**CHAPTER 5**

**CONCLUSION**

This thesis presents a detailed discussion about Cyber Attack Detection in Power System Scada Networks Using Machine Learning Techniques. During the process of this work, we simulated multiple types of power system faults – natural as well as cyber-attacks, collected relevant data from the generated data samples and analysed them using multiple machine learning techniques. Industry-standard tools like MATLAB, Simulink, Linux, Ettercap, Wireshark, Jupyter Notebooks, sklearn, pandas, numpy and more were used during this project. This further elevates the relevance of the work done.

Furthermore, a methodology was devised and proposed to simulate and investigate the occurrence as well as the impact of the different obstacles and sabotages on the system. Based on the observed results, inferences were gleaned and suggestions to counter as well as thwart the problems were proposed.

**5.1 SCOPE FOR FURTHER RESEARCH**

This thesis has a wide-ranging scope for further research as it delves into the domains of electrical engineering as well as software engineering. Smart-grid technologies are seeing increasing number of applications and that opens the distribution system to multiple types of malicious threats.

The scope for further research development in this field can be identified as follows:

* Expanding the scope of the project to incorporate multiple bus systems with differing sizes containing diverse types of buses and loads. This will lead to an even more representative dataset and help train the machine learning model in a way such that it can applied with lesser modifications.
* Incorporating a larger variety of cyber-attacks which leverage different media of attack allows the machine learning model to become more robust in detecting external interference.
* Performing the project upon a Real Time Digital System (RTDS) with relevant hardware like PLCs, RTUs, servers and attack machines will lead to more fruitful results and learnings.