IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 8 November 2023, accepted 30 December 2023, date of publication 4 January 2024,
date of current version 11 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3349660

RESEARCH ARTICLE

Defense Strategies for Epidemic Cyber Security Threats: Modeling and Analysis by Using a Machine Learning Approach

MUHAMMAD SULAIMAN[1], MUHAMMAD WASEEM[1], ADDISU NEGASH ALI[2], GHAYLEN LAOUINI[3], AND FAHAD SAMEER ALSHAMMARI[4]

[1]Department of Mathematics, Abdul Wali Khan University Mardan, Mardan, Khyber Pakhtunkhwa 23200, Pakistan
[2]Faculty of Mechanical and Industrial Engineering, Bahir Dar Institute of Technology, Bahir Dar University, Bahir Dar 6000, Ethiopia
[3]College of Engineering and Technology, American University of the Middle East, Egaila 54200, Kuwait
[4]Department of Mathematics, College of Science and Humanities in Alkharj, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia

Corresponding author: Addisu Negash Ali (addisuan@gmail.com)

This work was supported by Prince Sattam bin Abdulaziz University under Project PSAU/2023/R/1445.

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 backpropagated 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. Subsequently, we endeavor to analyze the surrogate solutions obtained for the system and determine the stability of our approach. Moreover, we aim to ascertain fitting curves to the target solutions with minimum errors and achieve a regression value of 1 for all the predicted solutions. 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.

INDEX TERMS Mathematical modeling, epidemic model, cybersecurity, compartmental model, optimization, numerical solution, artificial neural network, Levenberg-Marquardt algorithm (LMA).

I. INTRODUCTION

The progress of technology allows an industry to function quicker than ever before. There are technical tools, such as virtual meeting software, that enable high-level mobility within the structure of an industry. Different forms of software can operate on a computer system, including utility software and application software, and every place is beginning to substitute software in place of humans [1]. Without technology, this is nearly impossible since there

The associate editor coordinating the review of this manuscript and approving it for publication was Yang Liu.

will be a lot of delay. Technology has a significant role in increasing efficiency [2]. This means that people in an industry must be technologically prepared and accomplish their responsibilities significantly more quickly. Software is used to administer and regulate the country's entire economy [3]. Computer software is used in different industries in our lives. In the robotics industry [4], highly sensitive software is used to boost worker productivity in the robotic universe, agriculture [5], and medicine by enhancing the ability to analyse medical information [6], agricultural production, communication, and easy connection and sharing.

But one of the major drop bags of software is hacking or cyberattacks. In paradigms, the risk associated with these cyberattacks, such as the industry 4.1, is just named in [7] and [8]. To present an industrial security solution tailored exclusively for virtual reality (VR) devices. The emphasis is on solving the security difficulties and risks associated with virtual reality technology, with the goal of ensuring the integrity, confidentiality, and availability of data and systems in industrial settings [9]. A cyberattack is a cybercriminal attack carried out with one or more computers against a single or several computers or networks [10]. Cybercriminals utilize a variety of methods to launch their assaults, including DoS and DDoS attacks, middle (MitM) attacks, man-in-the-phishing, drive-by threats, spear-phishing attacks, SQL injection attacks, cross-site scripting (XSS) attacks, password attacks, eavesdropping attacks, malware attacks, and the use of carefully picked appropriate information. Framework for the Internet of Things (IoT) functioning in heterogeneous small cell networks [11], that is energy-efficient [12]. In order to improve the overall performance and sustainability of IoT applications [13], in a variety of network environments, the key goal is to optimize energy consumption by effectively managing communication resources and network deployment [14]. As a result of a cyberattack Corrupting address data and papers might have extended repercussions for your company's financial health. A commonly used control approach, model predictive control (MPC) [15], may address optimisation control issues with constraints. They have been widely used in modern industrial control systems. Even though some damaged data could be recovered, doing so frequently involves the help of IT specialists and consumes time and resources that your company could be using elsewhere. Trojan horses, or worms, are computer programs that resemble how epidemics propagate among people [16]. A computer virus, such as the human virus, may propagate across an interconnected computer system and transmit viruses from one person to another. Data loss prevention is crucial since erased files and information often cannot be recovered. With the ability to access Internet services, smartphones have developed into indispensable personal gadgets [17]. App use traces can be gathered by app developers and service providers to show links between users, applications, and handsets [18]. This survey compiles major trends in smart phone app usage behaviours as well as cutting-edge technology, such as surveys, monitoring applications, public opinion [19], network providers, 3D Point Cloud Upsampling [20], [21]and app stores.

Various mathematical models for malware spread have been suggested by various researchers [22], [23]. In the field of machine learning, especially when working with sensitive or proprietary models [24], model stealing attacks highlight the necessity for strong security measures. The improvement of the security of uplink non-orthogonal multiple access (NOMA) systems is the primary emphasis of Physical Layer Security [25]. It suggests utilising energy-harvesting yammers to increase physical layer security while preserving system functionality. It also emphasises the significance of continued research and development of appropriate remedies to protect against such assaults and preserve model producers' intellectual property [26]. These mathematical models represent the different scenarios that accrue in the system during a cyberattack. This model is mostly compartmental and deterministic. Because gadgets are categorised into separate sections, they are compartmental models: (S) Susceptible(Total), (I) Infected,(A) Asymptomatic, (E) Exposed, and (R) Recovered among others. These compartments can be obtained by different types of dynamics: SIS, SEIR, SCIR, SI, and SIR just a few names from [23]. These models are important in a variety of domains because differential equation theory may be used to investigate the performance and interaction of their solutions. Discrete techniques, including the Euler, Crank-Nicolson, and Runge-Kutta methods, among others [27] are frequently used to solve ODEs. But in this case, the solutions to a system are obtained by the machine learning method. This procedure achieves a solution that is much more closely related to a practical mathematical model. To overcome the constraints of solutions acquired via the machine learning method, artificial neural network (ANN) [28], [29] witch approaches have been suggested in [30] and [31]. It has been shown that an ANN with a hidden layer and a linear activation function may approximate any function when there are a lot of hidden neurons [32]. Furthermore, the model will be solved and the results will be explained using a deep learning-based approach [33].

A. RESEARCH CONTRIBUTION

Our research contribution 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.

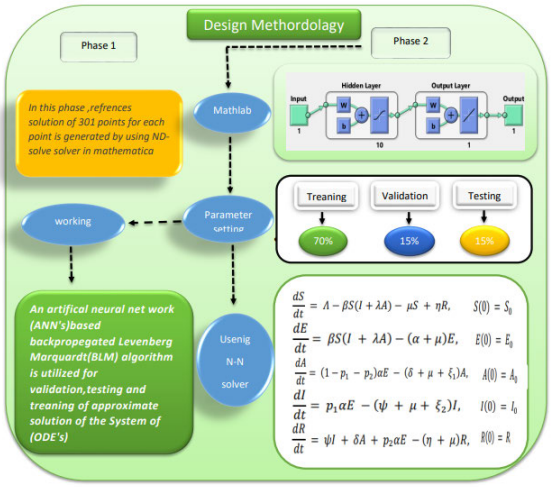


FIGURE 1. Mechanism of the BLMA for the solution of the system of ODEs.

B. TECHNICAL DETAIL

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 well-established 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.

C. EXPERIMENTAL EVALUATION GUIDELINES

- The SEIAR compartmental model is used to depict the various hardware employed during the cyberattack. The variables utilized in the differential equations are included in the detailed description of the model.
- The study presents the numerical solution strategies used to discover the general solution to differential equations, including the Machine learning, ANN, and Runge-Kutta methods. The backpropagated Levenberg-Marquardt algorithm (BLMA) is also used to solve numerical problems using feed-forward neural networks (FNNs).
- Statistical analysis: The outcomes of the trials should be analyzed statistically to see if the variations in performance across models are statistically significant.
- The study presents the testing, validation, and training of the reference data set in order to give the value of the approximate solution using BLMA. Additionally, a thorough description is given of the testing, validation, and training procedures.
- The study employs a number of methods to assess the robustness and correctness of the design strategy, including convergence analysis, error histograms, regression analysis, and curve fitting. These methods are used for the analysis of each differential equation.

D. COMPARATIVE EXPERIMENTS FOR SEIAR MODEL

Comparative experiments can give important insights into a proposed model's complex nature, but they are not always feasible or practicable. In our example, we created a revolutionary SEAIR cyber security model based on a machine learning process that especially targets DDOS assaults. We think that our model offers a novel and effective strategy for mitigating such threats and that it has the potential to dramatically improve computer system security. We also tested our approach against the well-known RK-4 method and obtained good results. While we recognize the value of comparable tests, we are confident in the advanced nature of our suggested model based on rigorous mathematical analysis and detailed performance evaluation.

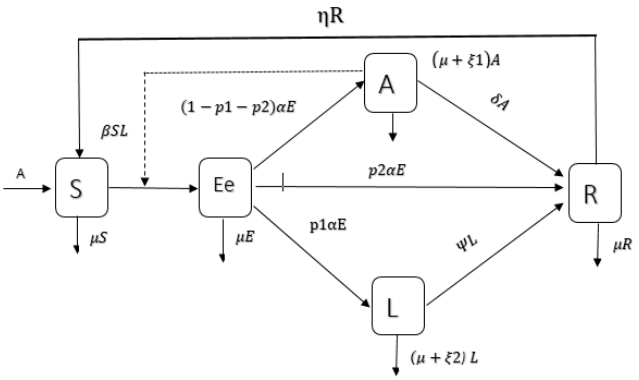


FIGURE 2. Flowchart for SEIAR Model.

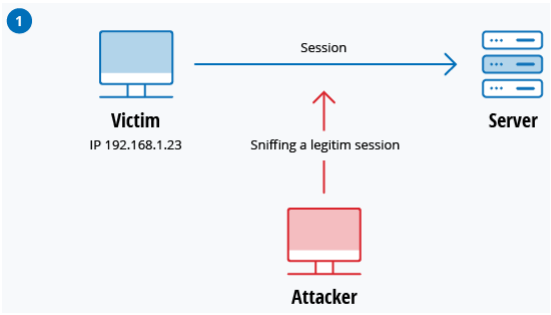


FIGURE 3. (ARPs) injection-based active sniffing attacks.

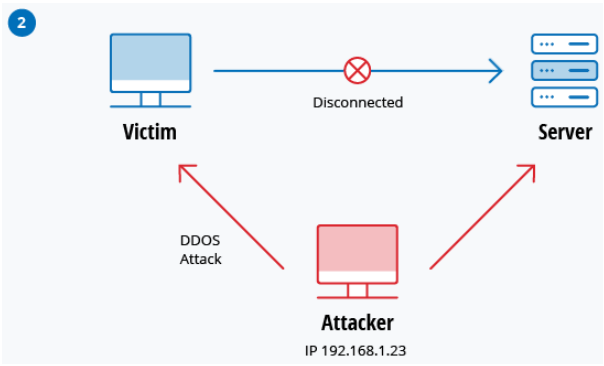


FIGURE 4. Damaged system due to injection-based sniffing attacks.

II. ESTABLISHMENT OF MATHEMATICAL MODEL

Mathematical modelling is the process of describing a real-world problem in mathematical terms and enabling a systematic understanding of the system modelled. Artificial neural networks (ANNs) are utilised as a machine learning approach based on the monitored learning of neurons to investigate cyberattacks in a variety of systems. This is a serious threat because the cyberattack creates destabilisation. The attacker uses a different path to trace the manipulated data. In the case of a DDOS attack [37], the attacker is sniffing a legitim session between the server and the victim to trace the IP of the system, as shown in Figure (3), and finally, the attacker disconnected the victim (system) from the server and got the IP from the

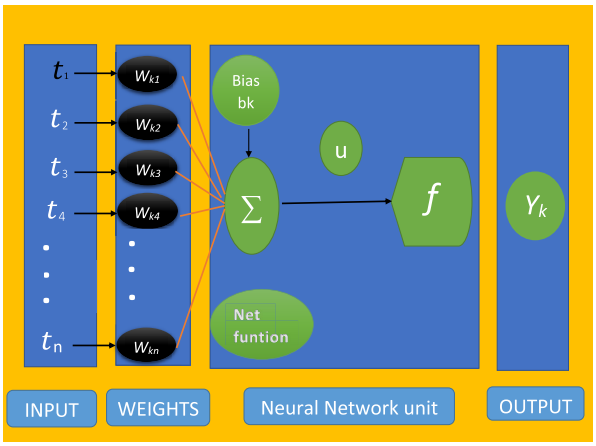


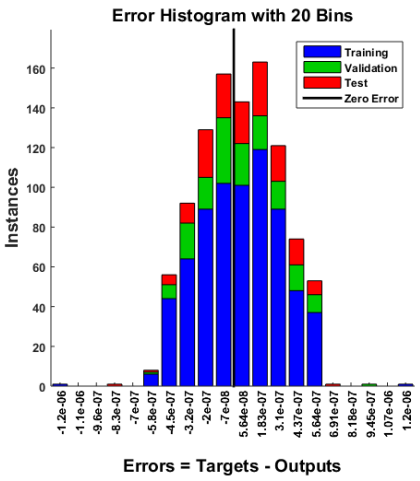
FIGURE 5. The architecture of a single neural network.

TABLE 1. Parameter Interpretation.

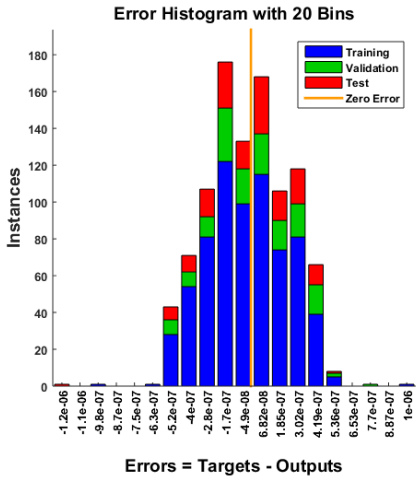
Index	description
layer structure	One Hidden layer for each input and output
Hidden neuron	10 to 20
Validation	10-FLOD CROSS VALIDATION
Input grid	1001 sample points
Output grid	16×201
Training samples	70%
Validation samples	15%
Testing samples	15%
Leaning methodology	Levenberg-Marquardt
Label target data	Created with Adams numerical method

victim, as shown in Figure (4). this services is also a variety of location-base services (LBSs) [38]. Visual tracking that is now focused on segmentation-driven frameworks incurs high computing costs, which create a bottleneck in actual application [39].

