CHAPTER 7

CONCLUSION

7.1 SUMMARY AND CONCLUSION

CHAPTER 7

CONCLUSION

A comprehensive methodology has been developed for detection and mitigation of both intentional and unintentional insider threat, addressing challenges in P&ID, UIM, and IIM phases to secure data breach. The contributions span data preprocessing with tuned Nearmiss2 sampling to handle imbalanced datasets, a hybrid machine learning framework to enhance classification accuracy in P&ID phase, and innovative feature engineering techniques for meaningful data representation is proposed in UIM phase. Additionally, IIM phase introduces user profiling mechanism to manage access control efficiently through adaptive Allowlist and Denylist mechanisms. Together, these phases offer a robust solution for securing systems against intentional and unintentional insider threats while significantly improving overall performance. This chapter concludes the research work.

7.1 SUMMARY AND CONCLUSION

The main goal of this research is to detect and mitigate both intentional and unintentional insider threats. The proposed methodology consist of three phases namely P&ID, UIM and IIM.

Phase I (P&ID) consist of Preprocessing layer and Insider Detection layer. In Layer 1, preprocessing using data integration, encoding and sampling using Nearmiss2 is employed. In Layer 2, B-SVM algorithm is applied to detect and classify user into genuine, intentional and unintentional insiders. The two contributions are made in phase I is tuning Nearmiss2 sampling technique to handle class imbalance problem, and proposed a B-SVM algorithm for detection of genuine, intentional and unintentional insiders. In Phase I, preprocessing with tuned Nearmiss2 sampling technique is successfully done to obtain balanced data. After sampling, B-SVM achieved 99.15% accuracy with 0.84% misclassification rate and outperforms SVM and BIRCH for intentional and unintentional insider detection. It detected 8 intentional and 1 unintentional insiders using CERT dataset. In CIC darknet dataset, 4783 intentional darknet users and 68 unintentional darknet users.

In Phase II (UIM), the detected unintentional insiders are mitigated using keystroke-based user authentication. Phase II consist of two layers namely Feature Engineering, and Core Behavior Identification. In Layer 1, Feature Engineering using CKPCA is employed. In Layer 2, Deep Belief Network is applied for core behaviour identification. The significant contribution of this phase is obtaining intricate feature representation using proposed CKPCA technique. These features were further processed using Deep Belief Networks to authenticate unintentional insider and classify them into genuine, and intentional insiders. By leveraging CKPCA, the DBN model obtained accuracy of 99.84% and lowest EER of 0.15% in user authentication. In CERT dataset, CKPCA-DBN mitigated one unintentional insider as intentional insider. In CIC darknet dataset, CKPCA-DBN mitigated 68 unintentional darknet users as 64 intentional darknet and 4 genuine users.

In Phase III (IIM), the detected intentional insiders from P&ID and UIM phases are mitigated using user profiling mechanism. Phase III consists of three layers namely Data Preprocessing, Model Training and Evaluation, and User Profiling. In Layer 1, preprocessing using label encoding and train test split is accomplished. In Layer 2, the Decision tree algorithm is trained to classify and predict the high risk and low risk users. In Layer 3, the high risk users are profiled into Allowlist and low risk users are profiled into Denylist. The significant contribution of this phase is training classification model to profile and manage genuine and intentional insider based on outcome obtained from P&ID and UIM phases. IIM phase sing Decision tree obtained 100% accuracy, precision, recall, and f-score for unintentional insider mitigation. The CERT dataset analysis profiled 57 genuine users in the Allowlist and identified 8 intentional insiders in the Denylist. In CIC Darknet dataset, 5063 benign users are successfully profiled in the Allowlist and detecting 4847 intentional insiders in the Denylist. The summary of significant contribution is depicted in Table 7.1.

Table 7.1: Significant Contribution in Proposed Methodology

Phases	Contribution (s)	Method(s) Applied	Outcome achieved	Result(s)
Preprocessing and Insider Detection (Phase I)	Tuned Nearmiss2 for sampling	Nearmiss2 with 'Majority' sampling strategy	Addressed the class imbalance problem successfully.	Detected 8 intentional and 1 unintentional insiders using CERT dataset. Detected 4783 intentional darknet users and 68 unintentional darknet users using CIC darknet dataset.
	B-SVM for Classification	Combined SVM and BIRCH (B-SVM)	B-SVM achieved 99.15% accuracy with 0.84% misclassification rate.	
Unintentional Insider Mitigation (Phase 2)	CKPCA for Feature Engineering	Clonal Kernel Principal Component Analysis (CKPCA)	CKPCA with DBN obtained 99.84% accuracy and lowest EER of 0.15%.	In CERT dataset, one unintentional insider mitigated as intentional insider. In CIC darknet dataset, 68 unintentional darknet users mitigated as 64 intentional darknet and 4 genuine users.
Intentional Insider Mitigation (Phase 3)	Comprehensive Insider Profiling	Decision Tree	User profiling using decision tree obtained 100% accuracy, precision, recall and f-score.	Profiled 57 genuine users in the Allowlist and identified 8 intentional insiders in the Denylist using CERT insider dataset. In CIC Darknet dataset, 5063 benign users are successfully profiled in the Allowlist and detecting 4847 intentional insiders in the Denylist.

From the table 7.1, it is concluded that the proposed methodology had successfully detected and mitigated both intentional and unintentional insiders.