SPECIMEN FORMAT FOR THESES OF MONTH

Faculty	:	School of Physical Science and Computational Sciences
Department	:	Computer Science
Branch/ Area:	:	Cyber Security
Sub Subject Heading:	:	Zero-Day Attack
Candidate's Name	:	Swathy Akshaya M
Candidate's Address with email	:	Ph.D Research Scholar (FT Without M. Phil), Department of Computer Science Avinashilingam Institute for Home Science and Higher Education for Women Coimbatore 17phcsf003@avinuty.ac.in
Title of the thesis	:	Performance Efficient Methods to Handle Zero-Day Attacks in Cloud Environment
(i) In Roman Script		-
(ii) In roman Script		-
Nomenclature of Degree:	:	Ph.D
Month & Year of Enrolment:	:	July, 2017
Month & Year of Registration:	:	July, 2017
Month &Year of Submission:	:	January, 2026
Month &Year of Award	:	April, 2026
Name of Supervisor	:	Dr. G. Padmavathi
Designation of Supervisor	:	Former Professor
Centre/department/school in which research was conducted	:	Department of Computer Science

University's Name & Address : Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore – 641043.

Abstract within 300 words:

A zero-day attack exploits previously unknown vulnerabilities in software or systems, leaving developers with no prior opportunity to implement defensive patches. Such attacks pose significant cybersecurity risks due to their stealthy nature and ability to bypass traditional signature-based and reactive detection mechanisms. The challenge becomes more critical in dynamic cloud computing environments, where increased system complexity, shared infrastructure, and large-scale network traffic expand the attack surface and complicate real-time monitoring. Existing detection approaches often suffer from limited adaptability, inadequate behavioral learning, high false alarm rates, and substantial computational overhead, reducing their effectiveness against evolving threats. To address these limitations, this research proposes a proactive, intelligent, and adaptive multi-phase framework for predicting, identifying, and detecting zero-day attacks. The framework integrates Machine Learning (ML), Deep Learning (DL), probabilistic modeling, game theory, and optimization techniques to enable behavior-driven predictive security. By focusing on attacker behavior and system vulnerabilities rather than predefined signatures, the proposed approach enhances early threat prediction and strengthens intrusion detection capabilities in cloud environments.

The methodology consists of four phases. Phase 1 identifies potential zero-day attack paths using a probabilistic graph model combined with an Enhanced Back Propagation Neural Network, supported by Improved Decision Trees and Weighted K-Means clustering within a CloudSim simulation environment. Phase 2 introduces a hybrid prediction model integrating Nash Equilibrium-based Game Theory with a Modified Bi-Directional Long Short-Term Memory network to forecast potential attack strategies. Phase 3 presents a Residual Network-based Deep Convolutional Zero-Day Adversarial Safety Network designed for real-time anomaly detection across cloud communication traffic. Phase 4 performs comparative evaluation using an OLFFOA-optimized hybrid deep learning model to determine the most efficient predictive architecture. The framework is evaluated using simulated cloud environments and real zero-day attack datasets. Experimental outcomes demonstrate improved detection reliability, reduced false positives, and enhanced scalability. Overall, the research contributes

a comprehensive predictive security framework enabling proactive defense, resilient intrusion detection, and reliable protection of cloud infrastructures against emerging zero-day threats.

i) Major objectives :

Primary Objective

- To Devise Performance-Efficient Methods for Early Identification of Zero-day Attack Paths in cloud environment to enable accurate Prediction and Detection of attacks.

