unique to every client.
3. Anti-virus scanner and app monitor implemented on each of our servers to ensure high availability and no malicious activity.
4. Firewall is implemented to allow or block IPs and ports that are not authorized.
5. Automatic blocking of IPs that can cause DDoS.
6. All the data that we need to store like user key, parsed filename are stored as **MD5 hash encrypted data**.

Measures on our web-host provider Amazon AWS:

7. **Load balancer:** It not only balances the traffic between web servers but also shields servers from outsiders, as it provides a point of access (public IP) without telling the real IPs of servers to the world. It reroutes all the queries internally.
8. Each load balancer has its own firewall to prevent any malicious activity.
9. **Web Server Monitor:** It continuously monitor each server on hardware level, to ensure security and integrity of server.

Additional Security (Optional):

SSL (https)

(Clients need to purchase this, we will implement for them)

SSL certificate ensures that the data that is being transferred between the servers are encrypted, so even if somebody can record the data being transferred, they will not be able to decrypt (read) it.

Pre requisites :

Linux Server with Apache Tomcat Installed

16GBs of RAM, Quad Core Xeon Processor (+3.0 GHz), 100GB or more as per requirement.