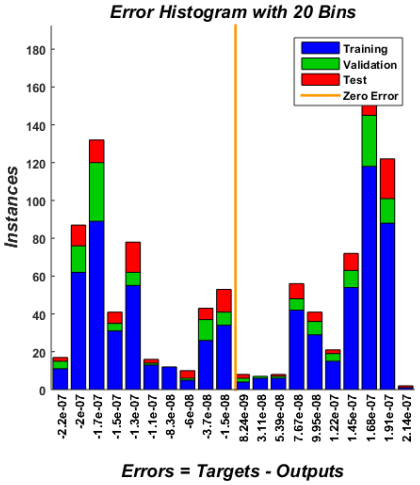
The proposed model is a compartmental SEIAR model, which is an acronym that stands for Susceptible, Exposed, Infectious, Asymptomatic, and Recovered, as depicted in Figure (2). Table (17) describes the notation for the SEIAR model. In this compartmental SEIAR model, I is infectious devices and the addition of infectious devices is represented by A. They may be considered to have a reduced $\beta\lambda$ transmission rate when it comes to being infectious, as evidenced by the results shown in Figure (2). A dashed line in the same illustration serves as a representation of this. During the attack, although devices were infected, exposed devices were not yet infectious. In a DDOS attack, PαE acquires short immunity. If the security software resists the attacker



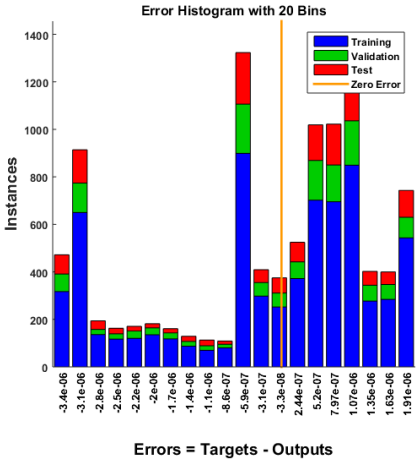
(a)



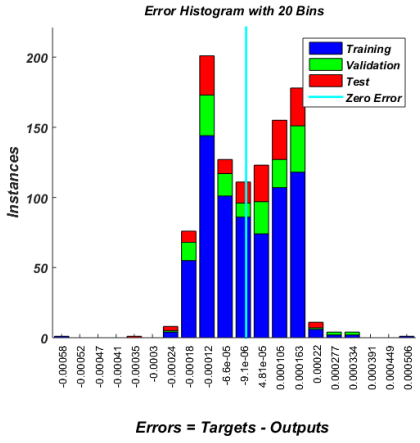
(b)



(c)



(d)



(e)

FIGURE 6. Histogram analysis for the system of (ODE) of case 1.

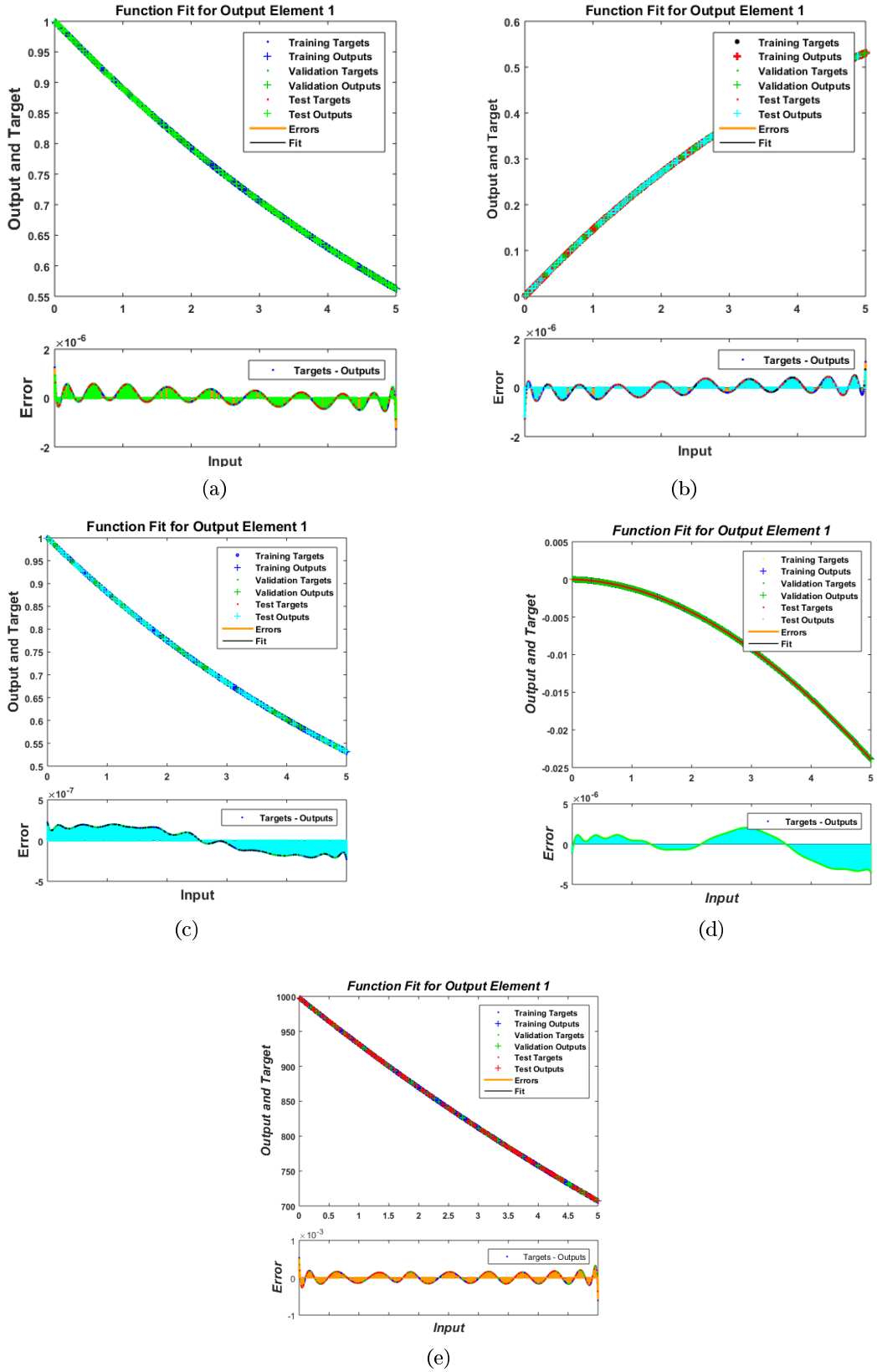
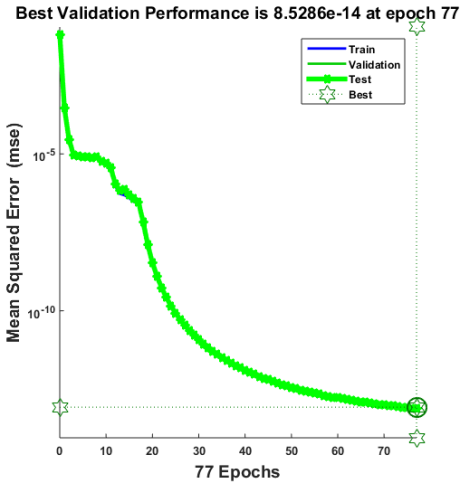
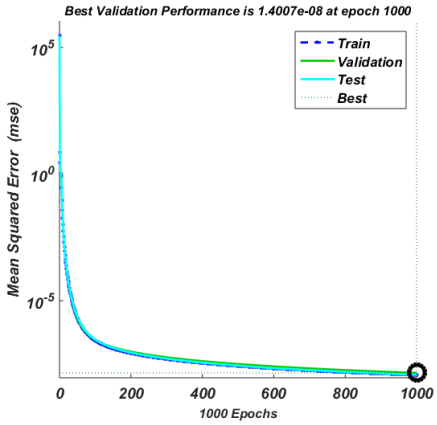


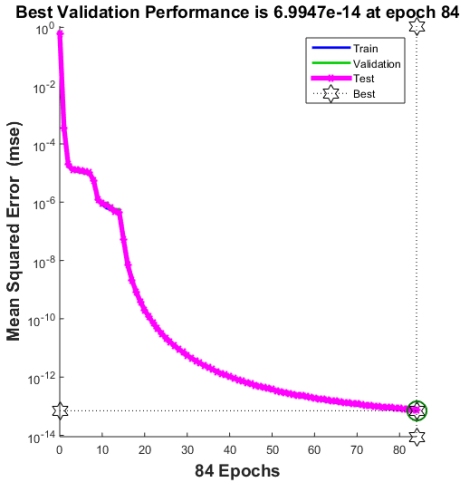
FIGURE 7. Fitting analysis for the system of (ODE) of case 1.



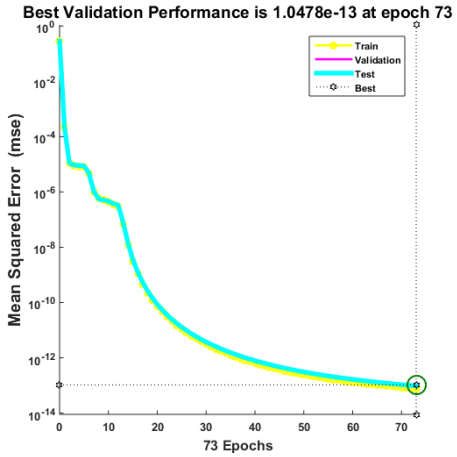
(a)



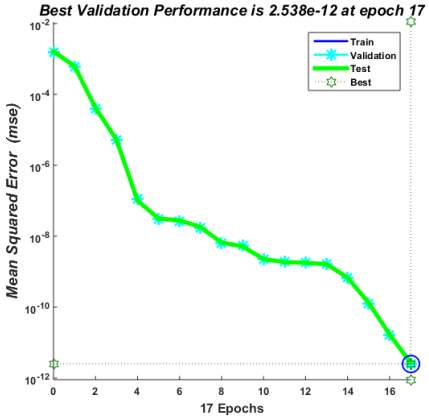
(b)



(c)

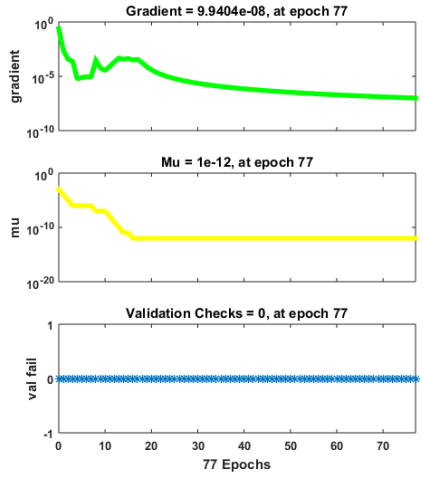


(d)

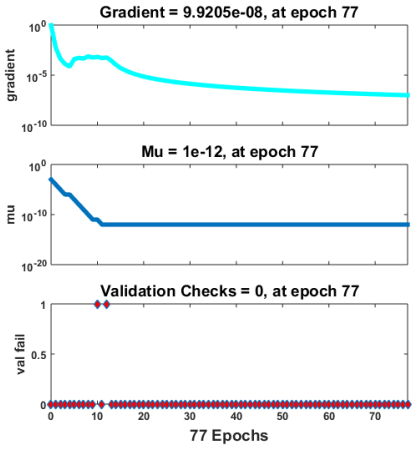


(e)

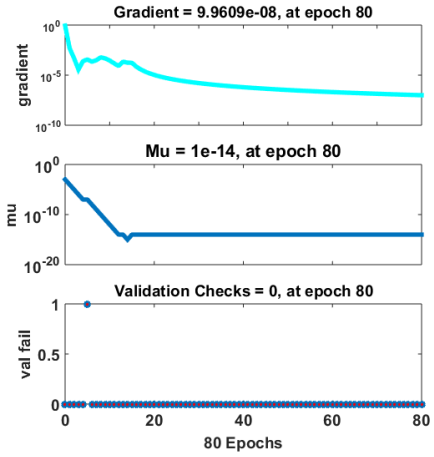
FIGURE 8. Analysis of performance function in terms of mean square error for the system of (ODE) of case 1.



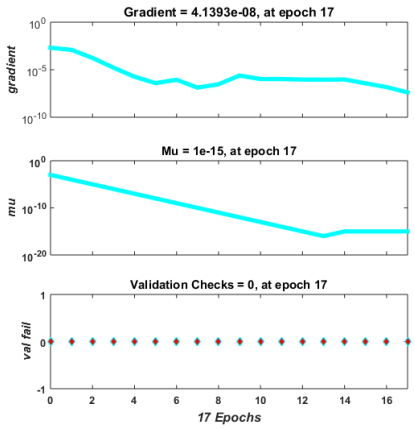
(a)



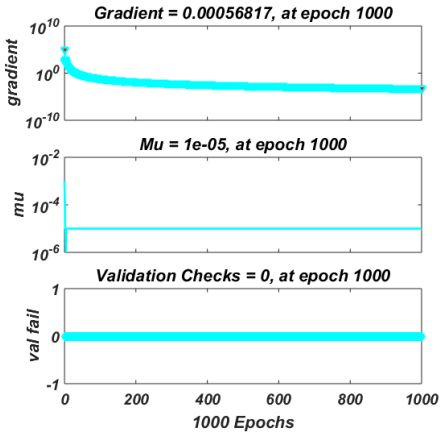
(b)



(c)



(d)



(e)

FIGURE 9. Training analysis for the system of (ODE) of case 1.

