CHAPTER 8

FUTURE RESEARCH DIRECTIONS

8.1 Future Research Directions

CHAPTER 8

FUTURE RESEARCH DIRECTIONS

8.1 FUTURE RESEARCH DIRECTIONS

This research contributes in addressing the challenges in the domain of insider threats, particularly in detecting and mitigating intentional and unintentional insider threats. Although, the proposed methodology provides promising results for detecting and mitigating intentional and unintentional insider threats, there is an expansion of research. Some of the possibilities of extending the research in future are given below.

- To enhance the practical applicability, future work should focus on analyzing real-time log data for detecting and mitigating insider threats in both structured and unstructured formats.
- The integration of predictive analytics with live streaming data using cloud infrastructure will allow organizations to respond preemptively to evolving threats.
- Leveraging the log data from widely used cloud service providers such as AWS, Microsoft Azure, and Google Cloud can further refine and expand the detection capabilities of the system. It assesses cloud-specific behaviors and address multi-tenancy challenges that lead to robust and scalable mitigation systems.
- Integrating deep learning and federated learning models with this research framework could lead to adaptive and privacy-preserving solutions. Such advancements will establish a comprehensive benchmark for secure enterprise practices.