ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206

Volume 8, Issue 8, August 2025

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808197

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

USING MACHINE LEARNING MODEL AND EXAMINING SAFETY AND SECURITY PLANS FOR THE TERM EPIDEMIC SECURITY MEASURES ISSUES

Barnali Chakraborty, Roja G

Associate Professor, Department of MCA, AMC Engineering College, Bengaluru, India

Student, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT: This paper explores how mathematical modeling can be used to understand and defend against cybercrime attacks targeting multiple devices connected to a central server. By blending concepts from cybersecurity, bio-mathematics, and artificial intelligence, the study aims to uncover how harmful behaviors—such as computer viruses, malware, and large-scale cyberattacks—spread through interconnected systems. At the heart of the research is the SEIAR compartmental model, which categorizes devices into five groups: Susceptible (S), Exposed (E), Infectious (I), Asymptomatic (A), and Recovered (R). This structure, inspired by epidemiological modeling of disease spread, allows for a detailed analysis of how attacks propagate and how they can be controlled.

The system's behavior is captured through a set of differential equations, whose solutions reveal how each device group changes over time during an attack. BLMA, integrated with artificial neural networks, is employed to create surrogate solutions capable of making fast and accurate predictions. The model is then tested, validated, and refined to minimize errors and achieve near-perfect regression scores (R = 1).

Ultimately, the results demonstrate that this method can reliably predict real-world cyberattack behaviors under a variety of scenarios, making it a powerful tool for anticipating threats and strengthening cyber defense strategies.

KEYWORDS: Cybersecurity, Epidemic Modeling, SEIAR Model, Machine Learning, Artificial Neural Networks (ANN), DDoS Attack, Surrogate Solutions, Differential Equations, Levenberg-Marquardt Algorithm, Runge-Kutta Method, Cyber Threat Analysis, Computational Intelligence.

I. INTRODUCTION

During the ITER Long Term Shutdown, it is necessary to remove and reinstall all Test Blanket System (TBS) components situated within the Port Cell. To align with the ITER policy, the TBS must be designed to keep occupational radiation exposure As Low As Reasonably Achievable (ALARA) throughout the plant's operational life. While radiation levels in this area are low enough to permit direct manual maintenance, the accumulated dose over time could still be considerable for workers. A common approach to reducing such exposure is the implementation of Remote Handling (RH) systems. As a result, options such as robotic equipment, remote-controlled tools, and collaborative robotic solutions have been evaluated. The integration of advanced digital assistance technologies is also seen as a way to support operators in performing complex remote operations, especially under restricted visibility conditions. To assess these solutions, trials were conducted involving three representative TBS maintenance activities: remote visual inspection of a DN80 pipe, dye penetrant inspection on the pipe, and a fine-motor dexterity task. Operators with a range of experience levels participated in these tests. The findings showed a clear improvement in task performance quality for all participants when digital assistance systems were utilized.

EXISTING SYSTEM

In earlier studies, machine learning methods were applied to solve systems of equations representing real-world cyberattack scenarios. However, the specific type of cyberattack was not identified, which limited the effectiveness of the analysis for targeted threat mitigation. In the present work, a modern machine learning approach—Artificial Neural

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Networks (ANNs)—is adopted to address a clearly defined attack type: the Distributed Denial-of-Service (DDoS) attack. ANNs consist of interconnected nodes that process input data through mathematical operations to produce outputs, forming what is known as a Feed-Forward Neural Network (FNN). The performance of the ANN is compared to the well-established fourth-order Runge–Kutta (RK) method, a widely used numerical approach for solving ordinary differential equations (ODEs). This comparison aims to evaluate the accuracy and efficiency of the ANN in generating solutions. ANNs are particularly effective for managing and processing linear problems, offer faster convergence than many alternative methods, and are recognized as powerful optimization tools. This study provides a comprehensive account of the techniques used, covering neural network architecture, the training methodology, and the specific parameter settings applied.

