

ARTICLE

Nonlinear Fractional Computer Virus Propagation in Safety Critical Heterogeneous Networks Analysis with Surrogate Deep Neuroarchitecture

Kiran Asma and Muhammad Asif Zahoor Raja*

Graduate School of Engineering Science and Technology, National Yunlin University of Science and Technology, Douliu, Taiwan

*Corresponding Author: Muhammad Asif Zahoor Raja. Email: rajamaz@yuntech.edu.tw

Received: 20 April 2026; Accepted: 27 May 2026; Published: 27 July 2026

ABSTRACT: The accelerated digital transformation of critical infrastructure has yielded unprecedented system interconnectivity, enhancing operational efficiency, simultaneously expanding the epidemiological propagation surface in heterogeneous networks. A novel machine learning-driven neuroarchitecture is designed in the present study, leveraging multilayer autoregressive exogenous neural networks (ARXNNs) iteratively trained with the Levenberg Marquardt (LM) algorithm, i.e., ARXNNs-LM, to address the intricate temporal dynamics of nonlinear fractional epidemiological computer virus propagation in the networks. The proposed ARXNNs-LM methodology effectively models the dynamic state transitions between susceptible, infected, and recovered systems. The dataset is synthesized through the application of the Grünwald–Letnikov (GL) fractional finite difference to numerically solve the nonlinear fractional computer virus propagation (FCVP) model for sundry case studies, such as variation in the infection rate of susceptible computers, the recovery rate of infected computers, and the removal rate from the network, while maintaining the fixed external computers connection rate. The simulated information is arbitrarily divided into training, testing, and validation subsets, while the network optimization is achieved by minimization of mean squared error (MSE), with achieved error magnitude around 10^{-9} to 10^{-13} . The proposed ARXNNs-LM methodology is compared with referenced numerical solutions of the FCVP model in terms of MSE convergence, absolute deviation from actual values, error frequency histograms, cross and autocorrelation analysis, optimization control parameters analysis, and time series analysis, to highlight the accuracy, robustness, and resilience. The precision and stability of the designed technique are further validated through the analysis of variance (ANOVA) assessment across multiple optimization algorithms applied to the FCVP model.

KEYWORDS: Cyberattack; heterogeneous channels; autoregressive exogenous neural networks; Levenberg Marquardt; Grünwald–Letnikov; fractional computer virus propagation

1 Introduction

Computer viruses continue to pose a serious threat to both common users and large-scale critical networking systems in the contemporary digital environment. These malicious programs exhibit the potential to replicate themselves, spread by themselves, and cause significant security compromises, including failure of the systems and data losses. The escalating dependency on networked infrastructure like wireless communication networks, Internet of Things technology, and centralized computing also increases their impacts, so it is essential to adequately comprehend and mitigate such potential threats.

There are three distinct types of subroutines that exist in a computer virus. Computer viruses infect the system in a similar way to how a typical disease virus infects and spreads in the human body, and can

also become a source of infection to other human beings. Similarly, computer viruses propagate throughout the system networks and affect the systems by connecting to other system application programs. When a computer system boots up, malicious code can activate instantly and infect the hard drive and boot media. This is a very dangerous type of computer virus because it activates itself and functions even before the computer system is completely loaded. The most serious impact of computer viruses occurs when they take control of system applications without user knowledge, such as web browsers, etc., changing settings and causing abnormal behavior of the computer system [1,2].

A computer virus can damage, delete, or modify large amounts of data, crash the entire network system, corrupt the files, and steal user financial information, which may lead to severe cybersecurity vulnerabilities. There are different types of computer viruses, but their behavior generally is like a parasite when they infect a system by attaching themselves to the application programs and transmit into the system and then spread through the whole network. These malicious programs are developed as executable files; users unknowingly click on this type of file to open it, a computer virus runs in the background, initiates operations, and starts to spread and infect the system. Depending upon the severity of the computer virus, it may fully bring the system down. The different examples of various types of computer viruses are illustrated in Fig. 1 to better understand the diverse behavior of virus propagation in the networks [3,4].

