ABSTRACT

A zero-day attack is a type of cyber-attack that exploits a previously unknown vulnerability in a software application or a system. These attacks are called "zero-day" because the software developer has zero days to address the vulnerability since it has just been discovered. The term zero-day attack refers to a single or specific instance of an attack exploiting a newly discovered vulnerability, whereas zero-day attacks refers to multiple instances of such attacks or the general concept of attacks exploiting zero-day vulnerabilities. Zero-day attacks have become a significant cybersecurity concern as attackers continuously exploit previously unknown vulnerabilities, causing severe consequences such as data breaches, financial losses, and reputational damage. Although vulnerability identification can be performed using techniques such as code analysis, vulnerability scanning, penetration testing, and threat intelligence, traditional detection approaches remain largely dependent on signature-based and reactive mechanisms, making them ineffective against unknown and evolving threats. These limitations are further amplified in dynamic cloud environments, where increased system complexity, shared infrastructure, and large-scale network traffic expand the attack surface and hinder accurate real-time monitoring. Existing methods also suffer from high false positive rates, limited adaptability, inadequate behavioral learning, and increased computational overhead, reducing their effectiveness in large-scale deployments. To address these challenges, this research proposes a proactive, intelligent, and adaptive multi-phase framework for predicting, identifying, and detecting zero-day attacks. The proposed methodology integrates Machine Learning (ML), Deep Learning (DL), probabilistic modeling, game theory, and optimization techniques to enable behavior-driven predictive security. By moving beyond signature-based detection and learning attacker behaviors and system vulnerabilities, the framework enhances detection accuracy, minimizes false alarms, and provides scalable real-time protection suitable for dynamic cloud computing environments.

The proposed research outlines a four-phase methodology for predicting zero-day attacks by combining machine learning and deep learning techniques. The first phase employs an Enhanced BPNN with CloudSim simulator to map the attack paths. In subsequent phases, data is systematically preprocessed, feature selection is performed, and multiple ML (Machine Learning) / DL (Deep Learning) models are trained and evaluated, followed by a comparative analysis of results across approaches. The objective is to proactively suggest performance efficient methods to identify and predict previously unseen (zero-day) threats, enabling organizations to detect attacks before they manifest. This approach proves to enhance the accuracy and reliability of intrusion detection systems by leveraging both traditional machine learning and advanced deep neural network methods, ultimately improving protection of digital assets through early, learned prediction of emerging threats. The research is conducted using a combination of simulation and real-world data to evaluate

the proposed models performance. The simulation is performed using CloudSim, synthetic datasets Dataset 1 (Path Dataset) and Dataset 2 (Attack Dataset) is obtained from actual zero-day attack. The results of the comparative analysis will provide insights into the effectiveness of the proposed methodology and its potential for practical applications in cyber security.

The core contribution of the research for Phase 1 is dedicated to identify the potential paths through which a zero-day attack can infiltrate the system. This phase traces the attack path in the cloud environment using a Probabilistic Graph Approach combined with an Enhanced Back Propagation Neural Network (BPNN), supported by Improved Decision Trees (DT) and Weighted K-Means clustering. Outcomes include improved accuracy by 3.01%, precision by 2.63%, recall by 2.27%, and F1 score by 2.34% compared to Bayesian, Scalable Bayesian, and Probabilistic Bayesian models. Phase 2 employs a hybrid method of Game Theory based on the Nash Equilibrium and an Adaptive Gaming Model based on a Modified Bi-Directional Long Short-Term Memory (LSTM) network to predict zero-day attacks. It enhances the ability to predict the potential zero day threats within the system through enhanced accuracy prediction, system performance and improved communication between security components achieving up to 11.4% higher accuracy, 11.3% higher precision, 5.5% higher recall, and 5.4% higher F1-score compared to DT, SVM, GNB, and Logistic Regression. Phase 3 propose a Residual Network integrated Deep Convolutional Zero-Day Adversarial Safety Network, designed for live zero-day attacks. It uses deep learning over the cloud communication network traffic analyzing and detecting events given in Dataset 1 (Path Dataset) and Dataset 2 (Attack Dataset) for real-time anomalies. Advanced convolutional layers and residual connections enhance generalization and classification up to 12.4% higher accuracy, 10.2% higher precision, 9.1% higher recall, and 9.2% higher F1-score over HMM, and up to 9.7% higher accuracy and 10.8% higher recall and ensure faster learning to identify zero-day attacks effectively compared to Bayesian GNN, BERT, TransVAE, and HADE-SVM models. Phase 4 presents an OLFFOA-optimized hybrid deep learning model. This comparative analysis allows for evaluating different models to determine the most efficient and accurate approach for zero-day attack prediction. The model achieves up to 98.1% accuracy, 95.2% precision, 94.4% recall, and 94.8% F1-score on Dataset 2, outperforming ResNet50, CNN-LSTM, and Bi-LSTM individually by 1.9% – 3.1%. The results show improved recognition rates, fewer false positives, and minimized time complexity, thus making the prediction models credible and scalable. Overall, this research work recommends performance efficient methods to handle zero-day attacks in cloud environment. The results are evident when tested with simulated dataset and benchmark dataset in zero-day attack. The anticipated research impact contributes to the development in enabling proactive, intelligent, and adaptive cloud security mechanisms, while the practical implication of this work supports real-world deployment in cloud infrastructures for early threat prediction, resilient intrusion detection, and enhanced security reliability in dynamic and large-scale environments.