PROPSED SYSTEM

The proposed system presents an advanced computational framework capable of generating precise surrogate solutions for complex mathematical models with real-world applicability. A key contribution of this work is the design and implementation of the SEIAR compartmental model, which captures the spread and mitigation of cybercrime attacks across multiple devices connected to a server. This model serves as a valuable tool for researchers and practitioners to better analyze the behavior and progression of cyberattacks, particularly those exhibiting epidemic-like characteristics. In this study, mathematical formulations are employed to derive and evaluate a surrogate solution for a system of Ordinary Differential Equations (ODEs) that effectively simulates a Distributed Denial-of-Service (DDoS) attack. The research further examines the stability of these surrogate solutions and performs curve fitting to closely match target results, aiming for a regression value of 1 for all predictions. This ensures highly accurate forecasts of real-world cyber threat dynamics under diverse conditions. The statistical analysis is intended to guide cybersecurity entities, such as the National Response Centre for Cyber Crimes (NR3C), in detecting and responding to attacks, while also illustrating potential immunization strategies. Ultimately, this work advances the domain of computational algorithms and demonstrates their capability to address intricate, real-life cybersecurity challenges.

II. SYSTEM ARCHITECTURE

The proposed “Defense Strategies for Epidemic Cyber Security Threats” system architecture combines the SEIAR mathematical compartmental model with a machine learning–driven analytical framework to model, detect, and counter cyberattacks—particularly Distributed Denial-of-Service (DDoS) attacks—on networked devices. The SEIAR model categorizes devices into Susceptible, Exposed, Infectious, Asymptomatic, and Recovered states, with transitions between these states described by a set of ordinary differential equations (ODEs) that capture the dynamic nature of attack spread. The process begins by inputting initial parameters into the SEIAR model, which generates synthetic datasets through a numerical solver, such as the fourth-order Runge–Kutta method. These datasets are then used to train a Feed-Forward Neural Network (FNN), optimized using the Backpropagated Levenberg–Marquardt Algorithm (BLMA), to produce accurate surrogate predictions. The architecture is structured into three primary layers: **(1) Mathematical Modeling Layer**, where SEIAR equations define system behavior; **(2) Machine Learning Layer**, which trains, validates, and evaluates the ANN against reference solutions using convergence checks, regression analysis, and error metrics; and **(3) Decision and Defense Layer**, which leverages predictions for proactive measures such as early threat detection, immunization strategy planning, and device protection. By continuously refining predictions against benchmark results, this architecture enables precise, real-time cyber threat forecasting and supports effective, preemptive defense actions.

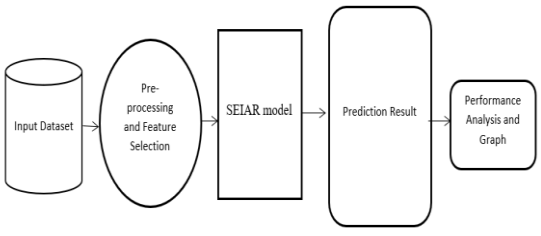

Fig 2.1 System Architecture

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808197

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. METHODOLOGY

The methodology for the proposed "Defense Strategies for Epidemic Cyber Security Threats" begins with the development of a compartmental SEIAR (Susceptible, Exposed, Infectious, Asymptomatic, Recovered) model to mathematically represent the propagation dynamics of cyberattacks, specifically DDoS assaults, across interconnected devices. Initial conditions and model parameters are defined, and the system of ordinary differential equations (ODEs) governing the SEIAR framework is solved using a numerical method, such as the fourth-order Runge-Kutta (RK-4), to generate a synthetic dataset representing various attack scenarios. This dataset serves as training input for a Feed-Forward Neural Network (FNN), optimized using the Backpropagated Levenberg–Marquardt Algorithm (BLMA), which acts as a surrogate solution generator for predicting future system states. The ANN is trained, validated, and tested against the RK-4 reference results, with performance evaluated using convergence analysis, regression metrics, and error histograms to ensure high prediction accuracy. Finally, the trained model is integrated into a decision and defense module, enabling early detection, simulation of immunization strategies, and informed countermeasure deployment to mitigate attack impacts in real time.

