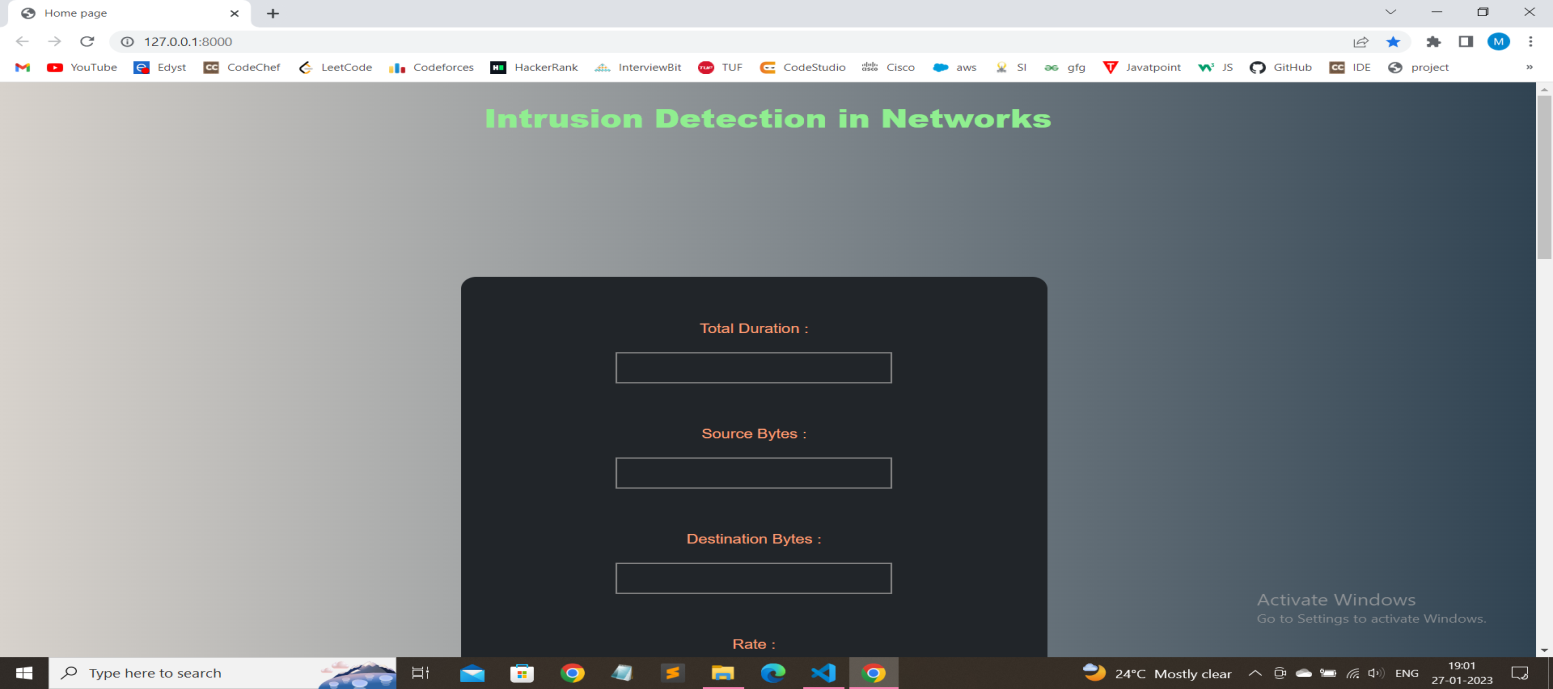
The most sensitive and important data are stored on servers, strong security is required to avoid data theft and misuse.

When an intrusion occurs in a system, an intrusion detection system (IDS) is used to identify it and alert the admin. A network and devices are inspected by an IDS for malicious activity or policy breaches. Any unlawful behaviour or violation is often recorded either centrally using a security information and event management (SIEM) system or notified to an admin. In order to discern between hostile behaviour and false alerts, a SIEM system aggregates outputs from many sources and use alarm filtering mechanisms.

In order to track traffic to and from all networked devices, intrusion detection systems (IDS) are installed at one or more strategically located locations inside the network.

Our study is on UNSW\_NB15 dataset which comprises of different attacks.



1. https://towardsdatascience.com/building-an-intrusion-detectionsystem-using-deeplearning-b9488332b321
2. https://www.codespeedy.com/intrusion-detection-model-usingmachine-learningalgorithm-in-python/
3. https://www.researchgate.net/publication/281451813\_Using\_Machine\_Learning\_in\_Netwo rks\_Intrusion\_Detection
4. https://cybersecurity.springeropen.com/articles/10.1186/s42400- 019-0038-7#availabilityof-data-and-materials
5. https://www.geeksforgeeks.org/intrusion-detection-systemusing-machine-learningalgorithms/
6. <https://www.geeksforgeeks.org/best-python-libraries-formachine-learning/>
7. <https://anderfernandez.com/en/blog/code-decision-tree-pythonfrom-scratch/>
8. <https://arxiv.org/ftp/arxiv/papers/2101/2101.0506>
9. https://www.geeksforgeeks.org/principal-componentanalysis-with-python