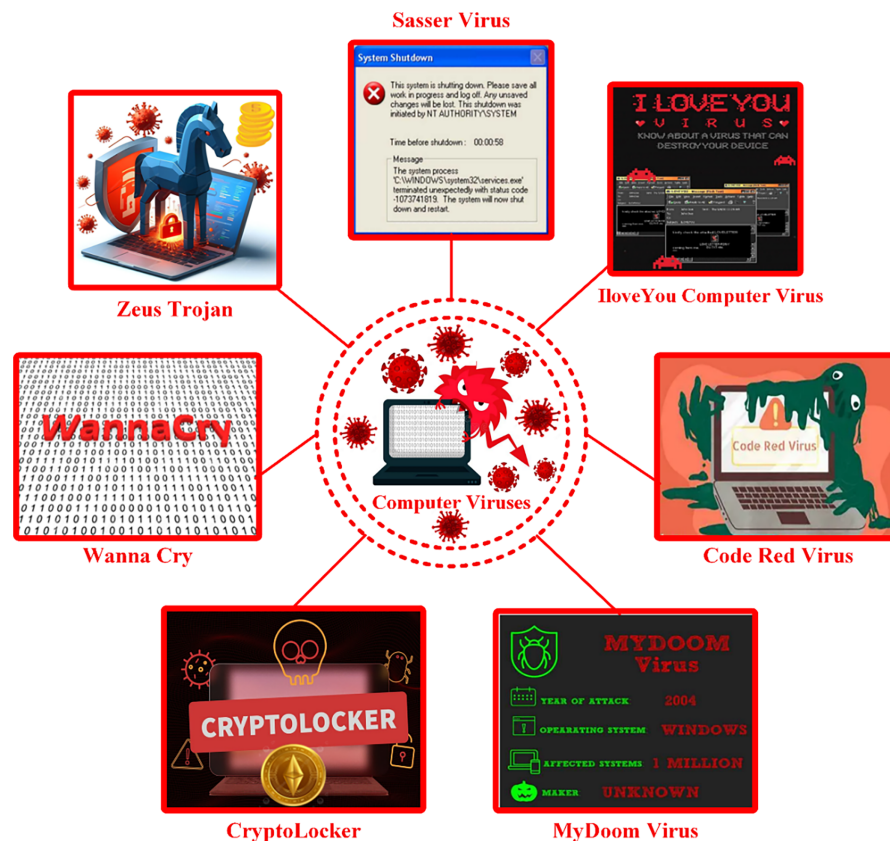


Figure 1: Taxonomical presentation of computer viruses with impact in diversified environments.

For instance, Zeus Trojan targeted banking credentials via phishing and botnet infrastructure; ILOVEYOU achieved large-scale dissemination through infected email attachments; CodeRed targeted Microsoft internet information services servers through buffer overflow exploits; Sasser exploited vulnerabilities in the window's local security authority subsystem services for autonomous propagation; MyDoom

leveraged rapid email-based propagation, installed persistent backdoors, and initiated large-scale distributed denial of service attacks; CryptoLocker executed high-impact file encryption to extort ransom payments; and WannaCry integrated ransomware payloads with worm-like spreading capabilities [5–8].

The first generation of cyber-epidemiological studies drew from biological disease models in the early 1990s, framing malware spread as an infection process within interconnected networked environments. Computers are divided into two compartments, susceptible and infected, with state transitions driven by exposure to compromised nodes and subsequent remediation activities [9,10]. Although foundational, this information lacked the granularity required to model computer virus latency, reinfection, dormant stages, and heterogeneous user responses, making biological models inadequate to the contemporary computer virus threat landscape. From a prevention and control perspective, computer viruses exhibit limitations comparable to biological infections, largely due to restricted system resources [11–13]. As shown in Fig. 2, a multistage computer virus propagation chain where an initial system compromise enables the computer virus to circulate between endpoints, web servers, and internal file servers that act as distribution hubs. The attacker further extends to peripheral devices via insecure interfaces, enabling lateral movement back into core infrastructure and amplifying overall virus propagation.