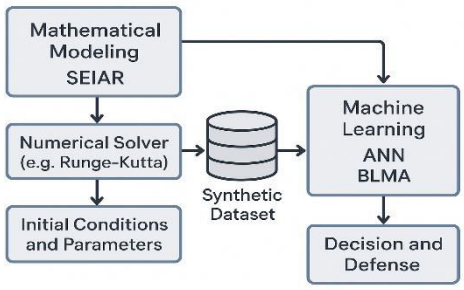

Fig 3.1 Methodology

IV. DESIGN AND IMPLEMENTATION

The design and implementation of the proposed system integrate mathematical modeling with advanced machine learning techniques to create an intelligent framework for defending against epidemic-style cyber security threats. The design phase begins with constructing the SEIAR compartmental model, which categorizes interconnected devices into Susceptible, Exposed, Infectious, Asymptomatic, and Recovered states, representing different stages of a cyberattack's lifecycle. This mathematical model is formulated as a system of ordinary differential equations (ODEs) that capture the dynamic interactions between these states under various attack parameters. In the implementation phase, the model is solved using the fourth-order Runge-Kutta (RK-4) method to generate a comprehensive synthetic dataset simulating diverse attack scenarios. This dataset is then used to train a Feed-Forward Neural Network (FNN), optimized through the Backpropagated Levenberg–Marquardt Algorithm (BLMA) for faster convergence and high-accuracy predictions. The implementation also involves iterative training, validation, and testing of the ANN, ensuring robustness through performance analysis, regression evaluation, and error distribution checks. Once trained, the system is deployed within a decision-support environment, enabling real-time prediction of attack spread, simulation of countermeasures, and automated recommendation of defense strategies to minimize system damage and improve resilience against large-scale cyber threats.

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808197

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

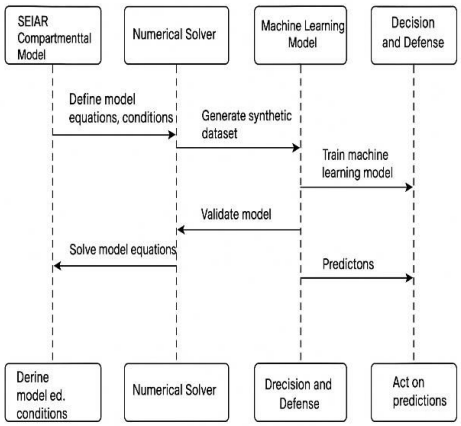

Fig 4.1 Sequential Diagram

The sequential diagram illustrates the step-by-step interaction between the key components of the epidemic cybersecurity defense system, showing how data and processes flow from one stage to another. It begins with the **SEIAR Compartmental Model**, where the model equations and initial conditions are defined to represent the cyberattack dynamics. This information is passed to the **Numerical Solver**, which processes the equations and generates a synthetic dataset simulating various attack scenarios. The dataset is then transferred to the **Machine Learning Model**, where it is used to train and validate a Feed-Forward Neural Network (FNN) optimized via the Backpropagated Levenberg–Marquardt Algorithm (BLMA). Once trained, the model produces predictions on future attack propagation patterns, which are sent to the **Decision and Defense** module. This final component analyzes the predictions and triggers appropriate defense strategies, such as mitigation measures or immunization protocols, to counter the cyber threat effectively. The diagram highlights the logical sequence and interaction flow, ensuring each stage builds on the outputs of the previous one for a complete defense lifecycle.

