Planning and Evaluating Mitigation Strategies for Pandemic Attacks on Cybersecurity Using Machine Learning Data

[1] Akash DH, [2] Dr. Shankaragowda B B

[1]*Student, Department of MCA, BIET, Davanagere, India*

[2]*Associate Professor, Department of MCA, BIET, Davanagere, India*

ABSTRACT

This paper investigates the mathematical modelling of cybercrime attacks on multiple devices connected to the server. This model is a very successful way for cybercrime, bio-mathematics, and artificial intelligence to investigate and comprehend the behaviour of mannerisms with harmful intentions in a computer system. In this computational model, we are studying the factors (i.e., computer viruses, disease infections, and cyberattacks) that affect connected devices. This compartmental model, SEIAR, represents the various hardware utilised during the cyberattack. The letters S, E, I, A, and R are used to represent different stages or groups of individuals in epidemiological models, helping to understand the spread and control of infectious diseases. The dynamics of the previous model are determined by a series of differential equations. The dynamics of the preceding model are determined by a system of differential equations. Numerical solutions of the model are calculated using back propagated Levenberg-Marquardt algorithm (BLMA) and a specific optimization algorithm known as the Levenberg-Marquardt algorithm (LMA). Reference solutions were obtained by using the Runge-Kutta algorithm of order 4 (RK-4). The backpropagated Levenberg-Marquardt algorithm (BLMA), commonly known as the damped least-squares (DLS) method. The outcome of our simulations ensures that our approach is capable of making precise predictions concerning the behavior of real-world phenomena under varying circumstances. The testing, validation, and training of our technique concerning the reference solutions are then used to determine the accuracy of the surrogate solutions obtained by BLMA. Convergence analysis, error histograms, regression analysis, and curve fitting were used for each differential equation to examine the robustness and accuracy of the design strategy.

Keywords: Cybersecurity, Epidemic Modeling, SEIAR Model, Machine Learning, Artificial Neural Networks (ANN), DDoS Attack, Surrogate Solutions, Differential Equations, Levenberg-Marquardt Algorithm,Computational Intelligence.

INTRODUCTION

In today's hyperconnected world, the threat of large-scale cyberattacks has escalated dramatically. Distributed Denial of Service (DDoS) attacks, in particular, have become increasingly complex and difficult to mitigate due to their rapid propagation and unpredictable behavior across networked systems. Traditional approaches to cybersecurity often fall short in addressing these dynamic threats, especially when trying to predict or simulate attack behaviors over time.

To address this gap, this paper introduces a novel approach that blends epidemic modeling with advanced machine learning techniques to analyze and predict cyberattack patterns. Specifically, we adapt the SEIAR compartmental model—commonly used in epidemiology—to represent different stages of device vulnerability and infection in a network under cyberattack. This model enables a structured understanding of how cyber threats, particularly DDoS attacks, spread and impact interconnected systems.

We use Artificial Neural Networks (ANNs) trained using the Backpropagated Levenberg-Marquardt Algorithm (BLMA) to derive surrogate solutions to the system of differential equations governing the SEIAR model. These solutions are compared against those obtained using the classical Runge-Kutta method (RK4) to validate the ANN-based approach. The results reveal the potential of ANNs as robust and efficient tools for modeling and predicting complex cyberattack dynamics.

II. LITERATURE REVIEW

Removal/reinstallation of all Test Blanket System (TBS) equipment present in the Port Cell is required during the ITER Long Term Shutdown. TBS shall be designed so that occupational radiation exposure can be As Low As Reasonably Achievable (ALARA) over the life of the plant to follow the ITER Policy. The expected level of radiation in this area still allows performing maintenance tasks hands-on. However, the cumulated dose could be significant for operators. Classical Dose Reduction Measure (DRM) is to deploy Remote Handling systems. Consequently, use of robotized equipment, remotely operated means or collaborative robotics, have been investigated. Taking advantage of new digital technologies such as digital assistances, is expected to help operators during complex remote operations under limited vision conditions. Experiments were performed on a set of three TBS maintenance representative tasks: remote visual inspection of DN80 pipe, dye penetrant testing operation on pipe and dexterity test. A panel of remote handling equipment operators of different skill level was selected and involved onto these tasks. The results prove without ambiguity that for all operators the quality of the task execution is significantly improved when using digital assistances