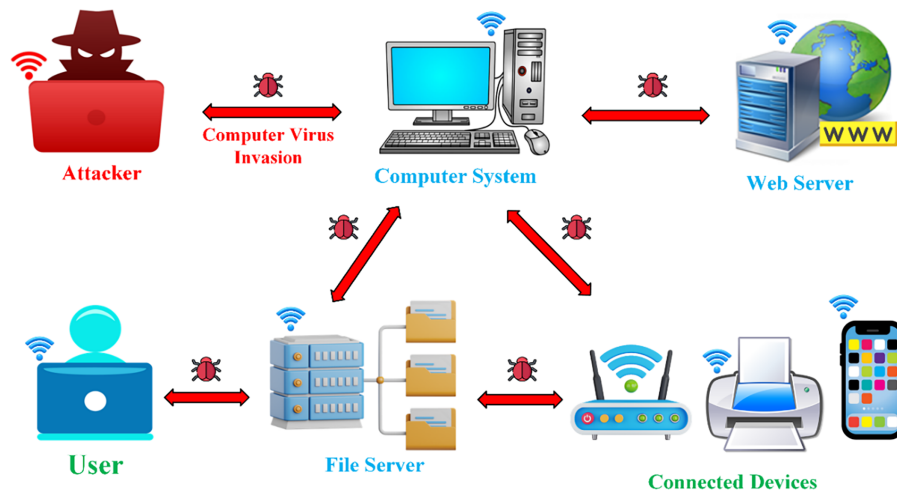


Figure 2: Multistage computer virus propagation mechanism exploiting endpoint, servers, and connected devices, forming feedback loops and enabling persistent, lateral virus spread in heterogeneous networks.

Several recent studies have focused on exploring diverse analytical models and mitigation strategies to deepen insight into computer virus propagation and enhance defense mechanisms within complex heterogeneous networks. The SLBRS model investigated virus transmission in complex networks via control strategies for susceptible, latent, breakout, and recovered states, highlighting the influence of network structure on computer virus dynamics [14]. The SEIQRS computer virus propagation model with impulse control and dual delays has been developed with susceptible, exposed, infected, quarantine, and recovered states, offering insight into delayed infection dynamics and periodic intervention strategies within network systems [15]. Bifurcation analysis in a time-delayed SIE computer virus model with susceptible, infected, and external state transitions has been conducted to investigate the effect of external computers entering the interconnected networks [16]. A SIQR model is implemented with susceptible, infected, quarantine, and recovered states by leveraging fuzzy fractional Atangana–Baleanu derivatives to analyze the malware propagation in wireless sensor networks [17].

The SEIRS model with susceptible, exposed, infected, recovered, and susceptible states investigated leveraging a generalized non-monotone-based technique, analyzing the dynamics of the self-propagating malware spread mechanism [18]. A classical epidemic SIR malware propagation model with transition of susceptible, infected, and recovered states has been developed to investigate the security protection mechanism and the probabilistic cellular automaton process using the Local transition functions endowed approach [19]. An expedition of deterministic numerical solvers is conducted for the computer virus spread by leveraging explicit Runge-Kutta and backward differential methods [20]. The SIHQR model with time delay is designed with state transformation of susceptible, infected, halted, quarantine, and recovered nodes for worm spread analysis in an industrial internet of things (IIoTs) enabled programmable logic controllers (PLCs) network [21]. A machine learning approach using nonlinear autoregressive exogenous neural networks is investigated with the Bayesian regularization method for epidemic malware propagation analysis in critical network infrastructures [22]. A VEIQS worm propagation model with vaccinated, exposed, infected, quarantine, and susceptible nodes with two delays has been analyzed for its Hopf bifurcation behavior, revealing conditions under which periodic oscillations and outbreak cycles emerged in mobile networks [23].

The queueing theory and HJ-biplot approach are used to investigate the SIRS system with susceptible, infected, and recovered system states to explore vulnerabilities and malware spread dynamics in wireless systems [24]. To study the influence of cybersecurity awareness, a machine intelligence-based neuroarchitecture has been designed to investigate the mobile malware propagation mechanism under the fractional dynamics of the cybersecurity awareness model [25]. The STSIR virus spread model with state transition of susceptible, traced, susceptible, infected, and recovered systems is investigated by implementing an individual-group game-based model in a social internet of things (SIoTs) environment [26]. The supervisory control and data acquisition (SCADA) systems are highly sensitive and vulnerable to cyber intrusions. In this context, an AI-based analysis has been conducted for the fractional dynamics of industrial virus spread with infusion of immunity [27]. A fractional-order SVEIR-KS model with susceptible, vaccinated, exposed, infected, and recovered systems is investigated for computer virus propagation and its stability and Hopf bifurcation analysis [28].