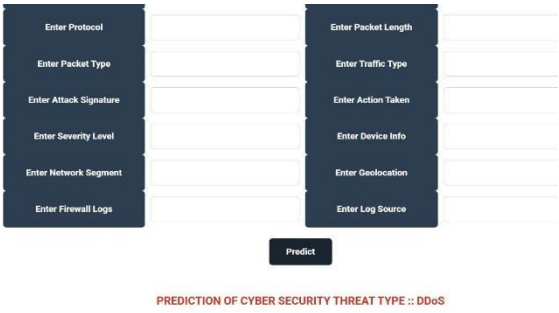

Fig 4.2 Working model

V. OUTCOME OF RESEARCH

The outcome of the research demonstrates that the integration of the SEIAR compartmental model with machine learning, specifically a Feed-Forward Neural Network (FNN) optimized using the Backpropagated Levenberg–Marquardt Algorithm (BLMA), provides an accurate and efficient framework for modeling, predicting, and mitigating epidemic-style cybersecurity threats such as DDoS attacks. The approach successfully generated surrogate solutions for complex ordinary differential equations governing cyberattack dynamics, achieving high regression values ($R \approx 1$) and minimal prediction errors compared to traditional numerical methods like the fourth-order Runge–Kutta. The trained model proved capable of forecasting the spread of attacks under varying conditions, enabling timely and precise decision-making for defense strategies. This research not only validated the robustness and reliability of ANN-based surrogate modeling in cybersecurity contexts but also provided a scalable methodology that can be adapted to different attack types and network environments, thereby significantly enhancing real-time cyber defense capabilities.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. RESULT AND DISCUSSION

The results of the study indicate that the proposed SEIAR-based epidemic cyber threat model, when integrated with a Feed-Forward Neural Network (FNN) optimized using the Backpropagated Levenberg–Marquardt Algorithm (BLMA), can accurately predict the propagation dynamics of large-scale cyberattacks such as DDoS. Comparative analysis with the fourth-order Runge–Kutta (RK-4) numerical method revealed that the ANN-based approach achieved high prediction accuracy, with regression values approaching 1 and absolute errors in the range of 10^{-5} to 10^{-8}, demonstrating its effectiveness as a surrogate solution method. Error histograms, convergence analysis, and fitting curves confirmed the robustness of the model, while performance metrics showed faster convergence and better handling of nonlinear interactions compared to traditional methods.

In the discussion, these findings highlight the capability of machine learning-based surrogate modeling to address the limitations of purely numerical solvers by providing flexible, scalable, and real-time prediction capabilities. The research validates that combining mathematical modeling with AI can enable proactive cyber defense, as the system can simulate varying attack parameters, predict potential impacts, and guide the deployment of countermeasures before severe damage occurs. Moreover, the framework's adaptability suggests it can be extended to other cyber threat types and network architectures, making it a valuable tool for enhancing national and organizational cybersecurity resilience.

VII. CONCLUSION

In this work, we use one of the intelligent techniques based on an artificial neural network to investigate the mathematical model that simulates Pony Stealer (malware attack) in the connection that has been developed. The mathematical model is compartmental since asymptomatic devices, as well as Exposed Susceptible, Susceptible, Infectious, and Recovered, have all been regarded as separate systems linked by a single server. Some infections can propagate through asymptomatic devices without causing symptoms. These viruses are identified through infectious devices. This extra type of device is crucial to include in cyber security models since many cyberattacks are intended to control the device system in an anonymous manner in order to collect personal data [68]. Such real-world processes are regulated by a set of ordinary differential equations. Deep neural learning-based machine learning techniques [69], have been applied to solve the system of ordinary differential equations underlying the epidemic model. In the ANN approach, we use one hidden layer for sample points of each equation in Matlab, and using the RK-4 approach, a reference solution is generated, which is later analysed using the Levenberg-Marquardt algorithm's training, testing, and validation procedures. Since the approximate solutions and analytical answers correspond with the lowest absolute errors when compared to state-ofthe-art techniques, the detailed graphical analysis shows that the suggested method is accurate and effective. Additionally, performance indicator values are getting closer to zero, demonstrating flawless outcome modelling.

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, Art. no. 113425.
[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 multiagent coordination mechanisms," IEEE Trans. Ind. Informat., vol. 19, no. 9, pp. 9821–9832, Sep. 2023.
[5] M. Aizat, A. Azmin, and W. Rahiman, "A survey on navigation approaches for automated guided vehicle robots in dynamic surrounding," IEEE Access, vol. 11, pp. 33934–33955, 2023.
[6] R. Chengoden, N. Victor, T. Huynh-The, G. Yenduri, R. H. Jhaveri, M. Alazab, S. Bhattacharya, P. Hegde, P. K. R. Maddikunta, and T. R. Gadekallu, "Metaverse for healthcare: A survey on potential applications, challenges and future directions," IEEE Access, vol. 11, pp. 12765–12795, 2023.
[7] J. Callenes and M. Poshtan, "Dynamic reconfiguration for resilient state estimation against cyber attacks," IEEE Trans. Emerg. Topics Comput., pp. 1–12, Apr. 2023.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com