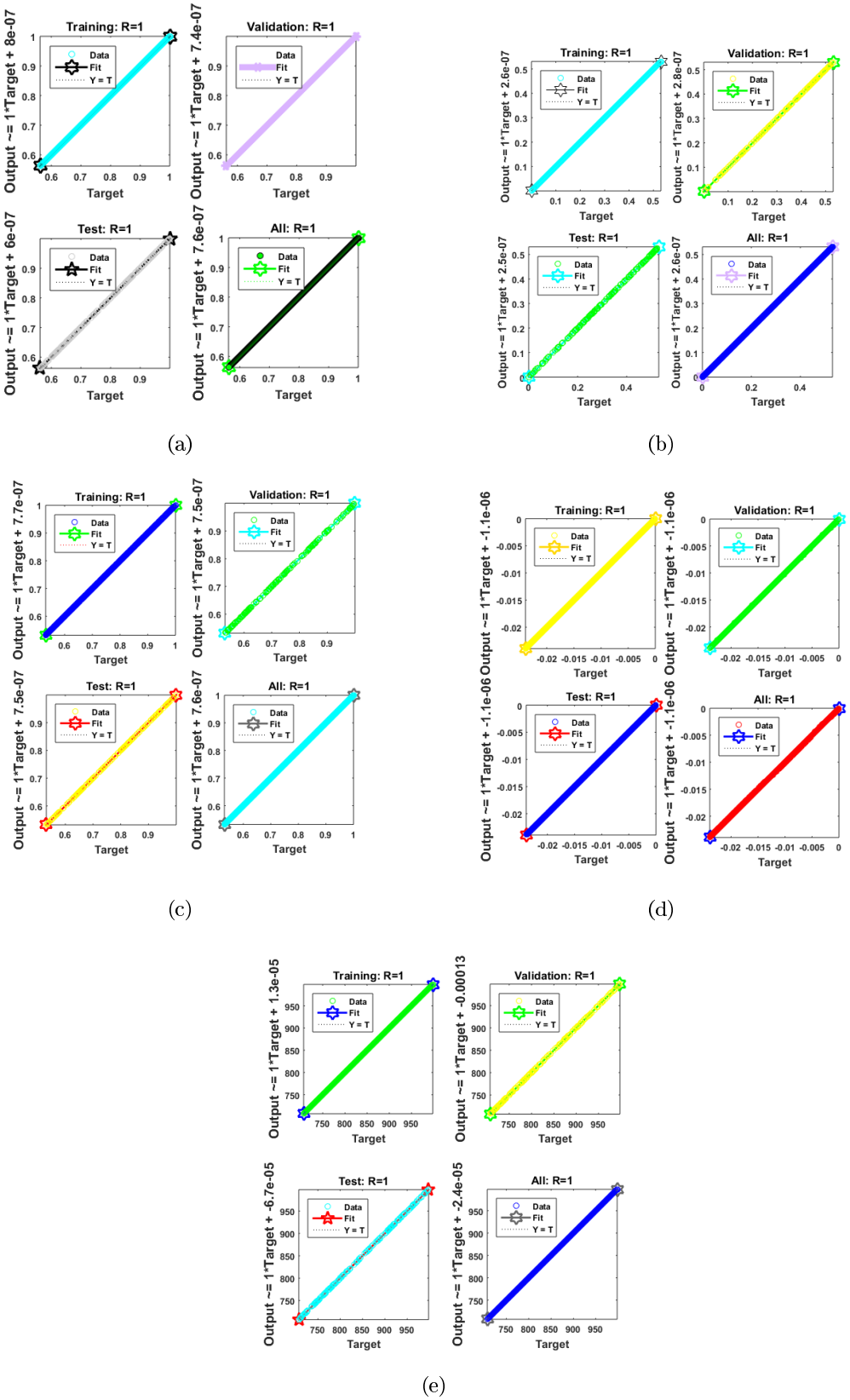


FIGURE 10. Regression analysis for the system of (ODE) of case 1.

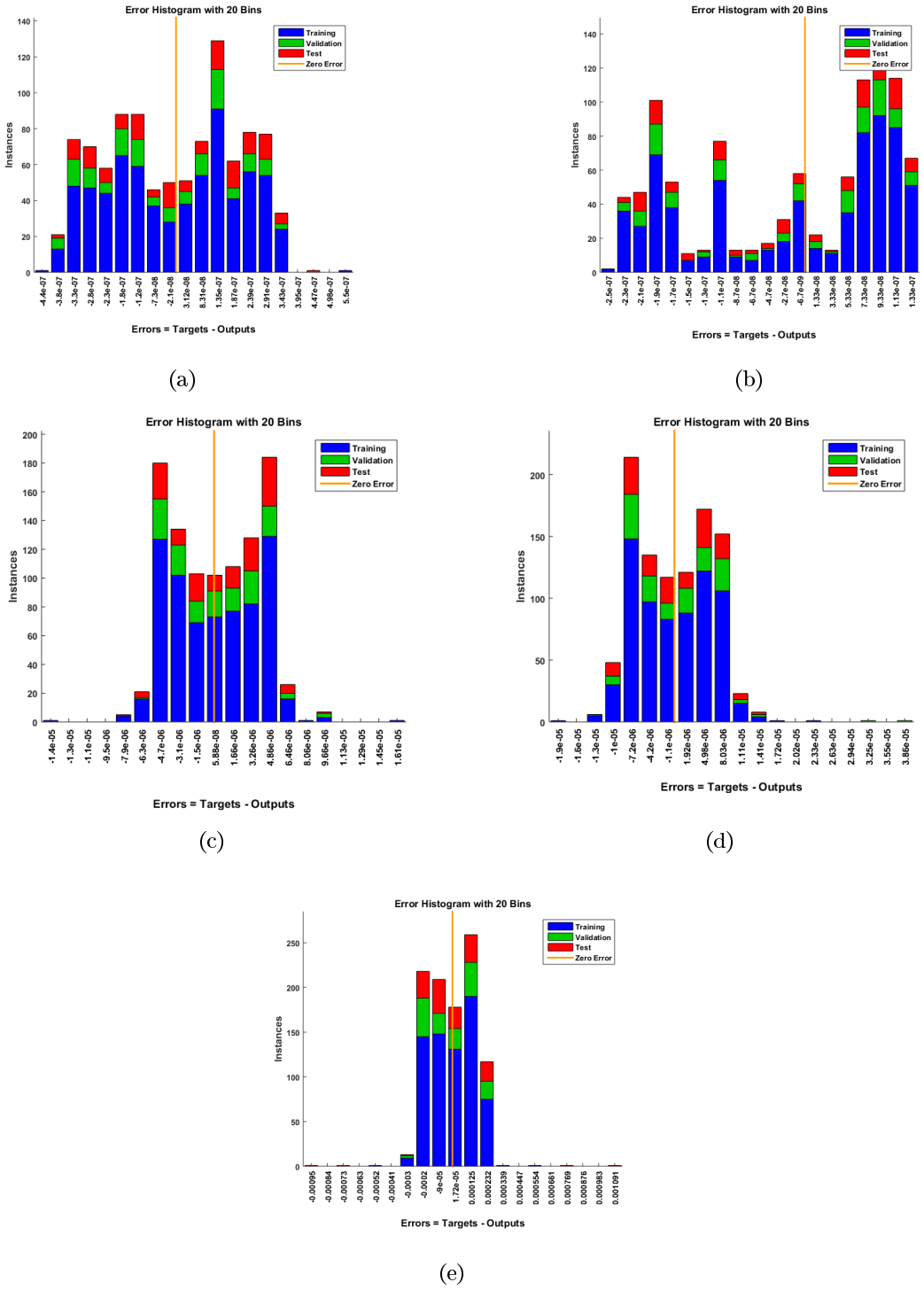


FIGURE 11. Histogram analysis for the system of (ODE) of case 2.

software to remove the action of a DDOS attack, such a time-sensitive immunity will exist at the rate δA and ψI, accordingly. In the absence of this, devices will be eliminated from the computer at the rate of $(\mu + \xi_1)$ and $(\mu + \xi_2)$I where ξ_1 and ξ_2 the attack on the A and I compartment results in device damage rates, μ is the normal device damaged. After losing their temporal susceptibility, recovered devices finally return at an η rate towards the unprotected compartment. The corresponding system of ordinary differential equations represents the mathematical dynamic model of the preceding

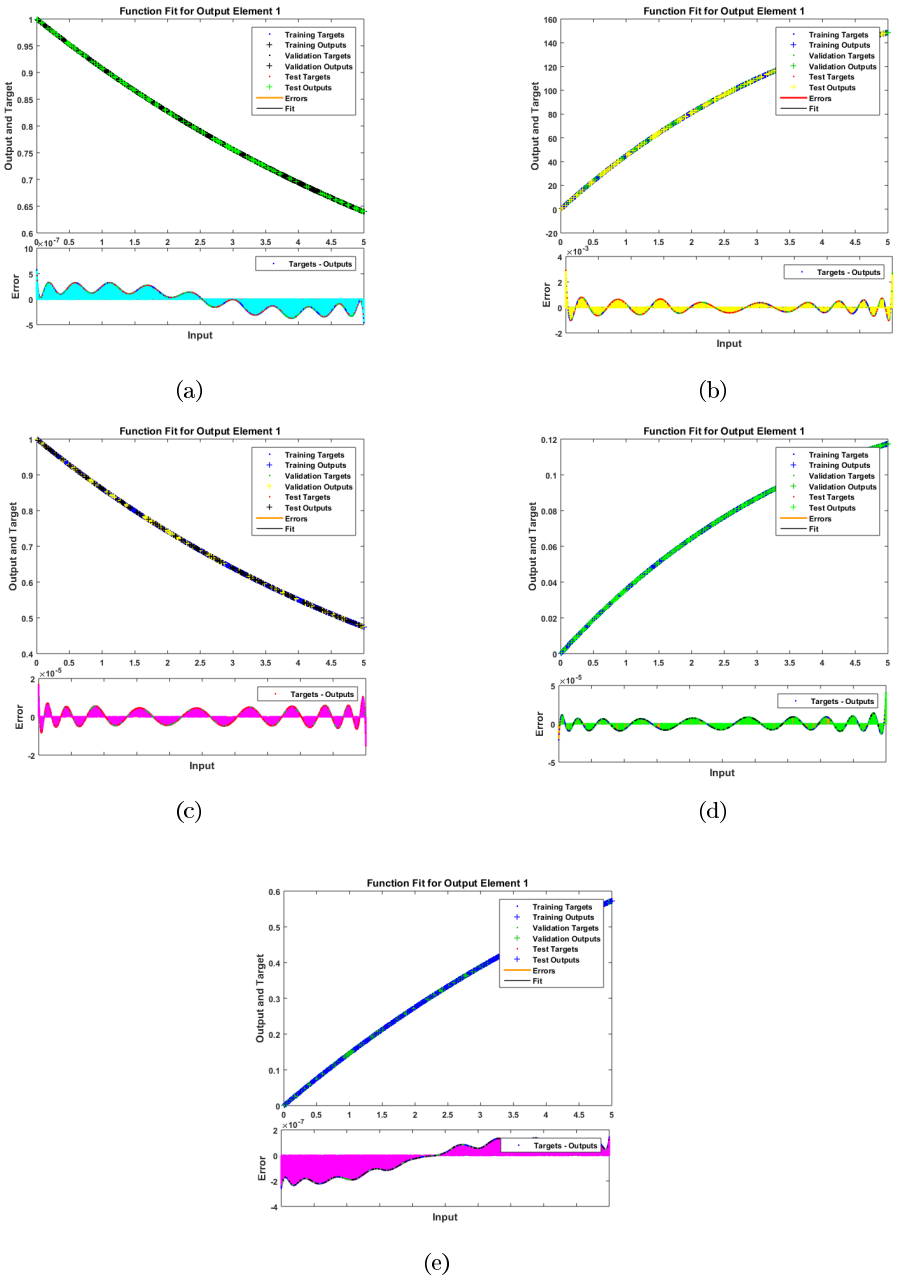


FIGURE 12. Fitting analysis for the system of (ODE) of case 2.

Figure (2):

$$\begin{cases} \dfrac{dS}{dt} = A - \beta S(I + \lambda A - \mu S + \eta R), & S(0) = S_0 \\ \dfrac{dE}{dt} = \beta S(I + \lambda A) - (\alpha + \mu)E, & E(0) = E_0 \\ \dfrac{dI}{dt} = P_1 \alpha E - (\psi + \mu + \xi_2)I, & I(0) = I_0 \\ \dfrac{dA}{dt} = (1 - P_1 - P_2)\alpha E - (\delta + \mu + \xi_1)A, & A(0) = A_0 \\ \dfrac{dR}{dt} = \psi I + \delta A + \delta P_2 \alpha E - (\eta + \mu). & R(0) = R_0 \end{cases} \tag{1}$$

The total number of devices (N) represents infectious and infected devices in these compartments.

$$N(t) = S(t) + I(t) + E(t) + R(t) + A(t). \tag{2}$$

The behaviour of the model was simulated with the following 1000 connected devices: $S(t_0) = 998$, $E(t_0) = 0$, $I(t_0) = 1$, $A(t_0) = 1$, $R(t_0) = 0$. All devices were assumed to be susceptible at time $t = t_0$.