An immune knowledge-driven SCADA-based industrial virus propagation SELBR model is investigated with susceptible, enhanced susceptible, latent, breakout, and recovered nodes [29]. Research scholars have developed a graph neural network-based framework to investigate virus propagation mechanisms and intrusion detection in the networks [30]. Recently, a delayed malware propagation model with state transition of the SIP susceptible, infected, and protected machines by leveraging the Linear matrix inequalities method for the cloud computing security [31]. A stochastic games-assisted disclosure mechanism is introduced to explore malware propagation dynamics with state transformation of SIQR susceptible, infected, quarantine, and recovered nodes in industrial internet of things (IIoT) environments [32]. A Hybrid gradient-based global optimization framework is designed for the Internet malware propagation model with states of SEIRV susceptible, exposed, infected, recovered, and vaccinated compartments [33].

Artificial intelligence (AI) based methodologies have also emerged as powerful tools for modelling and analyzing the dynamics of epidemiological computer virus propagation (CVP) mechanism in heterogeneous networks. Conventional antivirus mechanisms and epidemiological CVP models, while informative, are inadequate for representing the intricate and nonlinear behaviors observed in real-world network architectures. Recent developments include AI-driven antivirus frameworks and cyber threat intelligence systems designed to reinforce cybersecurity infrastructures [34–36].

Multilayer autoregressive exogenous neural networks (ARXNNs) employed in this study represent a supervised stochastic approach for computational analysis (SSACA), where system dynamics are learned from labeled input-output data through iterative optimization-based training. The present methodology

leverages multilayer ARXNNs trained using the Levenberg Marquardt (LM) optimization algorithm, i.e., ARXNNs-LM framework, to capture the chronological behavior of the nonlinear fractional computer virus propagation (FCVP) system with state transitions of susceptible computers, infected computers, and recovered computers (SIR) in heterogeneous networks. Leveraging a multi-layer architecture coupled with exogenous input allows the model to emulate nonlinear dependencies across network entities, yielding a robust analytical foundation for both interpretability and predictive assessment of virus propagation. In heterogeneous networks, the infection spread is not dependent only on the current state but also on the past system behaviors, delayed malware detections, hidden infections, and residual vulnerabilities after the recovery process. The traditional integer order models only capture the instantaneous transition of the state without supporting the memory effect in the network environment. Therefore, fractional order models provide the hereditary behaviors by incorporating the influence of the past system state on the present system dynamics.

The cross paradigm comparative analysis between existing studies and the proposed ARXNNs-LM neuroarchitecture is tabulated in [Table 1](#).

Table 1: Existing studies comparison with the proposed neuroarchitecture.

Reference	Model	State Parameters	Technique	Fractional Order Modelling	Intelligent Computing
[3] Manohara and Kumbinarasaiah, 2024	SIR epidemiological model	S, I, R	Fibonacci wavelets	✗	✗
[14] Tang et al., 2024	SLBRS model	S, L, B, R, S	Control strategies	✗	✗
[15] Wang et al., 2025	SEIQRS model	S, E, I, Q, R, S	Impulse control with dual delays	✗	✗
[16] Zhang and Bi, 2015	SIE model	S, I, E	Bifurcation analysis with time-delay	✗	✗
[17] Dong et al., 2022	SIQR model	S, I, Q, R	Fuzzy fractional Atangana–Baleanu derivatives	✓	✗
[18] Liu et al., 2022	SEIRS e-epidemic model	S, E, I, R, S	Delay, non-monotone incidence	✗	✗
[19] del Rey et al., 2022	SIR epidemic model	S, I, R	Local transition functions endowed	✗	✗
[20] Asma et al., 2025	SIR epidemic model	S, I, R	Explicit Runge-Kutta method	✗	✗
[21] Wu et al., 2024	SIHQR with time delay (IIoT PLC)	S, I, H, Q, R	Disease-free equilibrium and Hopf bifurcation	✗	✗

(Continued)

Table 1 (continued)