Secondary Objectives

- **Improve Detection Accuracy and Security**- To enhance classification accuracy, reduce misclassification rates, and strengthen overall data security using imbalance-aware and optimized learning techniques.
- **Enhance Predictive Capability**- To develop robust and precise predictive models capable of forecasting zero-day attacks and ensuring reliable system communication.
- **Develop a Generalized Detection Framework**- To design an effective zero-day attack detection model with strong generalization capability, high classification accuracy, and improved detection efficiency across diverse cloud infrastructures.
- **Integrate Explainable and Efficient Decision Mechanisms**- To incorporate interpretable and scalable ML/DL approaches that support transparent decision-making and analyst trust.
- **Enable Comprehensive Evaluation and Benchmarking**- To establish standardized performance metrics and comparative evaluation strategies for validating zero-day attack detection performance.
- **Achieve Effective Mitigation in Dynamic Cloud Environments**- To develop an integrated framework capable of identifying, predicting, detecting, and mitigating zero-day attacks in dynamic and evolving cloud ecosystems.

ii) Methodology :

The Conceptual Framework of the Proposed Research Methodology is given below:

Research Design

Phase I – Zero-Day Attack Path Identification (Enhanced BPNN with CloudSim)

- **Objective:** Identify **potential zero-day attack propagation paths** before exploitation.
- Developed an **Enhanced Back Propagation Neural Network (EBPNN)** integrated with a **Probabilistic Graph Model**.

- Utilized **CloudSim simulation** to generate **realistic cloud network behavior and attack scenarios**.
- Modelled **network nodes, transitions, and vulnerability interactions** as graph structures.
- Applied **learning rate and momentum optimization** to improve neural network convergence.
- Enabled **early detection of vulnerable attack routes** and unknown threat propagation paths.
- Achieved **high attack-path identification performance** (≈99% accuracy, precision, recall, and F-measure).
- Demonstrated **superior routing-path identification** compared to traditional Bayesian approaches.

Phase II – Zero-Day Attack Prediction (Game Theory + ML Ensemble + M-BiLSTM)

- **Objective:** Predict **attacker behavior and future zero-day attack strategies**.
- Designed a **hybrid Machine Learning prediction framework** combining:
  - **Improved Decision Tree**
  - **Random Forest**
  - **Logistic Regression**
  - **Modified Bi-Directional LSTM (M-BiLSTM)**
  - **Autoencoder for feature reduction**
  - **Game Theory with Nash Equilibrium modeling**
- Simulated **attacker–defender strategic interactions** using Game Theory principles.
- Implemented **Stacking Ensemble Learning** to enhance prediction reliability and reduce model bias.
- Evaluated performance using **accuracy, precision, recall, F-measure, and false alarm rate**.
- Achieved **consistent prediction accuracy (~95%) across multiple datasets**.
- Improved **model stability, reliability, and predictive intelligence** for proactive defense.

Phase III – Real-Time Zero-Day Attack Prediction and Detection (ResNet50 + BiLSTM – DL & TL Framework)

- **Objective:** Perform **real-time detection and classification of unknown zero-day attacks**.
- Developed a **Deep Learning + Transfer Learning framework** integrating:
  - **ResNet50** for spatial feature extraction
  - **BiLSTM** for temporal traffic behavior analysis

- Applied **Decision Tree Regressor preprocessing** and **RF + Logistic Regression feature selection**.
- Used **Stacking Ensemble classification** for final threat identification.
- Enabled learning of **complex spatial–temporal attack patterns** in network traffic.
- Demonstrated **strong generalization capability** against unseen and adversarial threats.
- Achieved **high detection performance** (≈95.9% accuracy with strong precision and recall).
- Reduced **training cost and inference latency** through Transfer Learning.
- Supported **real-time decision making** with low computational overhead.

Phase IV – Zero-Day Attack Prediction Comparative Analysis and Optimization (OLFFOA-Based Optimization) using Ensemble Neural Network

- **Objective:** Optimize and validate **prediction and detection performance**.
- Conducted **comparative evaluation** between:
  - **ML-based Prediction Model (Phase II)**
  - **DL + Transfer Learning Model (Phase III)**
- Applied **Optimized Levy Flight–based Fruit Fly Optimization Algorithm (OLFFOA)** to:
  - Enhance model stability
  - Optimize classifier parameters
  - Reduce prediction errors
- Demonstrated **≈0.9% higher accuracy** and improved generalization for the Phase III model.
- Validated **ResNet50 + BiLSTM with optimization** as the **most effective framework** for zero-day attack prediction and detection.