III. DESIGN METHODOLOGY

This section discusses a machine learning strategy based on an artificial neural network and emphasises guided neural

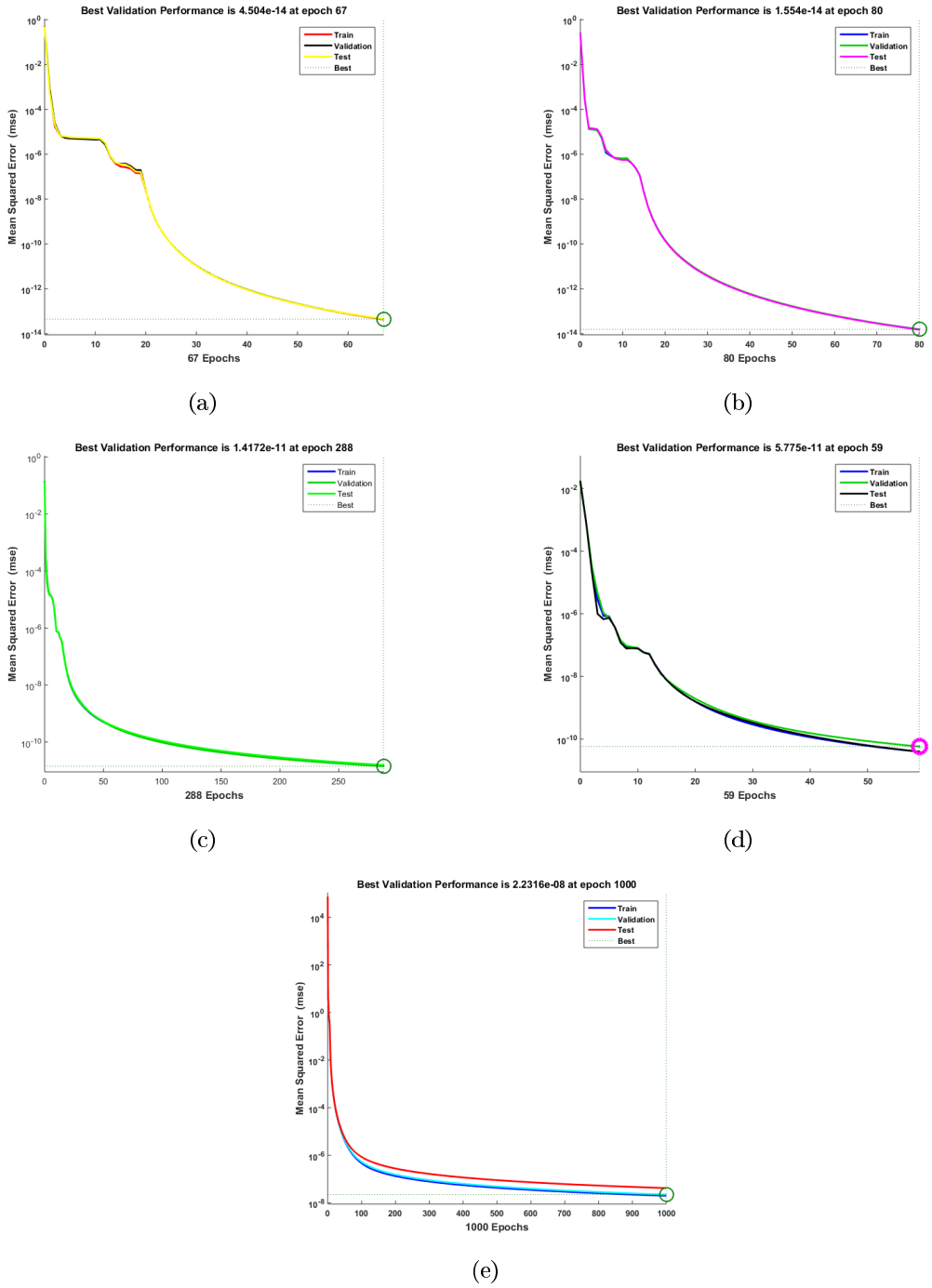


FIGURE 13. Analysis of performance function in terms of mean square error for the system of (ODE) of case 2.

processes (ANN). An ANN is a network of interconnected neurons that can analyse several inputs but only generate one output. Using a multi-layer perceptron, we may optimise the number of hidden units (MLP). MLPs are artificial neural networks composed of interconnected nodes that perform mathematical operations on input data to generate outputs [40]. It is frequently referred to as the Feed-Forward Neural Network (FNN). In this instance, the hidden layer contains neutrons from the [32]. This system of differential equations is solved using a different strategy, such as the Metropolis-Hastings technique derived from the Markov Chain Monte Carlo discussed in [41]. To reduce the log loss function and achieve a solution closer to the real system of ordinary differential equations (ODEs), In the previous

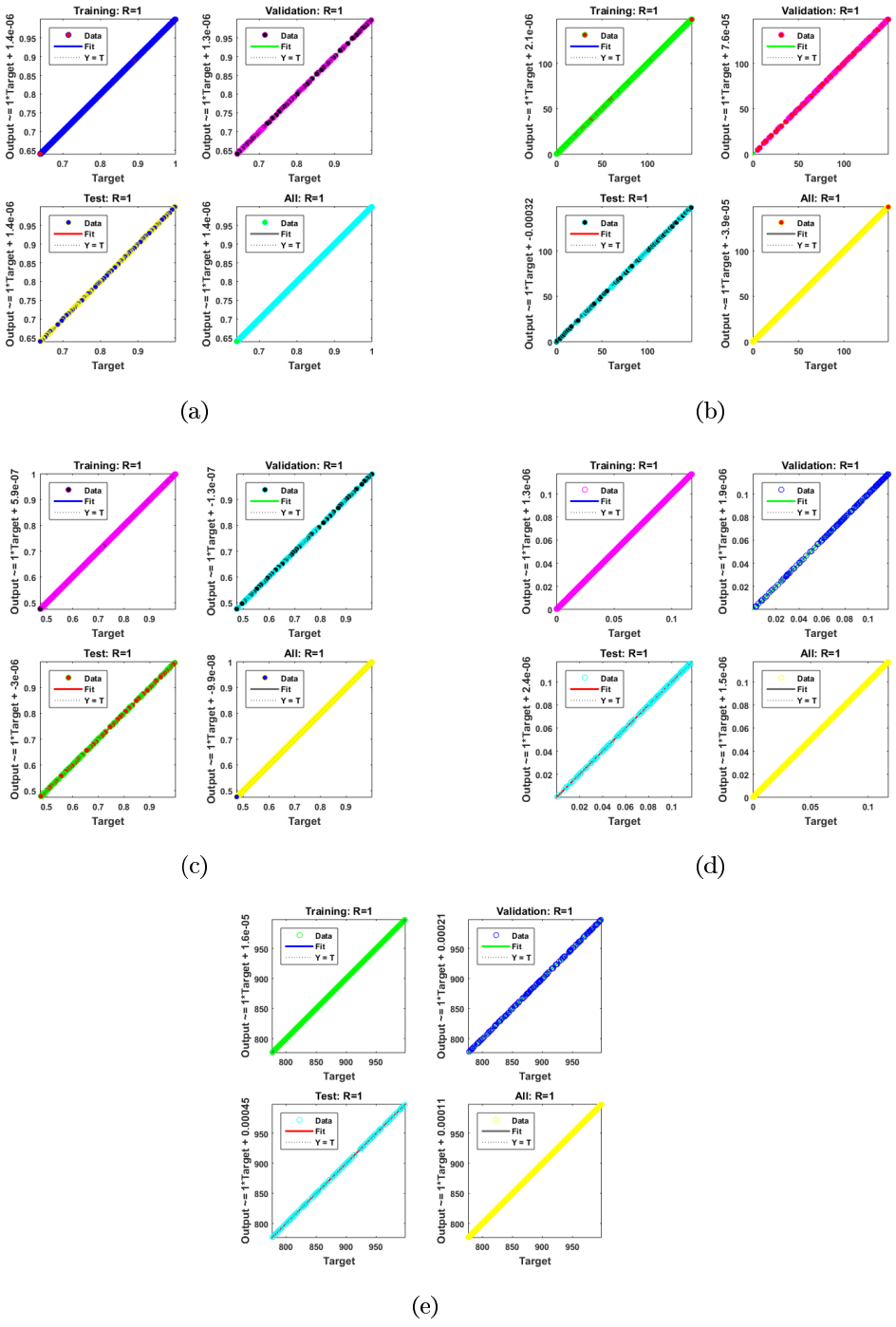


FIGURE 14. Regression analysis for the system of (ODE) of case 2.

work DDOS model is solve by employed three optimization techniques such as Conjugate-Gradient method (CG) [42], Broyden-Fletcher-Goldfarb-Shanno method (BFGS) [43], and Limited-Memory BFGS for Bound-constrained methods (L-BFGS-B) [44].

In this paper, we employ a modern machine learning technique, Artificial Neural Networks (ANNs). ANN is an effective machine learning approach for handling and processing linear scenarios, converging at a faster rate than other methods. ANNs are sophisticated nonlinear statistical models that leverage complex interactions between inputs and outputs to identify new surrogate solutions System of ODEs. Similar to neurons in the nervous system, ANNs consist of input, hidden, and output layers and

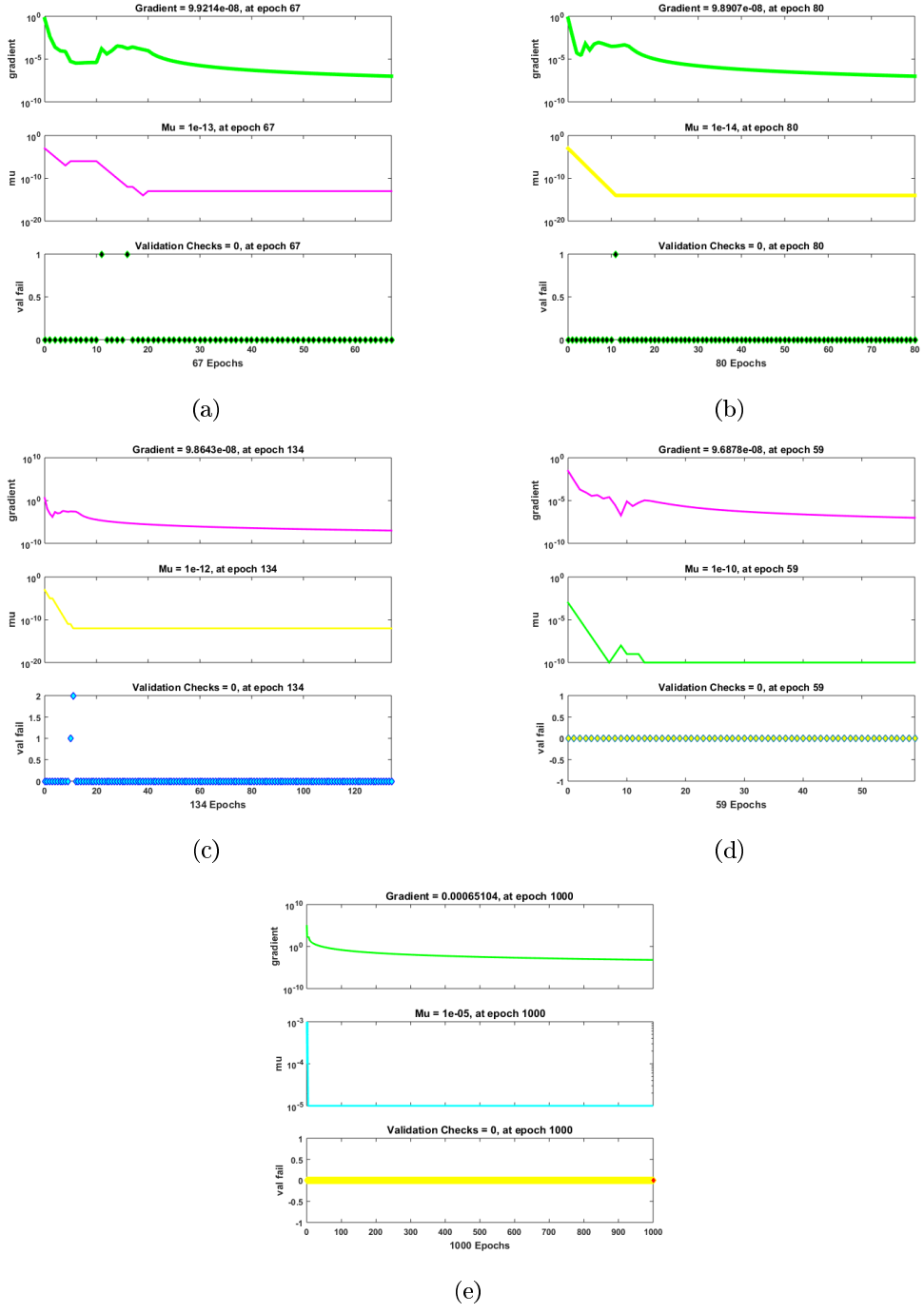


FIGURE 15. Training analysis for the system of (ODE) of case 2.

utilize deep learning methods with the help of activation functions. The algorithm receives input data, processes it, and generates an output. These algorithms are used for different optimization problems, including neural networks, and are effective for training different types of neural networks. The ANN is thought to be an efficient optimization method. Following the usual MLP architecture with one hidden layer.

$$N_j = \sum_{i=1}^{n} (W_{ij} X_i + b_j), \tag{3}$$

where, respectively, w_{ij} represents connection weights, bj denotes biassed vectors, and xi denotes inputs. A log-sigmoid activation function is used in the feed-forward neural network