Reference	Model	State Parameters	Technique	Fractional Order Modelling	Intelligent Computing
[22] Asma et al., 2025	SDIQTTPR epidemic nonlinear malware propagation model	S, D, I, Q, T, P, R	Neurocomputing	✗	✓
[23] Yang et al., 2021	VEIQS model (2 delays)	V, E, I, Q, S	Hopf Bifurcation	✗	✗
[24] Frutos-Bernal et al., 2024	SIRS with queuing theory	S, I, R, S	Queueing theory and HJ-Biplot	✗	✗
[26] Wu et al., 2023	STSIR in Social IoT	S, T, S, I, R	Individual-group Game model	✗	✗
[28] Yang et al., 2024	SVEIR-KS model	S, V, E, I, R, KS	Stability & Hopf Bifurcation	✓	✗
[29] He et al., 2024	SCADA-based industrial virus model	S, E, L, B, R	Immune Knowledge-Driven Control	✗	✗
[30] Ying et al., 2024	SIR model	S, I, R	Graph Neural Network	✗	✓
[31] Yu and Zhang, 2026	Time delayed malware propagation model	S, I, P	Linear matrix inequalities method	✗	✗
[32] Shen et al., 2026	Malware propagation model	S, I, Q, R	Stochastic games-assisted method	✗	✗
[33] Ghosh and Kumar, 2026	Internet malware propagation model	S, E, I, R, V	Hybrid gradient-based global optimization framework	✗	✗
Proposed Technique	FCVP model	S, I, R	ARXNNs-LM technique	✓	✓

The following are the insights of the presented ARXNNs-LM technique:

- The designed neuroarchitecture leverages a sophisticated hybrid machine learning model, nonlinear multilayer autoregressive exogenous neural networks (ARXNNs) trained with the Levenberg Marquardt (LM) optimization algorithm, providing an effective solution for simulating the nonlinear fractional epidemiological behavior of computer virus propagation. The ARXNNs-LM approach efficaciously

modeled the nonlinear fractional computer virus propagation (FCVP) system, capturing the temporal dynamical state transition of susceptible computers S , infected computers I , and recovered computers R (SIR) in the networks.

- The Grünwald–Letnikov (GL) inspired fractional finite difference method is employed to generate a synthetic dataset for the ARXNNs-LM neuroarchitecture, to address the temporal variations in the infection, recovery, and node removal rate while the external connection rate is held constant.
- The accuracy and robustness of the proposed ARXNNs-LM technique are quantified via mean square error (MSE) analysis, absolute error deviation (AE), cross and autocorrelation analysis, and error histograms analysis, using the numerical outcomes of the nonlinear FCVP model as a benchmark, demonstrating the stability and resilience of the employed framework.
- The precision of the presented hybrid ARXNNs-LM framework is further validated through the analysis of variance (ANOVA) assessment across multiple optimization algorithms applied to the FCVP system.
- The extensive numerical experiments demonstrated that the ARXNNs-LM methodology provides accurate, stable, and robust performance in capturing the fractional order chronological variations of computer virus propagation. The findings highlight the potential of this advanced machine learning-driven framework to deliver sophisticated cybersecurity tools, strengthening the prevention and control strategies against computer viruses in complex interconnected heterogeneous networks.

The rest of the study is structured as follows: [Section 2](#) details the nonlinear FCVP model, [Section 3](#) describes the ARXNNs-NN methodology and GL fractional finite difference computational procedure. [Section 4](#) provides the performance evaluation strategies, [Section 5](#) presents the results and discussion, and [Section 6](#) concludes the paper with final remarks and future research directions.

2 Preliminaries

A few renowned fractional operators are presented in this section. The fractional derivatives are reported here, including the Atangana–Baleanu (AB) fractional operator [37], Caputo–Fabrizio (CF) fractional operator [38], Grünwald–Letnikov (GL) fractional operator [39], Riemann–Liouville (RL) [40], Caputo fractional operator [41], and Hadamard [42]. All these definitions have their own significance, the presented studies remained focused on GL fractional operators.