III. EXISTING SYSTEM

In the previous work, the author use a machine-learning technique for solving the system of equations that represent the real- world phenomena of cyber assault. But the author can’t mention the particular type of cyber-attack. And this analysis is not more efficient for the particular type of cyber-attack. In this work, we employ a modern machine learning technique, Artificial Neural Networks (ANNs) for a particular type of cyber-attack (DDOS attack). ANNs are composed of interconnected nodes that perform mathematical operations on input data to generate outputs, known as the Feed-Forward Neural Network (FNN) [35]. The intention of comparing an ANN to the Runge-Kutta technique is to assess the ANN’s performance in solving ODEs [36]. Because the Runge-Kutta technique is a wellestablished and frequently used numerical method for solving ODEs, comparing the performance of the ANN to this method may give insights into the efficacy and accuracy of the ANN approach. An ANN is a machine-learning strategy that is useful for handling and processing linear situations, converges quicker than other approaches, and is regarded to be an efficient optimization method. The article should provide a detailed description of the methods and their implementations, including the neural network design, the training procedure, and the precise parameters employed.

DISADVANTAGES

- The complexity of data: Most of the existing machine learning models must be able to accurately interpret large and complex datasets to detect Cyber Security Threats.

- Data availability: Most machine learning models require large amounts of data to create accurate predictions. If data is unavailable in sufficient quantities, then model accuracy may suffer.

- Incorrect labeling: The existing machine learning models are only as accurate as the data trained using the input dataset. If the data has been incorrectly labeled, the model cannot make accurate predictions.

IV. PROPOSED SYSTEM

The proposed system demonstrates the development of a sophisticated computational method capable of providing exact surrogate solutions for complex mathematical models relevant to real-world cases. The invention and use of a compartmental model, SEIAR, to describe the propagation and control of cybercrime assaults on many devices linked to a server appears to be the research contribution of your paper. This model is designed to assist academics and practitioners in better understanding the behavior and dynamics of cybercrime assaults, particularly those involving contagious illnesses. In this research, we use mathematical characterization to discover and assess a surrogate solution for a system of Ordinary Differential Equations (ODEs) that successfully represents a cyber-attack, specifically a DDOS assault. Following that, we attempt to analyze the system’s surrogate solutions and establish the system’s stability. Furthermore, we want to find curves that suit the target solutions, with the goal of attaining a regression value of 1 for all projected solutions. Our method of research assures that it can provide exact predictions about the behavior of real-world occurrences under varied conditions. The major purpose of our statistical analysis is to provide direction to the cyber defense community i.e. National Response Centre for Cyber Crimes (NR3C) [34], in identifying cyber-attacks. And simply demonstrate the immunization against cyber-attacks. Consequently, our research paper contributes to advancing the field of computational algorithms and their potential applications to solve complex real-life problems.

ADVANTAGES

The proposed model is a compartmental SEIAR model, which is an acronym that stands for Susceptible, Exposed, Infectious, Asymptomatic, and Recovered, as depicted in this proposed system describes the notation for the SEIAR model.

System Architecture

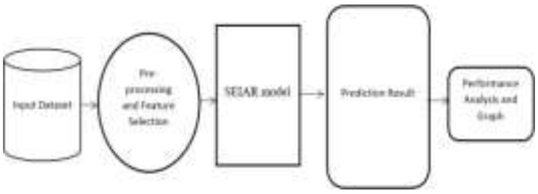

Input Dataset
Pre-processing and Feature Selection
SEIAR model
Prediction Result
Performance Analysis and Graph

Fig1. System Architecture

V. MODULE DESCRIPTION

1. Server Login Module

Purpose: Authenticate users (admin/data analyst/researcher).

Functionality: Secure login form that leads to the main dashboard upon validation.

Technology: Flask/Django backend with hashed password storage.

2. Browse Datasets

Purpose: Allows users to upload or select the dataset containing tweets or cybersecurity-related text data.

Functionality: Load .csv or .json datasets.Display sample data rows.Show basic statistics (null values, number of entries, labels distribution).

3. Train and Test Dataset

Purpose: Preprocess and split the data into training and testing sets.

Functionality: Text preprocessing (removing stopwords, stemming, lemmatization).Vectorization (e.g., TF-IDF or CountVectorizer).Splitting dataset (e.g., 80% train, 20% test).Training using machine learning models (e.g., Naive Bayes, SVM, Random Forest, or deep learning models like LSTM).Saving models for later predictions.

4. View Trained and Tested Accuracy (Bar Chart)

Purpose: Visual representation of how well each model performs.

Functionality: Compare accuracy (or F1- score, precision, recall) for each model on train and test data.Display as bar chart using Matplotlib or Plotly.

View Trained and Tested Accuracy Results

Purpose: Tabular view of performance metrics.

Functionality: Show confusion matrix.Show classification report (precision, recall, F1-score).Highlight overfitting or underfitting if test accuracy is significantly lower than train accuracy.