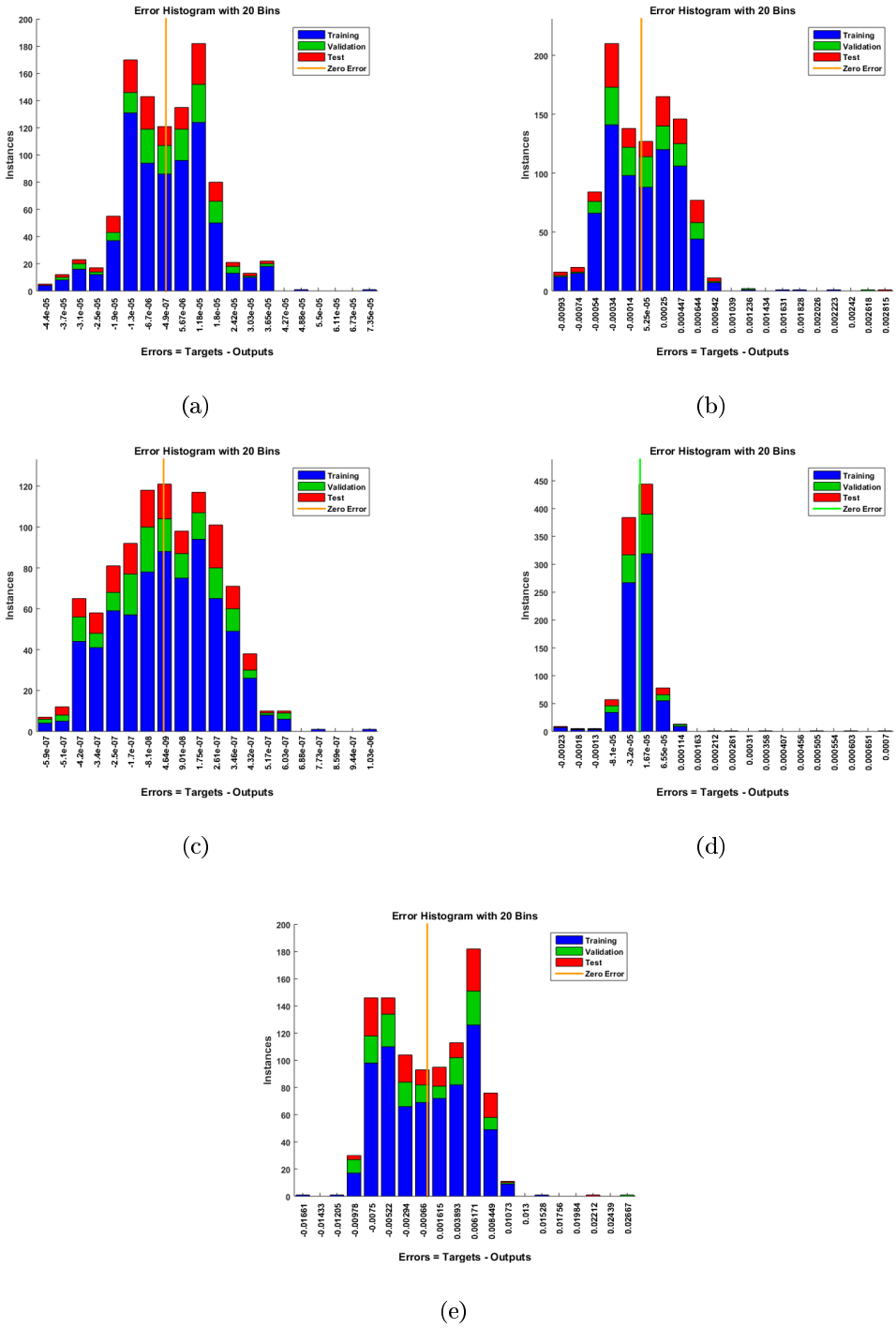


FIGURE 16. Histogram analysis for the system of (ODE) of case 3.

model, which is defined as:

$$f_j(x) = \frac{1}{1 + e^{-N_j}}. \tag{4}$$

The implementation of FNN-LMA is carried out in two stages, and the complete workflow of the design algorithms is depicted in Figure (1). Figure (1) depicts the mechanism used to obtain the surrogate solution. And how to Create an initial data set using a standard machine learning technique, and compare it with the fourth-order Runge-Kutta algorithm. Train a feedforward neural network (FNN) using the initial data set [45]. Use the FNN to predict the solution to the ODE system at future time steps using an Adams-Bashforth predictor. Validate and refine the FNN using a testing data

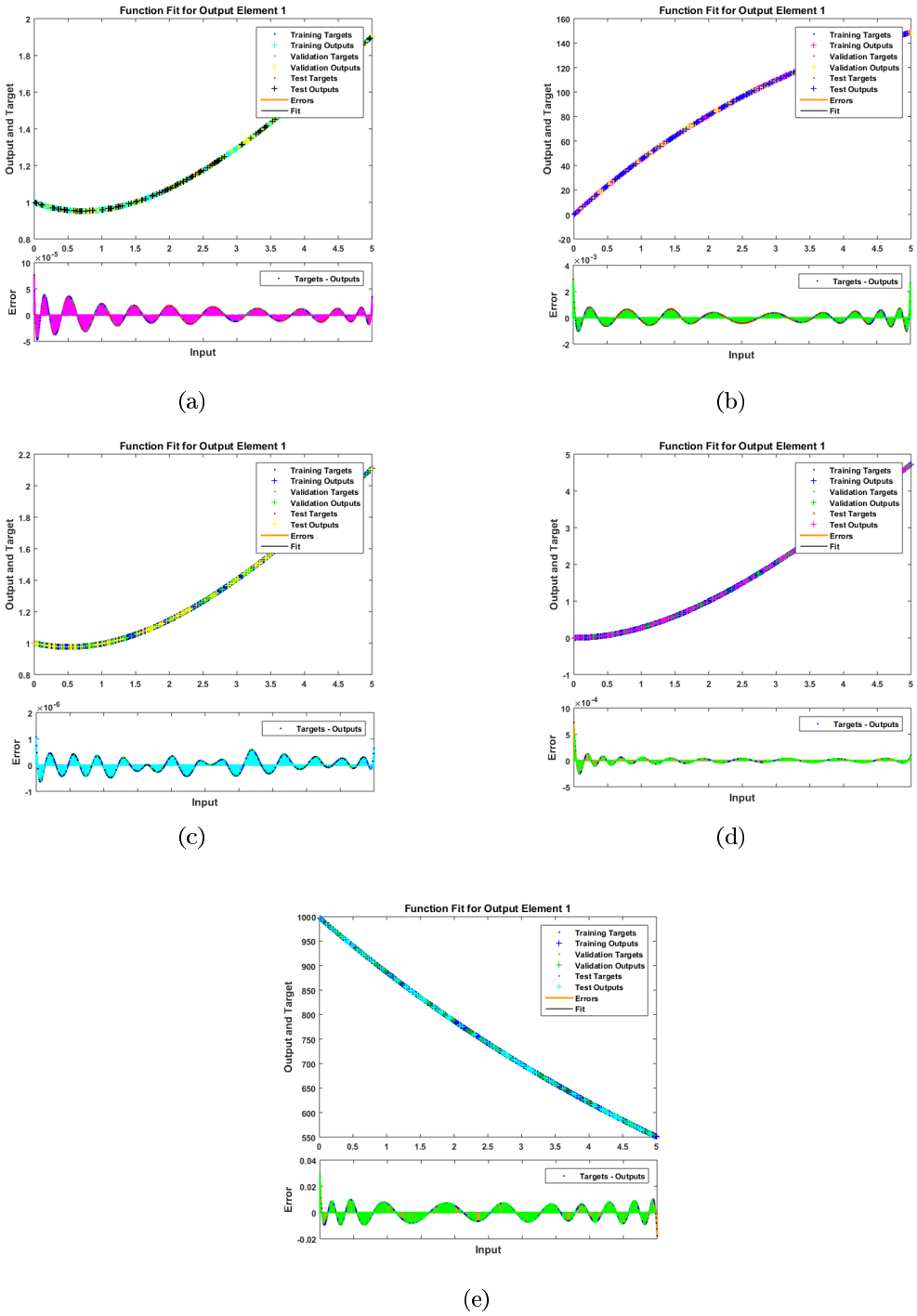


FIGURE 17. Fitting analysis for the system of (ODE) of case 3.

set. The FNN is refined using an error backpropagation algorithm to minimize the error between the predicted and actual solution. This figure displays the whole workflow of the design methods. In the first stage, a numerical solution is generated using the Runge-Kutta algorithm of fourth order in Mathematica's ''ND Solve'' module to generate an initial data set (Rk4).

• In the second step, the BLM method is executed with the appropriate hidden neuron settings and test data in the second phase using the ''nftool'' programme included in the MATLAB package. Furthermore, BLM exploits a reference solution and the testing, validation, and training processes to provide approximations for various system of equations instances. The NNs-LMT technique uses a single neural

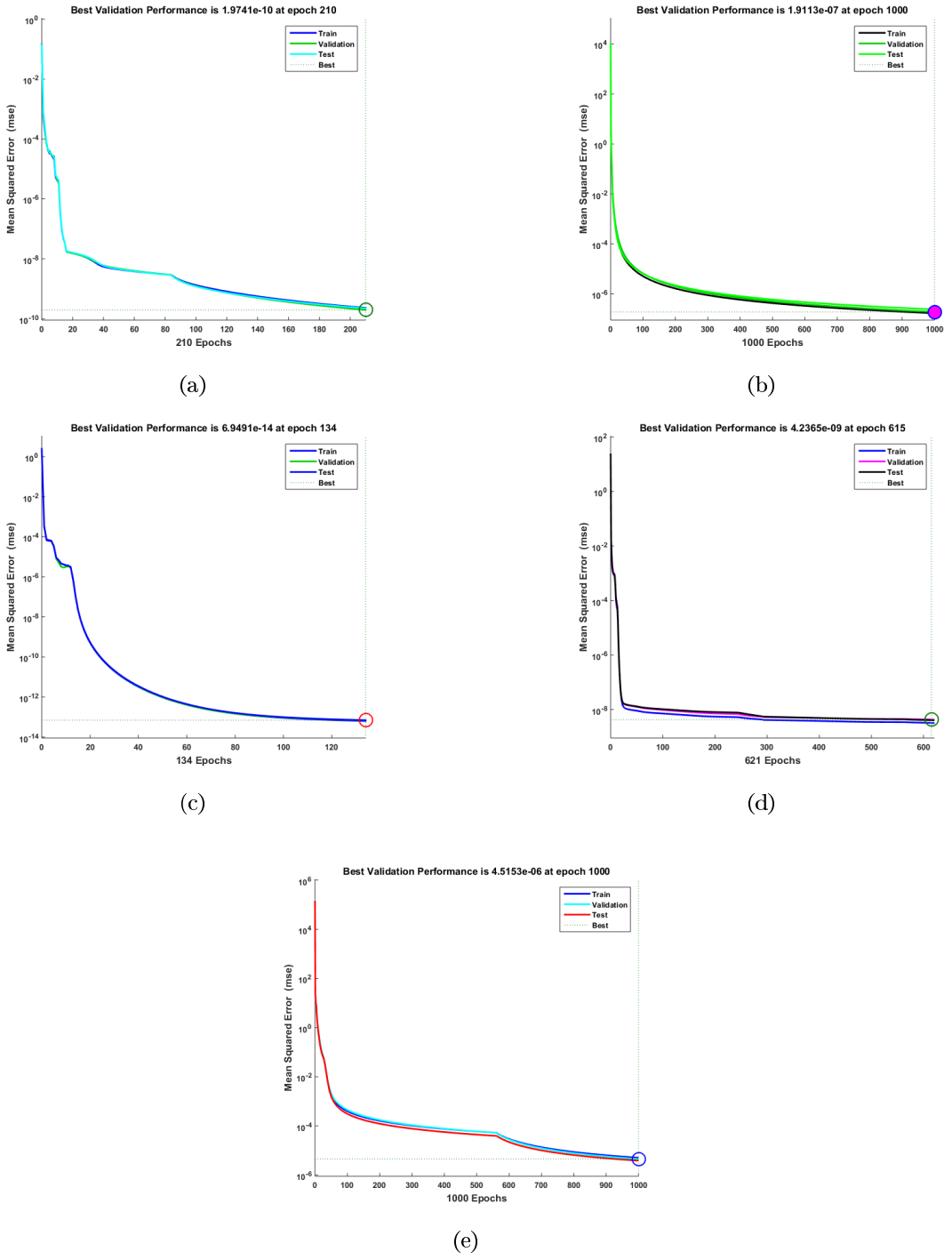


FIGURE 18. Analysis of performance function in terms of mean square error for the system of (ODE) of case 3.

network, as shown in Figure (5). Figure (3) demonstrates the architecture of the system that is connected to the domain controller.

IV. RESULTS

We tackle the mathematical problem by using the Feed-Forward Artificial Neural Network technique to find numerical solutions to the system of differential equations specified in equation (1). The solution is stored as a neural network on the base of the Levenberg–Marquardt algorithm (BLMA) [46]. Figure (5) depicts a neural network for the system of ODEs. For this compartmental mathematical model, we use one intermediate layer for each input and output as shown in Figure (5). To verify the resilience of the

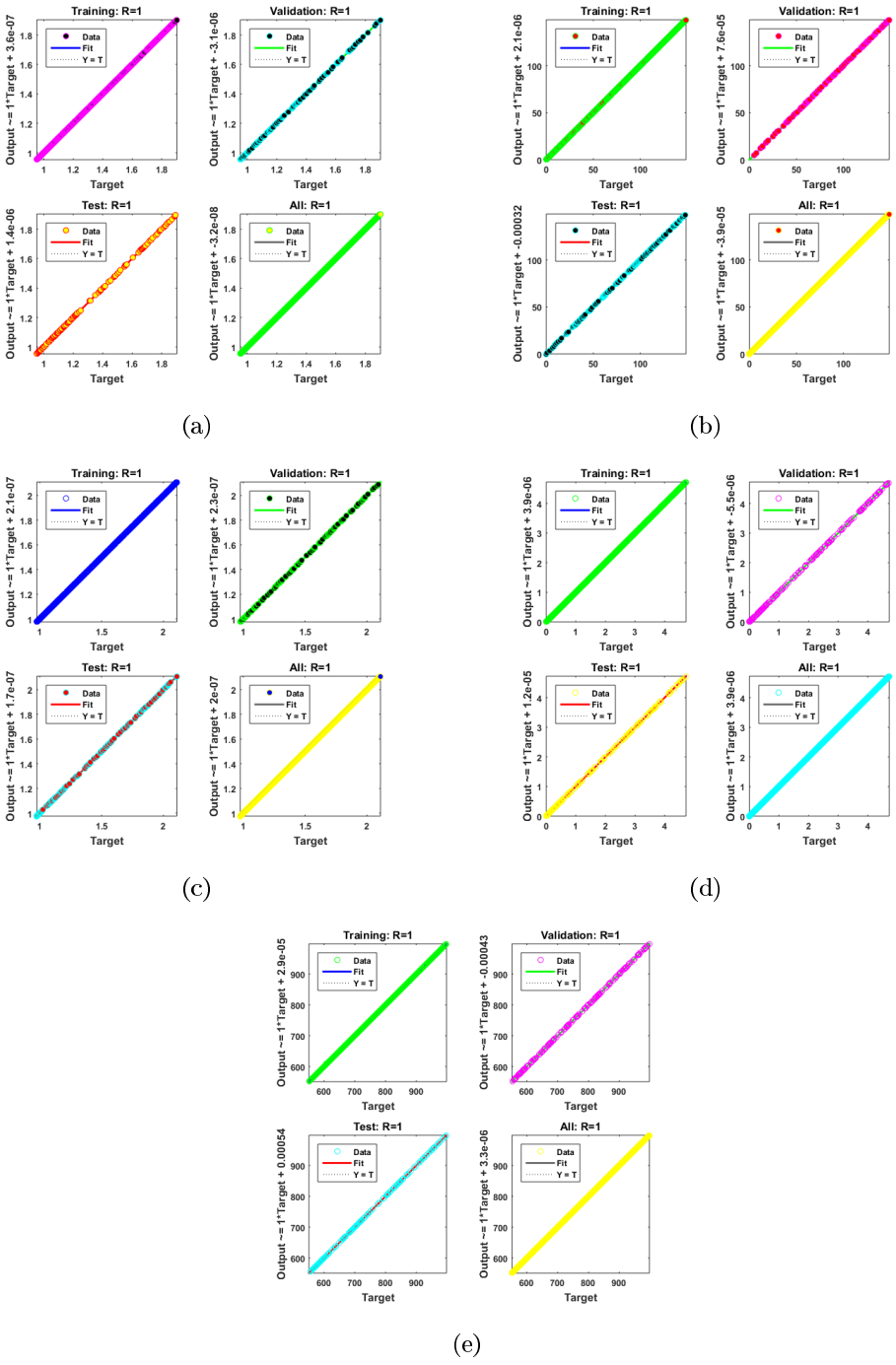


FIGURE 19. Regression analysis for the system of (ODE) of case 3.

