CHAPTER V
CONCLUSION AND RECOMMENDATION

5.1 Conclusion

In conclusion, the research underscores the need for further exploration and refinement of the Deep Belief Network (DBN) model to enhance its role in supporting cybersecurity. The study highlights the potential of utilizing DBN methods to boost efficiency and accuracy in detecting attacks, thereby addressing vulnerabilities. The empirical findings reveal that DBN exhibits exceptional performance in predicting class differences, achieving an impressive accuracy rate of 96.10% in real-world scenarios. Additionally, collaborative approaches, combining Isolation Forest and Support Vector Machine (SVM), yield attack detection models with high accuracy rates of approximately 95.60% and 96.56%, respectively.

The precision, recall, and F1-Score values around 97.20% demonstrate the balanced capacity of collaborative models to efficiently recognize and capture positive events. The comparable AUC values of 0.95 across models further affirm the reliable discrimination abilities of these collaborative techniques. In summary, the study concludes that DBN, particularly when employed in collaboration, emerges as an effective attack detection tool for. This contribution significantly enhances cybersecurity measures, addressing the identified weaknesses in the initial problem statement.

This research affirms the effectiveness of the Deep Belief Network (DBN) as a robust attack detection method, demonstrating commendable levels of accuracy, precision, and recall rates. The integration of DBN with other methodologies, such as Isolation Forest and Support Vector Machine (SVM), emerges as a strategic approach to enhance overall performance in attack detection. Particularly, the

collaborative model of DBN with Isolation Forest exhibits an improved balance between precision and recall, reinforcing the attack detection system's capabilities. Furthermore, the combination of DBN with SVM showcases excellent performance, highlighting heightened attack identification and response capabilities. This study underscores the significant advantages of integrating various attack detection methods, contributing to the development of a more agile and adaptive security system.

5.2 Recommendation

a. Given the success of combining DBN with other methods like Isolation Forest and SVM, future studies could look into further collaborative models. Investigating the synergy between multiple attack detection techniques can provide fresh approaches to improving overall system performance.
b. The combined DBN-Isolation Forest model revealed an improved balance of precision and recall. Further parameter fine-tuning and experimentation with various algorithms inside these collaborative models may optimize the trade-off between precision and recall for certain environments.
c. While the study demonstrated the efficacy of DBN and its collaborative models in a controlled setting, assessing their performance in real-world settings is critical. Practical implementations and assessments can provide insights into the adaptability and scalability of the models.
d. Recognizing the potential benefits of incorporating attack detection technologies, the study recommends developing a more agile and adaptive security system. Future research could focus on building dynamic integration strategies that can automatically adapt to changing cyber threats and architecture.
e. Investigate the DBN model's transferability and collaborative techniques across various designs and industries. Assessing

their performance in various circumstances can provide useful information about the generalizability of these attack detection approaches.

f. Then the next recommendation or suggestion is how the practical implementation of the findings can be applied in cybersecurity practice including recommendations for the integration of existing models and systems.
g. Then for further research, the modelling process can be carried out with more improvement in each parameter so as to reduce the potential bias in the model created.
h. Future research is expected to use the latest datasets to adjust to the growing cyber attacks.