# Chapter 9
# Summary and Conclusion

## 9.1 Summary of Contributions

The research came up with a multi-stage, all-encompassing approach to the detection, prediction, detection, and optimization of responses to zero-day attacks in dynamic environments including cloud networks. These phases were related to the specific purpose of research and it contributed input to the significance of the system as a whole.

### 9.1.1 Phase 1 Zero-Day Attack Path Identification

Phase 1 involved a new technique of determining potential zero-day attack paths and in this case an Enhanced Back Propagation Neural Network (BPNN) was the combination of a Probabilistic Graph Model. This phase applies the simulations on the CloudSim to generate realistic network behavior and attack processes that can be deployed to the model to train on detecting vulnerable paths, and these will be exploited by unidentified threats. The framework has the ability to build and analyze various attack paths in the sense that it logs the interaction between nodes and transition thus giving a basis on other prediction and detection actions. This is a step that has been successful in meeting Objective O1, which is focused on the adequate identification of zero-day attack routes in the dynamic and complicated settings.

### 9.1.2 Phase 2 Zero-Day Attack Prediction

Phase 2 In this phase, a Modified Bi-LSTM has been created and integrated with Game theory and an Autoencoder to predict the action of the attacker. The Autoencoder component uses the dimensionalities reduction to get the significant features and the Game Theory component is used to simulate the strategic interaction between the attacker and defender to model the actual world threat dynamics. This integration assists the system in making the right predictions of the chain and character of the potential attack plan before that are executed. Phase addresses Objective O2 because it will offer forecast information which will reinforce the perception of future threats which lie at the lower levels and enhance the preparedness of the detection mechanism in the upper stages.

### 9.1.3 Phase 3 Prediction and Detection of ZDA in Real-Time

Phase 3 entails a research introducing the DC-nZDA, which is a hybrid model, a combination of ResNet50 (extracting spatial features) and LSTM networks (temporal dynamics capture) in network activity. It is just this architecture that is designed to respond to the adversary state, where the attackers are able to attempt to evade this architecture through subtle manipulation of its inputs. The adversarial safety factor will ensure that the system is resilient to such deception, and will be in a position of classifying the zero day attack using high quality and real time. The stage is a successful realization of Objective O3 that targets the real-time and reliable detection of attack activities that are in progress because it delivers high detection accuracy and low false negativity.

### 9.1.4 Phase 4 Optimization of Detection Accuracy

Phase 4 Phase 4 entailed application of Optimized Levy Flight based Fruit Fly Optimization Algorithm (OLFFOA) To enhance the use of the detection system by optimizing the classifier parameters and improving the decision boundaries. Levy Flight integration assists in enhancing the global search ability and FFOA assists in finding the optimal solutions within a short period. Such a step of optimization can significantly increase the accuracy of classification, reduce the false positives, and also improve the overall system performance without compromising the accuracy of detection. This step therefore succeeds in meeting Objective O4 that will most likely streamline the post-classification abilities of the framework to react to real-time, precise, and low-latency threats.

## 9.2 Overall Summary

The methodology suggested in the proposal is an interdependence of ML, DL, game-theoretic approach, and metaheuristic optimization in single framework. The skills matching dealing with the lifecycle between the simulation and the actual-time response of zero-day attack are also introduced in each of the stages. The quantitative indicators ensure that the framework achieves all the intended goals and is much more superior to the existing frameworks in terms of Sensitivity, Correctness (95.9%), and False positive reduction.

## 9.3 Conclusion

This thesis is a new and proactive to the management of zero-day attacks since it is identified, predictive and detection and maximization. The system has performed more positively in integrative approach to probabilistic modelling, game theory and adversarial-resilient DL. It is not just superior in image identification but also tackles adversarial resistance, system scalability.