ANN-Approach, the model was trained 34 times, as shown in Figure (17), 34 percent of the fitting results are reasonably excellent, with an average error of 1.23×10^{-07}. More data points should be retained to reduce error. From [27] ass in Solution techniques for initial and boundary value problems by using Levenberg–Marquardt algorithm (BLMA). It has been demonstrated how the ANN-approach may be used to solve a set of ordinary differential equations. Many researchers have proposed Artificial Neural networks, such as Lagares et al.in [27] as an approach to solving boundary and initial value problems. The design algorithm BLMA is used to investigate the affect variations of the damaging rate of connected devices as shown in Figure (2). According to the universal approximation theory [47], which uses a twins ANN to provide approximation solutions for the system ODE [48]. A single hidden layer feed-forward neural network should be

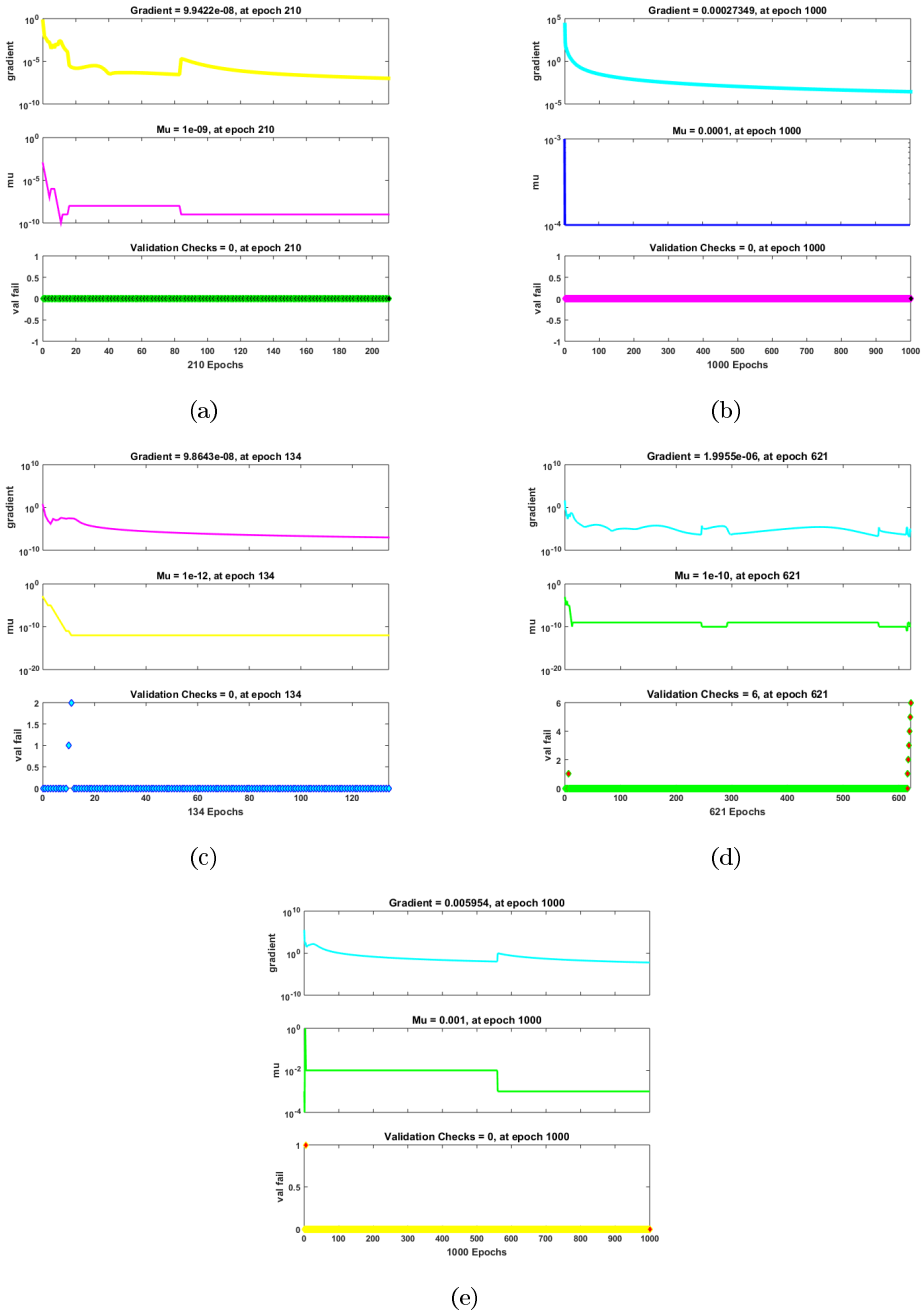


FIGURE 20. Training analysis for the system of (ODE) of case 3.

able to approximate any continuous function. To accomplish this, the system of ODE's should be written as follows:

$$\begin{cases} S'(t) = F_1(S(t), E(t), I(t), A(t), R(t), t), S(t_0) = S_0, \\ E'(t) = F_2(S(t), E(t), I(t), A(t), R(t), t), E(t_0) = E_0, \\ I'(t) = F_3(S(t), E(t), I(t), A(t), R(t), t), I(t_0) = I_0, \\ A'(t) = F_4(S(t), E(t), I(t), A(t), R(t), t), A(t_0) = A_0, \\ R'(t) = F_5(S(t), E(t), I(t), A(t), R(t), t), R(t_0) = R_0. \end{cases} \tag{5}$$

The solution of that differential equations can be expressed in term of

$$y'(t) = F(y(t), y(t)) = y_0. \tag{6}$$

In this solution, y'(t) symbolizes the left-hand side, F(y(t),(t)) indicates the right-hand side, and $y(t_0)=y_0$ represents the system's initial condition. We apply an ANN approach with 10 hidden layers to fit the function y(t), which may be represented in matrix multiplication form:

$$N(t, w) = W_{k2}\mathbf{u}(W_{k1} + b_1) + b_2, \tag{7}$$

TABLE 2. Machine learning techniques used in cyber security.

Paper	Methodology	ML Classifier Used	Problem Solved	Domain Selected
1 [58]	A distributed machine (SVM) employs a combination of machine learning, ontology, and fuzzy logic.	Support Vector Machine (SVM)	Intrusion Detection and Prevention (IDP)	Smart Grid ecosystem
2 [59]	Email components (header, body, and attachments) are utilized to extract general descriptive properties.	Random Forest (RF)	Detection of malicious email	Email
3 [60], [61]	Multi-Layer Perceptron (MLP) Artificial Neural Network (ANN) classifiers.	Multi-layer perceptron (MLP)	Detecting Denial of Service & Spoofing on Real Time Location Systems for autonomous robots.	Indoor real-time localization systems for autonomous robots mobile environment
4 [62]	Denial of Service detection and indoor real-time localization systems for autonomous robots Environment in Motion.	Rule-based classifier (DT, RIPPER)	Detection of Smashing Messages in Mobile Environment.	Mobile Environment
5 [63]	Using supervised ML, we are investigating the adversarial robustness of general security detection systems.	Ensemble algorithm	Studying adversarial resilience of cyber security detection system.	General
6 [64]	The Ngu-Incremental Learning Framework is based on the log history of mobile devices.	SVM, Logistic Regression, ANN	Mobile malware detection system.	Mobile
7 [65]	Principal Component Analysis (PCA) and ANN hybrid technique for identifying malicious traffic.	PCA and ANN	Malware traffic classification.	Malicious traffic classification
8 [66]	Malware detection using ensemble Ensemble classifiers based on the combination of static and dynamic features Malware identification.	Ensemble classifier	Malware Detection	Android Device
9 [67]	Automate cyber threat attribution (total of 36 threats) with various classifiers.	NB, KNN, Dtree, RF and deep learning NNs	Detection of 36 well-known threats.	General

where W is weights, t are the inputs and W_{k1} to W_{kn} are the weight matrices and b_1,b_2 are bias term,**u** is the linear activation function Sigmoid and Tanh are two examples [49]. All the parameters are represented by W [W_{k1},b_1,W_{k2},b_2]. The given solution is also rewrite as;

$$y(t, w) = y_0 + t - t_0 N(t, w), \tag{8}$$

where

$$N(t_0, w) \neq y_0, \tag{9}$$

such that the solution function y(t_0,w)=y_0 and it's derivation is y'(t_0,w)=y_0 By minimizing the loss function [49], such as Sigmoid or tanh, among others, the ideal parameter (w) can be obtained.

The FNN-BLM algorithm's results are compared with the Runge-Kutta technique, the least square method [50], and a machine learning algorithm (FNN-BLM) [51] to illustrate the correctness and efficiency of the design algorithm, as stated in Tables 3 and 4. The statistics show that the FNN-BLM technique is legitimate, and the solutions overlap with the numerical results with minimal absolute errors in the range of 10^{-5} to 10^{-8}.

V. DISCUSSION

The study is carried out by detecting cybercrime in Jordanian adopting COVID-19 problems and timeline mapping of significant events and cyber attacks to assess targeted sectors and their cyber security [52]. This article discusses cybercrime and its issues in Jordan's criminal justice system, Jordanian legislation dealing with cybercrime and computer-enabled offenses and as well as other crimes committed using electronic devices, [53], [54]. The impact of cybercrime

TABLE 3. Comparing machine-learning-derived solutions with RK-4 for Susceptible devices for case 1.

Input	Output	Target	absolute Error
0	1	1	4.74E-07
0.5	0.943225	0.943225	2.10E-07
1	0.889832	0.889832	2.10E-07
1.5	0.839618	0.839618	1.19E-07
2	0.792389	0.792389	2.55E-08
2.5	0.747966	0.747966	2.22E-08
3	0.706179	0.706179	6.90E-11
3.5	0.666868	0.666868	1.55E-07
4	0.629883	0.629883	2.50E-07
4.5	0.595084	0.595084	2.14E-07
5	0.562339	0.562339	4.07E-07

TABLE 4. Comparing machine-learning-derived solutions with RK-4 for Exposed devices for case 1.

Input	Output	Target	Absolute Error
0	0	1.20E-05	1.20E-05
0.5	0.076004	0.076007	3.93E-06
1	0.146066	0.14607	4.01E-06
1.5	0.210537	0.210539	2.03E-06
2	0.269749	0.269747	2.28E-06
2.5	0.324017	0.324015	1.66E-06
3	0.373638	0.373641	3.31E-06
3.5	0.418894	0.418893	1.27E-06
4	0.460053	0.460049	3.44E-06
4.5	0.497365	0.497362	3.31E-06
5	0.531071	0.53106	1.12E-05

TABLE 5. Comparing machine-learning-derived solutions with RK-4 for Infected devices for case 1.

Input	Output	Target	Absolute Error
0	0	1.08182E-06	1.08182E-06
0.5	-0.000362	-0.00036241	8.01E-07
1	-0.001222	-0.00122286	4.74516E-07
1.5	-0.002562	-0.00256125	6.25E-07
2	-0.004361	-0.00436063	5.39E-07
2.5	-0.006603	-0.006604	1.18155E-06
3	-0.009271	-0.00927278	1.98E-06
3.5	-0.01235	-0.0123508	4.0439E-07
4	-0.015828	-0.01582627	1.98E-06
4.5	-0.019692	-0.01968914	3.09369E-06
5	-0.023931	-0.0239279	3.49527E-06

TABLE 6. Comparing machine-learning derived solutions with RK-4 for Asymptomatic devices for case 1.