The RL fractional derivative of order $q > 0$ for a function $y(\xi)$ is defined in terms of the integral operator I as follows [43]:

$$(D^q y)(\xi) = \left(\frac{d}{d\xi} \right)^n (I^{n-q} y)(\xi), \quad (n-1 < q \leq n) \quad (1)$$

here, D^q denotes q -th fractional derivative, while n denotes an integer. The integral I expressed as:

$$(I^q y)(\xi) = \frac{1}{\Gamma(q)} \int_0^\xi (\xi - \tau)^{q-1} y(\tau) d\tau. \quad (2)$$

The Caputo operator: For a function $y(\xi)$, the Caputo fractional derivative D^q of order $q > 0$ is formally introduced in [44] as:

$$(D^q y)(\xi) = I^{n-q} \frac{d^n}{d\xi^n} y(\xi) = \frac{1}{\Gamma(n-q)} \int_0^\xi (\xi - \tau)^{n-q-1} y^{(n)}(\tau) d\tau. \quad (n-1 < q \leq n) \quad (3)$$

The Hadamard fractional operator: The Hadamard fractional derivative can be defined as follows [45]:

$${}_a D_{\xi}^{-q} y(\xi) = \frac{1}{\Gamma(q)} \int_a^{\xi} \left(\log \frac{\xi}{\tau} \right)^{q-1} y(\tau) \frac{d\tau}{\tau}, \quad t > a \quad (4)$$

AB fractional operator: The AB fractional derivative is presented mathematically as follows [46]:

$${}_a^{ABC} D_{\xi}^q y(\xi) = \frac{AB(q)}{1-q} \int_a^{\xi} y'(\tau) E_q \left(-q \frac{(\xi - \tau)}{1-q} \right) d\tau. \quad (5)$$

CF fractional operator: The CF fractional derivative is mathematically presented as follows: [47].

$${}_a^{CF} D^q y(\xi) = \frac{1}{1-q} \int_a^{\xi} y'(\tau) e^{\left(-q \frac{\xi - \tau}{1-q} \right)} d\tau, \quad a < 0, q \in (0, 1) \quad (6)$$

GL fractional derivative: The GL fractional derivative is mathematically presented in finite differences as follows: [48]

$$D^q y(\xi) = \lim_{h \rightarrow 0} \frac{1}{h^q} \sum_{m=0}^{\infty} (-1)^m \frac{\Gamma(q+1)}{\Gamma(q-m+1) m!} y(\xi - mh). \quad (7)$$

The present study focuses on the generation of synthetic datasets for numerical simulations and training the proposed ARXNNs-LM neuroarchitecture to efficaciously capture the dynamics of the FCVP model. The GL fractional differentiation operator is well-suited for numerical implementation because of its ability to capture memory effects, discrete structure, and strong compatibility with fractional order time-series dynamic simulations. The GL differentiation operator provides a controlled numerical analysis of computer virus propagation dynamics and memory dependent cyber behaviors [49].

3 Methodology

The methodology implemented in this study for solving the nonlinear FCVP model is portrayed in terms of process flow structures in Fig. 3. The material and methodology presented in the research work mainly consist of three parts. In the first stage, the system model for the nonlinear FCVP model is represented mathematically, in the second stage, the synthetic data generation for the nonlinear FCVP model using numerical computing procedure of GL-operator for fractional finite differences is presented, while in the third stage, multilayer ARXNNs backpropagated efficiently with LM optimization are used to approximate the FCVP model solutions.

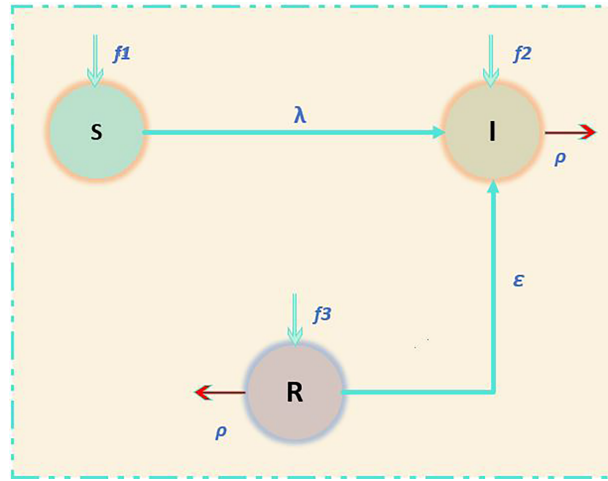


Figure 3: State transformation dynamics of the nonlinear CVP model.