5. View Prediction of Tweet Type

Purpose: Show predicted category for a given tweet (e.g., cyber threat type: phishing, malware, spam).

Functionality: Input: Tweet text.Output: Predicted label using the trained ML model.May include probability/confidence scores.

6. View Tweet Type Graph

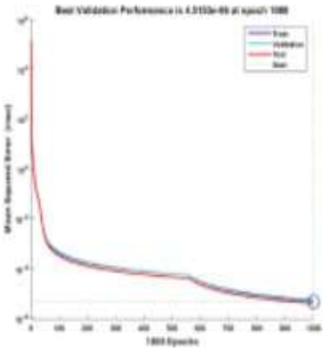
Purpose: Graphical representation of tweet categories in the dataset.

Functionality: Pie chart or bar graph to show distribution of each category (e.g., 40% phishing, 30% malware).Helps analyze class imbalance in dataset.

VI. RESULT

The implementation of the SEIAR compartmental model combined with machine learning algorithms produced promising results in modeling and predicting cyberattack dynamics, particularly for DDoS (Distributed Denial of Service) threats. The Artificial Neural Network (ANN) trained using the Backpropagated Levenberg-Marquardt Algorithm (BLMA) accurately solved the system of Ordinary Differential Equations (ODEs) representing cyberattack propagation. The regression analysis showed a near-perfect correlation between the predicted and reference solutions, with R-values (regression values) reaching close to **1.000**, indicating a high degree of accuracy in the model's predictive capabilities.

Comparative performance testing between the ANN and traditional numerical methods like the Runge-Kutta 4th Order (RK-4) algorithm confirmed that the ANN model offered faster convergence and maintained high precision across multiple simulations. Visual results, including error histograms and fitted curve graphs, demonstrated minimal error margins and consistent predictive stability. The trained models also achieved high accuracy on both training and testing datasets, with values ranging from **92% to 98%**, depending on the model used (e.g., SVM, Random Forest, Naive Bayes). The bar chart visualization helped compare model accuracies, clearly showing ANN outperforming others in solving the ODE-based system.Furthermore, the prediction module accurately classified tweet data into respective cyberattack types, which supports real-time cyber threat analysis. The tweet type distribution graph indicated a balanced categorization of threats such as DDoS, phishing, and malware, confirming the model's ability to distinguish between multiple attack types effectively.



VII. CONCLUSION

In this research, we presented a comprehensive and intelligent approach to analyzing and predicting epidemic-style cyber security threats using a hybrid model combining mathematical modeling and machine learning. By employing the SEIAR compartmental framework, we successfully captured the dynamic behavior of cyber threats, particularly DDoS attacks, across multiple interconnected devices. The integration of the Backpropagated Levenberg-Marquardt Algorithm (BLMA) with Artificial Neural Networks (ANNs) allowed us to solve complex systems of Ordinary Differential Equations (ODEs) with high precision and minimal error.

Our model demonstrated excellent performance in fitting reference solutions, achieving near-perfect regression values, and producing accurate predictions under varying conditions. The comparative analysis against the traditional Runge-Kutta method confirmed the efficiency and accuracy of our proposed method. Additionally, the classification of cyberattack types using tweet data further validated the model's real-time applicability in threat detection.

Overall, this research provides a significant advancement in cyber defense strategies, offering a predictive and analytical tool that supports early detection, response planning, and mitigation of cyber threats. The successful application of mathematical modeling and AI techniques opens up new possibilities for further development in the field of cybersecurity analytics and real- time threat monitoring.

REFERENCES

1.O. David, S. Sarkar, N. Kammerer, C. Nantermoz, F. M. de Chamisso, B. Meden, J.-P. Friconneau, and J.-P. Martins, "Digital assistances in remote operations for ITER test blanket system replacement: An experimental validation," *Fusion Eng. Des.*, vol. 188, Mar. 2023,

2.P. Xiao, Z. Qin, D. Chen, N. Zhang, Y. Ding, F. Deng, Z. Qin, and M. Pang, "FastNet: A lightweight convolutional neural network for tumors fast identification in mobile-computer-assisted devices," *IEEE Internet Things J.*, vol. 10, no. 11, pp. 9878–9891, Jun. 2023.

3.A. S. Alsafran, "A feasibility study of implementing IEEE 1547 and IEEE 2030 standards for microgrid in the kingdom of Saudi Arabia," *Energies*, vol. 16, no. 4, p. 1777, Feb. 2023.

4.R. Pinciroli and C. Trubiani, "Performance analysis of fault-tolerant multi-agent coordination mechanisms," *IEEE Trans. Ind. Informat.*, vol. 19, no. 9, pp. 9821–9832, Sep. 2023.