Input	Output	Target	Absolute Error
0	1	0.999988	1.21E-05
0.5	0.9379407	0.937937	4.06231E-06
1	0.879892	0.879888	3.9122E-06
1.5	0.8255924	0.825592	6.93321E-07
2	0.7747976	0.774801	3.6969E-06
2.5	0.7272789	0.727278	1.13302E-06
3	0.6828228	0.682819	3.28889E-06
3.5	0.6412293	0.64123	1.2188E-06
4	0.6023116	0.602315	3.58E-06
4.5	0.5658951	0.565899	3.5877E-06
5	0.5318165	0.531806	1.01044E-05

includes the theft of personal information from hundreds of millions of people. During the last year, events have touched more than 40 million individuals in the United States, 54 million in Turkey, 20 million in Korea, 16 million in Germany, and more than 20 million in China, to name a few [55]. According to the National Social Crime Records Bureau, 217 occurrences were registered under the IT Act in 2007, compared to 142 incidents the previous year (2006), signifying a 52.8 percent rise in 2007.The state of Maharashtra had the largest percentage of incidents (22.3%), followed by Karnataka (40), Kerala (38), and the states of Andhra Pradesh and Rajasthan (16 each). 99 of the 217 total incidents registered under the IT Act 2000 constituted obscene publishing or transmission in electronic form, sometimes known as cyber pornography. This accounts for 45.6 percent of all cases [56]. The Keller-Segel system [57], which models the group behaviour of chemotactic organisms with both attraction and repulsion terms, may be controlled using a mechanism that ensures stability. Its main focus is on finding control mechanisms that can stabilise the

TABLE 7. Comparing machine-learning derived solutions with RK-4 for Recovered device for case 1.

Input	Output	Target	Absolute Error
0	1	1	2.19E-07
0.5	0.952444	1.452444	2.22E-07
1	0.907898	1.907898	2.03E-07
1.5	0.866174	2.366174	1.62E-07
2	0.827094	2.827094	1.06E-07
2.5	0.790492	3.290492	3.09E-08
3	0.756209	3.756209	5.67E-08
3.5	0.724099	4.224099	1.51E-07
4	0.694023	4.694023	2.29E-07
4.5	0.665849	5.165849	2.80E-07
5	0.639454	5.639454	3.11E-07

TABLE 8. Comparing machine-learning-derived solutions with RK-4 for Susceptible devices for case 2.

Input	Output	Target	Absolute Error
0	0	0	1.93E-07
0.5	0.07534	0.57534	7.53E-02
1	0.146158	1.146158	1.46E-01
1.5	0.21266	1.71266	2.13E-01
2	0.275042	2.275042	2.75E-01
2.5	0.333493	2.833493	3.33E-01
3	0.388197	3.388197	3.88E-01
3.5	0.439325	3.939325	4.39E-01
4	0.487046	4.487046	4.87E-01
4.5	0.531519	5.031519	5.32E-01
5	0.572897	5.572897	5.73E-01

TABLE 9. Comparing machine-learning-derived solutions with RK-4 for Exposed devices for case 2.

Input	Output	Target	Absolute Error
0	1	1	4.54E-07
0.5	0.927992	0.927993	2.70E-07
1	0.861194	0.861194	2.35E-07
1.5	0.799228	0.799228	7.66E-08
2	0.741745	0.741745	1.40E-08
2.5	0.688421	0.688421	2.02E-09
3	0.638956	0.638956	2.92E-08
3.5	0.593069	0.593069	2.62E-08
4	0.550503	0.550503	8.75E-08
4.5	0.511016	0.511016	8.22E-08
5	0.474388	0.474387	3.06E-07

TABLE 10. Comparing machine-learning-derived solutions with RK-4 for Infected devices for case 2.

Input	Output	Target	Absolute Error
0	0	0	1.94E-06
0.5	0.018963	0.518963	8.95E-07
1	0.035933	1.035933	9.08E-07
1.5	0.051078	1.551078	5.00E-07
2	0.06455	2.06455	7.22E-08
2.5	0.076489	2.576489	1.09E-07
3	0.087026	3.087026	1.14E-07
3.5	0.096282	3.596282	3.27E-07
4	0.104367	4.104367	5.20E-07
4.5	0.111382	4.611382	4.85E-07
5	0.117423	5.117423	1.49E-06

system globally which implies that the population densities of the organisms reach a stable state regardless of the initial circumstances. This project will construct an effective and precise mathematical model to understand the behavior of numerous possible threats outside of a device network.

The first stage is to generate a dataset of solutions to the system of differential equations using a numerical approach, such as the Runge-Kutta method of order 4 (RK-4). The RK-4 method is used in the system of differential equations at this stage to provide a collection of discrete solutions, which are commonly represented as a time series of numbers. After creating the dataset, the next step is to use it to train an ANN. The results of RK-4 are then utilized as "target" data to train the ANN. The significance of training an ANN is to make predictions on previously unseen input data the training process begins with input data being presented to the network, and the network makes a prediction based on its current weights and biases. The predicted output is then compared to the target output, and the difference between the two is calculated as the error. The backpropagation algorithm is used to propagate the error back through the network by

TABLE 11. Comparing machine-learning derived solutions with RK-4 for Asymptomatic device for case 2.

Input	Output	Target	Absolute Error
0	997.9977	998	2.35E-03
0.5	973.2879	973.2886	6.41E-04
1	949.1893	949.1893	6.85E-05
1.5	925.6875	925.6871	3.89E-04
2	902.7665	902.767	5.86E-04
2.5	880.4152	880.4148	4.81E-04
3	858.616	858.6162	1.73E-04
3.5	837.3569	837.3575	5.78E-04
4	816.6249	816.6255	5.79E-04
4.5	796.4072	796.4069	2.58E-04
5	776.6915	776.6892	2.28E-03

TABLE 12. Comparing machine-learning derived solutions with RK-4 for Recovered device for case 2.

Input	Output	Target	Absolute Error
0	1	1	3.74E-07
0.5	0.956508	0.956508	2.55E-07
1	0.959358	0.959358	1.89E-07
1.5	1.000992	1.000992	2.17E-07
2	1.074703	1.074703	3.63E-07
2.5	1.174548	1.174548	7.84E-09
3	1.29528	1.29528	3.99E-07
3.5	1.43228	1.432279	1.89E-07
4	1.581494	1.581494	9.33E-09
4.5	1.739381	1.739381	2.49E-07
5	1.902855	1.902855	3.81E-07

TABLE 13. Comparing machine-learning-derived solutions with RK-4 for Susceptible devices for case 3.

Input	Output	Target	Absolute Error
0	-0.002914	0	2.91E-03
0.5	23.70345	23.7028	6.44E-04
1	45.00934	45.00918	1.56E-04
1.5	64.1015	64.10207	5.75E-04
2	81.15163	81.15195	3.16E-04
2.5	96.31803	96.31761	4.25E-04
3	109.7465	109.7469	3.68E-04
3.5	121.5775	121.5774	1.85E-04
4	131.9374	131.9371	3.44E-04
4.5	140.9449	140.9452	2.55E-04
5	148.7098	148.7124	2.67E-03

TABLE 14. Comparing machine-learning-derived solutions with RK-4 for Exposed devices for case 3.

Input	Output	Target	Absolute Error
0	0.999999	1	1.07E-06
0.5	0.975511	0.975512	2.07E-07
1	0.996069	0.996069	8.73E-08
1.5	1.055006	1.055006	2.29E-07
2	1.146323	1.146323	3.39E-07
2.5	1.26463	1.26463	9.47E-08
3	1.405097	1.405096	3.55E-07
3.5	1.563402	1.563401	2.43E-07
4	1.735694	1.735694	9.71E-09
4.5	1.918548	1.918549	2.46E-07
5	2.108927	2.108928	6.39E-07

propagating the error and adjusting the weights and biases to reduce it. This process is repeated for multiple iterations, with each iteration being called an epoch. The goal is to minimize the error between the predicted output and the targeted output for a given input by adjusting the weights and bias until the error is minimized to an acceptable level. Applying the testing, validation, and training of the reference data set yields the value of the approximate solution using BLMA. Convergence analysis, error histograms, regression analysis, and curve fitting were used for each data set to examine the robustness and accuracy of the design strategy.

Matlab software is used to construct the Figure of the numerical solution. The Backpropagation Levenberg-Marquardt method was used to train the network (BLMA). A clear framework and easy-to-use interface make BLMA techniques ideal for handling and analyzing linear scenarios. To compare the BLMA method with other machine learning methods it's a substantially faster rate of convergence than others. An BLMA method is a gradient-free approach. We used 70% (701 samples) of training data, 15% (150

TABLE 15. Comparing machine-learning-derived solutions with RK-4 for Infected devices for case 3.

Input	Output	Target	Absolute Error
0	-0.000819	0	8.19E-04
0.5	0.072705	0.072709	4.23E-06
1	0.27539	0.275434	4.38E-05
1.5	0.59005	0.590089	3.81E-05
2	1.000223	1.000253	3.06E-05
2.5	1.49101	1.491046	3.57E-05
3	2.04901	2.049007	3.05E-06
3.5	2.66201	2.661983	2.71E-05
4	3.319	3.319027	2.69E-05
4.5	4.010288	4.010297	9.41E-06
5	4.726885	4.726968	8.34E-05

TABLE 16. Comparing machine-learning derived solutions with RK-4 for Recovered device for case 3.

Input	Output	Target	Absolute Error
0	997.9722	998	2.78E-02
0.5	940.4433	940.4501	6.83E-03
1	886.2138	886.2207	6.90E-03
1.5	835.1255	835.1203	5.22E-03
2	786.9632	786.9685	5.27E-03
2.5	741.5966	741.5951	1.51E-03
3	698.8451	698.84	5.05E-03
3.5	658.5474	658.5522	4.79E-03
4	620.5917	620.5893	2.34E-03
4.5	584.8257	584.8173	8.42E-03
5	551.1275	551.1098	1.77E-02

samples) of validation data, 15% (150 samples) of testing data, and 10 hidden neurons in the fitting network's hidden layer for each input as shown in Figure (17). In figures, the histogram Figure compares the output data with the target and computes the error. A histogram analysis can help to understand the frequency and distribution of cyber assaults over time as shown in Figure 16. The histogram can depict the number of assaults per time interval as well as the distribution of attack attributes such as duration, kind, and intensity. The importance of histogram analysis for Cyber security experts can acquire insights into the patterns of cyber assaults and identify places where extra security measures may be required by analyzing the histogram. And the root of that error divided by the total sample points is known as the mean square error as shown in Figure (16). And fitting of the Figure shows the accuracy. Figure (17) illustrates what happens when the points in this plot are converging toward zero and are extremely close to zero: this indicates that the result is more accurate. Demonstrating that the points are convergent to one (R=1) and that the best validation performance is 8.1687×10^{-12} at epoch 106 is given in Figure (19). The training Figure (20) represents the behavior of the gradient. The gradient in the optimization method is for network performance concerning network weights. The regression Figure compares the target data with RK-4 to determine the error, as illustrated in Figure (10). We choose random setups for case 1. Furthermore use the same process to arrive at the surrogate solution. And using Matlab to plot the curve solution. In the second case the birth rate, recovery rate, infected recovered stage, the rate at which the device crashes (Natural death), and the rate at which devices leave respectively are variate. And keep constant the infection rate, devices leave Unprotected either to the infected, contact rate, and the rate of damaging devices due to attack as shown in table (17). In the third case the birth rate, recovery rate, infected recovered stage, the rate at which the device crashes (Natural death), and the rate at which devices leave respectively are kept constant. And attribute other variables such as: infection rate, devices leave exposed either to the infected, contact rate, and the rate of damaging devices due to attack as shown in Figure (4). The Figure histogram calculates the error by comparing the output data to the target. As illustrated in Figure (6), the mean square error is defined as the root of the error divided by the total number of sample points. And the fitting of the Figure demonstrates accuracy. Figure (6) can help to understand the frequency and distribution of cyber assaults over time. The histogram can depict the number of assaults per time interval as well as the distribution of attack attributes such as duration, kind, and intensity. Cyber security experts can acquire insights into the patterns of cyber assaults and identify places where extra security measures may be required by analyzing the histogram. Figure (7) depicts what happens when the points on this plot converge toward zero or are extremely near zero, indicating that the result is more accurate. Figure (8) indicates that the points are converging to one (R=1) (10) and that the best validation performance at epoch 77 is 8.1687×10^{12}. The training Figure (9) depicts the gradient's behavior. The gradient of the optimizing approach is for network performance in terms of network weights. Moreover, we aim to ascertain curves to the target solutions, intending to achieve a regression value of 1 for all the predicted solutions as shown in Figure (10). The same analysis histograms (11), fitting (12), performance analysis (13), regression analysis (14) and training analysis (15) are revised for the second and third scenario.

TABLE 17. Nomenclature.

Symbols	Explanations
S(t)	The number of computers that might be attacked at time t.
E(t)	Total number of Exposed computer at time t
I(t)	Total number of devices Infected at the time
A(t)	Total number of Asymptomatic devices at time t
R(t)	Total number of Recovered/Removed computer at time t
Ac	The number of additional devices that are added to the system. It is referred to as the birth rate.
μ	The rate at which a device crushes as a result of the number of times it has been used. It is known as a natural death.
λ	Infection rate of an Asymptomatic device.
ξ	The rate at which a device is harmed as a response of an assault that occurs during the Asymptomatic ξ_1 or Infected stage ξ_2.
β	Contact rate.
p_1 and p_2	The percentages at which devices transition from of the exposed compartment to the infected or recovered stages, respectively.
α	Devices are removed from exposed compartments at a rate that corresponds to the Infected, Recovered, or Asymptomatic stages, with proportions of , p_1, p_2 and (1-p_1+p_2) respectively.
δ ψ	Rates at which a device departs an Asymptomatic or Infected compartment and enters a compartment that has recovered.
η	Devices return to the susceptible compartment at a certain recovery rate after losing their temporary immunity.

VI. 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-of-the-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.

VII. CONFLICTS OF INTEREST

The author declare no conflicts of interest.

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 multi-agent 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.

[8] D. P. Möller, "Cyberattacker profiles, cyberattack models and scenarios, and cybersecurity ontology," in *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*. Berlin, Germany: Springer, 2023, pp. 181–229.

[9] Z. Lv, D. Chen, R. Lou, and H. Song, "Industrial security solution for virtual reality," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6273–6281, Apr. 2021.

[10] A. K. Dangi, K. Pant, J. Alanya-Beltran, N. Chakraborty, S. V. Akram, and K. Balakrishna, "A review of use of artificial intelligence on cyber security and the fifth-generation cyber-attacks and its analysis," in *Proc. Int. Conf. Artif. Intell. Smart Commun. (AISC)*, Jan. 2023, pp. 553–557.