3.1 The Nonlinear Fractional Computer Virus Propagation Model

Herein, the epidemiologically inspired design of the nonlinear fractional computer virus propagation (FCVP) is presented to incorporate the GL fractional differential operator in the standard integer order computer virus propagation (CVP) model. The nonlinear epidemiological mathematical model of computer virus propagation, as shown in Eqs. (8)–(10), represented three differential classes via susceptible computers that are vulnerable to infection S , computers currently infected and spreading virus I , and recovered or immunized computers R , i.e., (SIR) computer systems as follows [3]:

$$\frac{dS(\xi)}{d\xi} = f_1 - \lambda S(\xi) I(\xi) - \rho S(\xi), \quad S(0) = S_0 \quad (8)$$

$$\frac{dI(\xi)}{d\xi} = f_2 + \lambda S(\xi) I(\xi) - \varepsilon I(\xi) - \rho R(\xi), \quad I(0) = I_0 \quad (9)$$

$$\frac{dR(\xi)}{d\xi} = f_3 + \varepsilon I(\xi) - \rho R(\xi), \quad R(0) = R_0 \quad (10)$$

where the f_1 , f_2 , and f_3 stand for the external computers connecting rate to the network. f_1 denotes the rate of new susceptible computer systems joining the network, f_2 denotes the rate of external infected computer systems joining the network, f_3 denotes the rate external protected or recovered computer systems joining the network, λ denotes the infection rate associated with susceptible computers, ρ denotes the system removal rate from the networks, ε denotes the infected computers recovery rate, while S_0 , I_0 , and R_0 are fixed initial conditions for the CVP model. In the present study, heterogeneity refers to the variations in node functionality and operational roles within the interdependent networked environment, reflecting the realistic behavior of critical networks, where nodes differ in vulnerability, infection risk, recovery mechanism, and interactions during the computer virus propagation. This dynamic behavior reflects the functional heterogeneity among three different classes of the classical SIR -based compartmental model. For a complete exposition of the stability framework, convergence arguments, and parameter rationality, the reader may consult [3]. However, in the presented scheme, the ARXNNs-LM neuroarchitecture for capturing temporal dynamics of the nonlinear FCVP model is presented to provide deeper insights into the system's ultra-fast transient responses and its slow-scale evolutionary behavior by considering both integer ($\delta = 1$) and the fractional order δ values of D_{GL}^δ the GL operator. The fractional orders are arbitrarily chosen and showcased

in Table 1, uncovering a wide range of fractional orders to incorporate the memory effect of the fractional order to the conventional CVP model. Moreover, the fractional order serves as a knob and can be calibrated given we have reliable open-source real-world data, and it is established in literature that the heterogeneous environment within the computer networks infrastructure. The traditional integer order models only capture the instantaneous transition of the state without supporting the memory effect in the network environment. Therefore, fractional order models provide the hereditary behaviors by incorporating the influence of the past system state on the present system dynamics.

$$D_{GL}^{\delta} S(\xi) = f_1 - \lambda S(\xi) I(\xi) - \rho S(\xi), \quad S(0) = S_0 \quad (11)$$

$$D_{GL}^{\delta} I(\xi) = f_2 + \lambda S(\xi) I(\xi) - \varepsilon I(\xi) - \rho R(\xi), \quad I(0) = I_0 \quad (12)$$

$$D_{GL}^{\delta} R(\xi) = f_3 + \varepsilon I(\xi) - \rho R(\xi). \quad R(0) = R_0 \quad (13)$$

The FCVP model showcased in Eqs. (11)–(13) is solved for distinct scenarios and cases to mimic the real-world situations in the networked environment, as summarized in Table 2 with fixed and varying parametric values as per the pattern followed in the reported study [3]. Five cases of all three scenarios with six different fractional orders δ are constructed for the FCVP model using the values listed in Table 2 in Eqs. (11)–(13) with fractional order value $\delta = 0.99$, and the analytical expression associated with Scenario-1 (case-1) can be expressed as follows:

$$D_{GL}^{0.99} S(\xi) = 2 - 0.001 S(\xi) I(\xi) - 0.1 S(\xi), \quad S(0) = 20 \quad (14)$$

$$D_{GL}^{0.99} I(\xi) = 3 + 0.001 S(\xi) I(\xi) - 0.1 I(\xi) - 0.1 R(\xi), \quad I(0) = 15 \quad (15)$$

$$D_{GL}^{0.99} R(\xi) = 2 + 0.1 I(\xi) - 0.1 R(\xi). \quad R(0) = 10 \quad (16)$$

Table 2: Fixed and varying parameter values for FCVP model across distinct scenarios and cases.