Overall Methodological Outcomes

- Established a **four-phase unified threat intelligence framework** integrating **ML, DL, Transfer Learning, Game Theory, and Optimization**.
- Enabled **end-to-end zero-day security workflow**: **Attack Path Identification → Attack Prediction → Real-Time Detection → Performance Optimization**.
- Delivered **high accuracy, reduced false positives, faster detection time, and scalable cloud deployment capability**.
- Provided a **proactive, intelligent, and adaptive cybersecurity methodology** suitable for **dynamic cloud environments**.

iii) Findings:

- **Proposed a Novel Multi-Phase Intelligent Framework:** Developed a **comprehensive and integrated architecture** for **proactive prediction, detection, and optimization of zero-day attacks** in dynamic cloud computing environments.
- **Hybrid Intelligent Security Approach:** Demonstrated that combining **Machine Learning, Deep Learning, Transfer Learning, Probabilistic Modeling, Game Theory, and Optimization techniques** significantly **strengthens cybersecurity defenses** against previously unseen threats.
- **Effective Zero-Day Attack Path Identification:** Successfully achieved **early discovery of vulnerable attack routes** using an **Enhanced Back Propagation Neural Network integrated with a Probabilistic Graph Model**, enabling accurate **vulnerability mapping** and **reduced misclassification**.
- **Behavior-Driven Attack Prediction:** Established that integrating **Game Theory, Nash Equilibrium modeling, Modified Bi-LSTM, and Autoencoder mechanisms** enables **reliable prediction of attacker strategies** before execution.
- **Strategic Attacker–Defender Modeling:** Confirmed that **strategic interaction analysis** enhances **threat forecasting, system preparedness, and intelligent decision-making** within cloud security infrastructures.
- **Robust Real-Time Zero-Day Detection:** Achieved improved real-time detection using the **Deep Convolutional n-Zero Day Adversarial Safety Network combined with Residual Network architecture**, enabling **accurate classification of unknown and evolving threats**.
- **Enhanced Learning of Complex Threat Patterns:** Demonstrated that integrating **spatial and temporal deep learning features** improves recognition of **complex attack behaviors and adversarial network activities**.
- **Optimization-Driven Performance Improvement:** Validated that **Optimized Levy Flight–based Fruit Fly Optimization Algorithm (OLFFOA)** enhances **classifier efficiency**, **reduces false positives**, **refines decision boundaries**, and **minimizes computational complexity** for scalable deployment.
- **Transition Beyond Traditional Security Models:** Verified that the integrated framework enables **proactive, adaptive, and intelligent cybersecurity defense**, overcoming limitations of **signature-based and reactive intrusion detection systems**.

- **Empirical Validation and Practical Feasibility:** Experimental evaluation using **CloudSim simulations and benchmark zero-day datasets** confirmed **robustness, scalability, reliability, and real-world deployment feasibility**.
- **Improved Operational Security Performance:** Observed **higher detection reliability, faster response capability, improved scalability**, and efficient handling of large-scale cloud infrastructures.
- **Evolution Toward Adaptive Cloud Security:** Established a clear transition from **reactive intrusion detection mechanisms** toward **predictive, intelligent, and adaptive cloud security architectures** capable of mitigating evolving zero-day threats.
- **Overall Research Outcome:** The findings recommend **performance-efficient zero-day attack mitigation mechanisms** supporting **early threat prediction, resilient intrusion detection, enhanced security reliability, and practical real-world cloud deployment**.

Examiners

Internal Examiner: Dr. Sushil Chandra Jain,
Former Professor Computer Science and Engineering,
Dean, FA and Chairperson, DRC (MCA)
Rajasthan Technical University, Kota,
Rajasthan.

External Examiner: Dr. Gang Li,
Professor,
School of Information Technology,
Deakin University,
Australia.