[11] Y. Chen, L. Zhu, Z. Hu, S. Chen, and X. Zheng, "Risk propagation in multilayer heterogeneous network of coupled system of large engineering project," *J. Manag. Eng.*, vol. 38, no. 3, May 2022, Art. no. 04022003.

[12] H. Jiang, Z. Xiao, Z. Li, J. Xu, F. Zeng, and D. Wang, "An energy-efficient framework for Internet of Things underlaying heterogeneous small cell networks," *IEEE Trans. Mobile Comput.*, vol. 21, no. 1, pp. 31–43, Jan. 2022.

[13] B. Cheng, D. Zhu, S. Zhao, and J. Chen, "Situation-aware IoT service coordination using the event-driven SOA paradigm," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 2, pp. 349–361, Jun. 2016.

[14] P. Chen, H. Liu, R. Xin, T. Carval, J. Zhao, Y. Xia, and Z. Zhao, "Effectively detecting operational anomalies in large-scale IoT data infrastructures by using a GAN-based predictive model," *Comput. J.*, vol. 65, no. 11, pp. 2909–2925, Nov. 2022.

[15] B. Li, X. Zhou, Z. Ning, X. Guan, and K.-F.-C. Yiu, "Dynamic event-triggered security control for networked control systems with cyber-attacks: A model predictive control approach," *Inf. Sci.*, vol. 612, pp. 384–398, Oct. 2022.

[16] H. Saini, Y. S. Rao, and T. C. Panda, "Cyber-crimes and their impacts: A review," *Int. J. Eng. Res. Appl.*, vol. 2, no. 2, pp. 202–209, 2012.

[17] T. Li, T. Xia, H. Wang, Z. Tu, S. Tarkoma, Z. Han, and P. Hui, "Smartphone app usage analysis: Datasets, methods, and applications," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 937–966, 2nd Quart., 2022.

[18] T. Li, Y. Li, M. A. Hoque, T. Xia, S. Tarkoma, and P. Hui, "To what extent we repeat ourselves? Discovering daily activity patterns across mobile app usage," *IEEE Trans. Mobile Comput.*, vol. 21, no. 4, pp. 1492–1507, Apr. 2022.

[19] F. Meng, X. Xiao, and J. Wang, "Rating the crisis of online public opinion using a multi-level index system," 2022, *arXiv:2207.14740*.

[20] H. Liu, H. Yuan, J. Hou, R. Hamzaoui, and W. Gao, "PUFA-GAN: A frequency-aware generative adversarial network for 3D point cloud upsampling," *IEEE Trans. Image Process.*, vol. 31, pp. 7389–7402, 2022.

[21] S. Lu, Y. Ding, M. Liu, Z. Yin, L. Yin, and W. Zheng, "Multiscale feature extraction and fusion of image and text in VQA," *Int. J. Comput. Intell. Syst.*, vol. 16, no. 1, p. 54, Apr. 2023.

[22] D. K. Saini, "Cyber defense: Mathematical modeling and simulation," *Int. J. Appl. Phys. Math.*, vol. 2, no. 5, pp. 312–315, 2012.

[23] M. Martcheva, *An Introduction to Mathematical Epidemiology*, vol. 61. Berlin, Germany: Springer, 2015.

[24] J. Zhang, S. Peng, Y. Gao, Z. Zhang, and Q. Hong, "APMSA: Adversarial perturbation against model stealing attacks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1667–1679, 2023.

[25] K. Cao, B. Wang, H. Ding, L. Lv, R. Dong, T. Cheng, and F. Gong, "Improving physical layer security of uplink NOMA via energy harvesting jammers," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 786–799, 2021.

[26] H. Jin and Z. Wang, "Asymptotic dynamics of the one-dimensional attraction-repulsion Keller–Segel model," *Math. Methods Appl. Sci.*, vol. 38, no. 3, pp. 444–457, Feb. 2015.

[27] I. E. Lagaris, A. Likas, and D. I. Fotiadis, "Artificial neural networks for solving ordinary and partial differential equations," *IEEE Trans. Neural Netw.*, vol. 9, no. 5, pp. 987–1000, Sep. 1998.

[28] Z. Qu, X. Liu, and M. Zheng, "Temporal–spatial quantum graph convolutional neural network based on Schrödinger approach for traffic congestion prediction," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 8, pp. 8677–8686, Aug. 2023.

[29] Y. Deng, W. Zhang, W. Xu, Y. Shen, and W. Lam, "Nonfactoid question answering as query-focused summarization with graph-enhanced multihop inference," *IEEE Trans. Neural Netw. Learn. Syst.*, pp. 1–15, Mar. 2023.

[30] R. J. LeVeque, *Finite Difference Methods for Ordinary and Partial Differential Equations: Steady-State and Time-Dependent Problems*. Philadelphia, PA, USA: SIAM, 2007.

[31] P. Ramuhalli, L. Udpa, and S. S. Udpa, "Finite-element neural networks for solving differential equations," *IEEE Trans. Neural Netw.*, vol. 16, no. 6, pp. 1381–1392, Nov. 2005.

[32] H. Sug, "The effect of training set size for the performance of neural networks of classification," *WSEAS Trans. Comput.*, vol. 9, pp. 306–1297, Nov. 2010.

[33] Z. Lv, L. Qiao, J. Li, and H. Song, "Deep-Learning-Enabled security issues in the Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9531–9538, Jun. 2021.

[34] N. Kanwal, "Analysis of cybercrimes: A critical perspective," Dept. Comput. Sci., NCBA&E Lahore, Pakistan, Tech. Rep., Mar. 2023, vol. 1, no. 1.

[35] Z. Xiong, X. Li, X. Zhang, M. Deng, F. Xu, B. Zhou, and M. Zeng, "A comprehensive confirmation-based selfish node detection algorithm for socially aware networks," *J. Signal Process. Syst.*, pp. 1–19, Apr. 2023.

[36] X. Qin, Z. Liu, Y. Liu, S. Liu, B. Yang, L. Yin, M. Liu, and W. Zheng, "User OCEAN personality model construction method using a BP neural network," *Electronics*, vol. 11, no. 19, p. 3022, Sep. 2022.

[37] M. Malik and M. Dutta, "Feature engineering and machine learning framework for DDoS attack detection in the standardized Internet of Things," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8658–8669, May 2023.

[38] H. Jiang, M. Wang, P. Zhao, Z. Xiao, and S. Dustdar, "A utility-aware general framework with quantifiable privacy preservation for destination prediction in LBSs," *IEEE/ACM Trans. Netw.*, vol. 29, no. 5, pp. 2228–2241, Oct. 2021.

[39] H. Zhu, M. Xue, Y. Wang, G. Yuan, and X. Li, "Fast visual tracking with Siamese oriented region proposal network," *IEEE Signal Process. Lett.*, vol. 29, pp. 1437–1441, 2022.

[40] J. Lee and J. Jin, "Thickness and refractive index measurements of a thin-film using an artificial neural network algorithm," *Metrologia*, vol. 60, no. 2, 2023, Art. no. 025001.

[41] C. P. Robert, G. Casella, C. P. Robert, and G. Casella, "The metropolis—Hastings algorithm," in *Monte Carlo Statistical Methods*. Berlin, Germany: Springer, 1999, pp. 231–283.

[42] X. Xia, W. Xue, P. Wan, H. Zhang, X. Wang, and Z. Zhang, "FCGSM: Fast conjugate gradient sign method for adversarial attack on image classification," in *Innovative Computing Vol 2—Emerging Topics in Future Internet*. Berlin, Germany: Springer, 2023, pp. 709–716.

[43] W. Liu, Y. He, X. Wang, Z. Duan, W. Liang, and Y. Liu, "BFG: Privacy protection framework for Internet of Medical Things based on blockchain and federated learning," *Connection Sci.*, vol. 35, no. 1, Dec. 2023, Art. no. 2199951.

[44] M. Balaaditya and S. D. Dunston, "Analysis of the effect of adversarial training in defending EfficientNet-B0 model from DeepFool attack," in *Proc. 3rd Int. Conf. Intell. Commun. Comput. Techn. (ICCT)*, Jan. 2023, pp. 1–7.

[45] W. Lyu and Z.-A. Wang, "Logistic damping effect in chemotaxis models with density-suppressed motility," *Adv. Nonlinear Anal.*, vol. 12, no. 1, pp. 336–355, Sep. 2022.

[46] X. Xie, B. Xie, D. Xiong, M. Hou, J. Zuo, G. Wei, and J. Chevallier, "New theoretical ISM-K2 Bayesian network model for evaluating vaccination effectiveness," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 9, pp. 12789–12805, Sep. 2023.

[47] E. Negrini, "Universal approximation theorem, G. Cybenko," Worcester Polytech. Inst., Tech. Rep., Oct. 2019.

[48] Z. Lv, D. Chen, H. Feng, W. Wei, and H. Lv, "Artificial intelligence in underwater digital twins sensor networks," *ACM Trans. Sensor Netw.*, vol. 18, no. 3, pp. 1–27, Aug. 2022.

[49] S. Chakraverty and S. Mall, *Artificial Neural Networks for Engineers and Scientists: Solving Ordinary Differential Equations*. Boca Raton, FL, USA: CRC Press, 2017.
[50] A. Abazari, M. Zadsar, M. Ghafouri, and C. Assi, "Detection of cyber-physical attacks using optimal recursive least square in an islanded microgrid," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2022, pp. 1–5.
[51] A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," *Wiley Interdiscipl. Rev., Data Mining Knowl. Discovery*, vol. 9, no. 4, p. e1306, 2019.
[52] A. H. Amarullah, A. J. S. Runturambi, and B. Widiawan, "Analyzing cyber crimes during COVID-19 time in Indonesia," in *Proc. 3rd Int. Conf. Comput. Commun. Internet (ICCCI)*, Jun. 2021, pp. 78–83.
[53] R. S. Faqir, "Cyber crimes in Jordan: A legal assessment on the effectiveness of information system crimes law no (30) of 2010," *Int. J. Cyber Criminolog*, vol. 7, no. 1, pp. 1–10, 2013.
[54] P. Datta, S. N. Panda, S. Tanwar, and R. K. Kaushal, "A technical review report on cyber crimes in India," in *Proc. Int. Conf. Emerg. Smart Comput. Informat. (ESCI)*, Mar. 2020, pp. 269–275.
[55] E. F. G. Ajayi, "Challenges to enforcement of cyber-crimes laws and policy," *J. Internet Inf. Syst.*, vol. 6, no. 1, pp. 1–12, Aug. 2016.
[56] R. Montasari, "Cyber threats and the security risks they pose to national security: An assessment of cybersecurity policy in the United Kingdom," *Countering Cyberterrorism*. 2023, pp. 7–25.
[57] H.-Y. Jin and Z.-A. Wang, "Global stabilization of the full attraction-repulsion Keller–Segel system," 2019, *arXiv:1905.05990*.
[58] K. K. Jean-Claude, "Understanding the worldwide paths towards the creation of true intelligence for machines," Faculty Comput. Sci. Distance Learn., Bircham Int. Univ., Madrid, Spain, Tech. Rep., Feb. 2023, vol. 15, no. 1.
[59] A. Cohen, N. Nissim, and Y. Elovici, "Novel set of general descriptive features for enhanced detection of malicious emails using machine learning methods," *Exp. Syst. Appl.*, vol. 110, pp. 143–169, Nov. 2018.
[60] J. Naskath, G. Sivakamasundari, and A. A. S. Begum, "A study on different deep learning algorithms used in deep neural nets: MLP SOM and DBN," *Wireless Pers. Commun.*, vol. 128, no. 4, pp. 2913–2936, Feb. 2023.
[61] J. Yu, L. Lu, Y. Chen, Y. Zhu, and L. Kong, "An indirect eavesdropping attack of keystrokes on touch screen through acoustic sensing," *IEEE Trans. Mobile Comput.*, vol. 20, no. 2, pp. 337–351, Feb. 2021.
[62] S. Hemavathi and B. Latha, "FRHO: Fuzzy rule-based hybrid optimization for optimal cluster head selection and enhancing quality of service in wireless sensor network," *J. Supercomput.*, vol. 79, no. 11, pp. 12238–12265, Jul. 2023.
[63] V. Pantelakis, "Adversarial machine learning attacks against network intrusion detection systems," M.S. thesis, School Inf. Technol. Commun., Dept. Digit. Syst., 2023.
[64] N. Y.-R. Douha, M. Bhuyan, S. Kashihara, D. Fall, Y. Taenaka, and Y. Kadobayashi, "A survey on blockchain, SDN and NFV for the smart-home security," *Internet Things*, vol. 20, Nov. 2022, Art. no. 100588.
[65] D. Arivudainambi, K. A. V. Kumar, and P. Visu, "Malware traffic classification using principal component analysis and artificial neural network for extreme surveillance," *Comput. Commun.*, vol. 147, pp. 50–57, Nov. 2019.
[66] I. B. Mijoya, S. Khurana, and N. Gupta, "Performance analysis of hard voting and soft voting techniques on Android malware detection," School Eng. Technol., Sharda Univ., Greater Noida, India, Tech. Rep., Mar. 2023, vol. 58, no. 1.
[67] R. Ali, A. Ali, F. Iqbal, A. M. Khattak, and S. Aleem, "A systematic review of artificial intelligence and machine learning techniques for cyber security," in *Big Data and Security*. Berlin, Germany: Springer, 2020, pp. 584–593.
[68] J. Ma and J. Hu, "Safe consensus control of cooperative-competitive multi-agent systems via differential privacy," *Kybernetika*, vol. 58, no. 3, pp. 426–439, Sep. 2022.
[69] C. Qin, Y. Jin, Z. Zhang, H. Yu, J. Tao, H. Sun, and C. Liu, "Anti-noise diesel engine misfire diagnosis using a multi-scale CNN-LSTM neural network with denoising module," *CAAI Trans. Intell. Technol.*, vol. 8, no. 3, pp. 963–986, Sep. 2023.