**PROJECT REPORT**

**ON**

**“DATA ANALYSIS USING SPLUNK ”**

**PRESENTED**

**BY**

**AYAZ SAYYAD**

**SHAIKH IMRAN SADEKH**

**REPORTED TO**

**MUDDASSIR SHAIKH**

**Abstract of the Project:**

**About Splunk**

Its used for monitoring, searching, analysin, and visualising the machine genreted data in real time. It performs capturing, indexing and correlating the real time data in a searchable container and produces graphs alert dashboard.

**Product of Splunk**

* **Splunk Enterprise**
* **Splunk Cloud**
* **Splunk light**

**Architecture of Splunk**

**Universal Forward (UF)**

It pushes data to the heavy splunk forwarder. you can install this component on both side.it only forward log data.

**Load Balancer(LB)**

It balance the load it devide the network.

**Heavy Forward(HF)**

It allow you to filter the data

**Indexet (LB)**

It used to store index data it automatically perform the indexing.eg host,source,dat e time

**Search Head(SH)**

It used to gain intelligence and perform reporting.

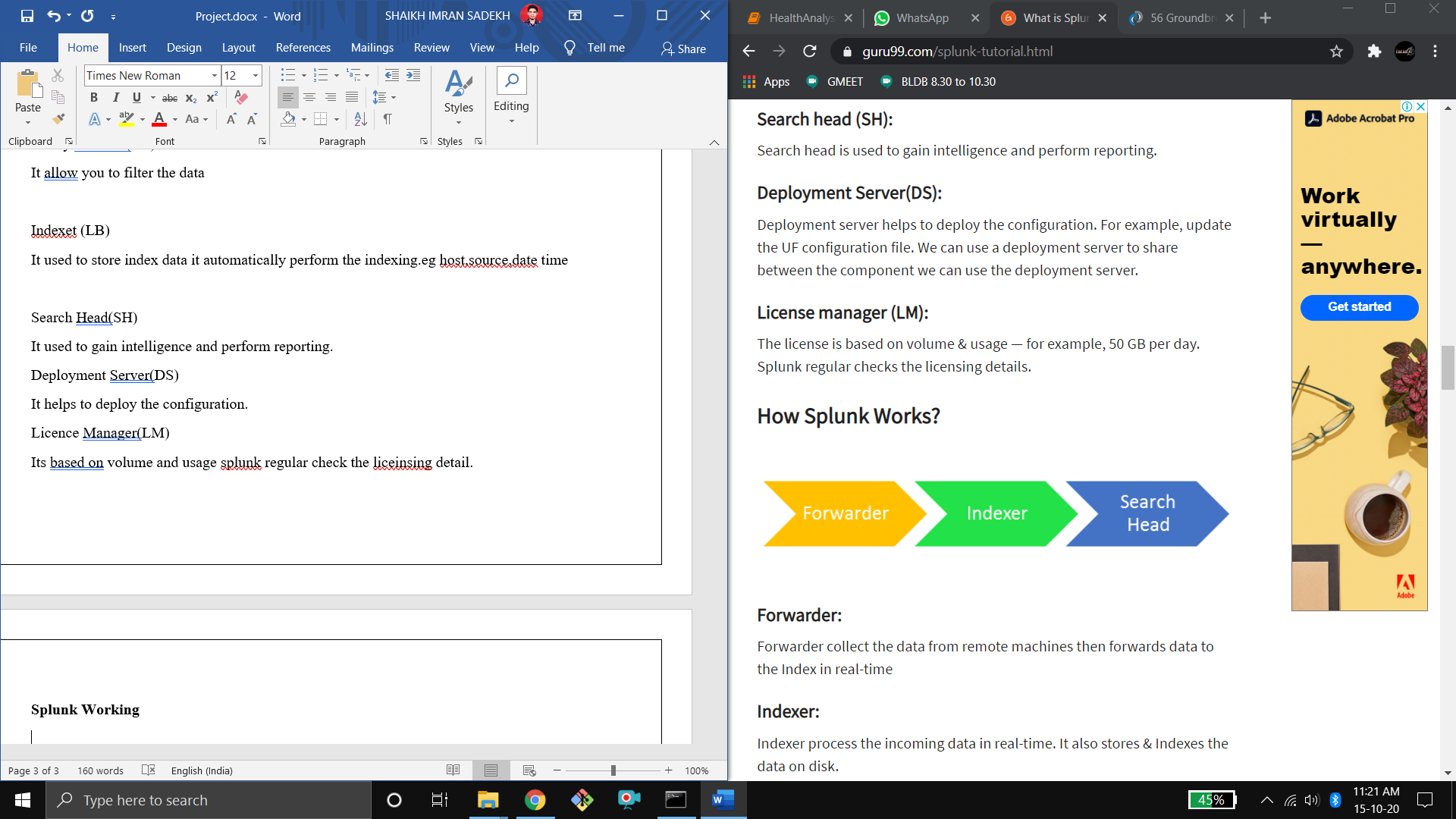
**Deployment Server(DS)**

It helps to deploy the configuration.

**Licence Manager(LM)**

Its based on volume and usage splunk regular check the liceinsing detail.

**Splunk Working**



**Forwarder**

It collect data form remote machine and forward data to the index in real time.

**Indexer**

Indexer process the incoming data in real time. Its also store and indexes the data on disk

**Search Head**

End user interact with splunk through search head. it allow user to do search analysis and visualisation.