Scenarios	Cases	Parameter of Interest		
		λ	ρ	ε
1	1	0.001	0.1	0.1
	2	0.003	0.1	0.1
	3	0.005	0.1	0.1
	4	0.007	0.1	0.1
	5	0.009	0.1	0.1
2	1	0.001	0.1	0.1
	2	0.001	0.2	0.1
	3	0.001	0.3	0.1
	4	0.001	0.4	0.1
	5	0.001	0.5	0.1
3	1	0.001	0.1	0.1
	2	0.001	0.1	0.2
	3	0.001	0.1	0.3
	4	0.001	0.1	0.4
	5	0.001	0.1	0.5

Note: Execute algorithm for integer and fractional order δ : $q_0 = 1, q_1 = 0.99, q_2 = 0.97, q_3 = 0.95, q_4 = 0.91, q_5 = 0.88$ and $q_6 = 0.85$. Fixed values of initial conditions: $S_0, I_0, R_0 = \{20, 15, 10\}$. Fixed values of external computer connection: $f_1, f_2, f_3 = \{2, 3, 2\}$.

Accordingly, the nonlinear FCVP system for scenarios (2–3) for case-1 can be expressed as follows:

$$D_{GL}^{0.97} S(\xi) = 2 - 0.001S(\xi)I(\xi) - 0.2S(\xi), \quad S(0) = 20 \quad (17)$$

$$D_{GL}^{0.97} I(\xi) = 3 + 0.001S(\xi)I(\xi) - 0.1I(\xi) - 0.2R(\xi), \quad I(0) = 15 \quad (18)$$

$$D_{GL}^{0.97} R(\xi) = 2 + 0.1I(\xi) - 0.2R(\xi), \quad R(0) = 10 \quad (19)$$

$$D_{GL}^{0.85} S(\xi) = 2 - 0.001S(\xi)I(\xi) - 0.2S(\xi), \quad S(0) = 20 \quad (20)$$

$$D_{GL}^{0.85} I(\xi) = 3 + 0.001S(\xi)I(\xi) - 0.3I(\xi) - 0.1R(\xi), \quad I(0) = 15 \quad (21)$$

$$D_{GL}^{0.85} R(\xi) = 2 + 0.4I(\xi) - 0.1R(\xi), \quad R(0) = 10 \quad (22)$$

Similarly, the analytical expressions associated with the remaining cases of the nonlinear FCVP model are constructed.

3.2 Grünwald–Letnikov Fractional Finite Differences Procedure for Synthetic Dataset Generation

The synthetic dataset utilized in this study is derived from numerical simulations of the nonlinear FCVP model (11–13) employing the standard finite difference formulations grounded in the GL fractional derivatives and a numerical scheme applicable to differential equations of arbitrary order is detailed in [50]:

The governing differential equation of fractional order $\delta = q$ can be written as:

$${}_a D_{\xi}^q x(\xi) = x(y(\xi), \xi), \quad (23)$$

$$y^{(i)}(0) = y_0^{(i)}, i = 0, 1, 2, \dots, n-1, \quad \text{for } n-1 < q < n. \quad (24)$$

The GL numerical solver's iterative scheme for Eq. (23), derived from Eq. (7), can be mathematically represented as [51]:

$$\frac{1}{h^q} \sum_{j=0}^{[(\xi-a)/h]} (-1)^j \frac{\Gamma(q+1)}{\Gamma(q-j+1)j!} y(\xi-jh) \approx x(y(\xi), \xi), \quad (25)$$

$$y(\xi) + \sum_{j=1}^{[(\xi-a)/h]} (-1)^j \frac{\Gamma(q+1)}{\Gamma(q-j+1)j!} y(\xi-jh) \approx h^q x(y(\xi), \xi), \quad (26)$$

for discrete inputs grid within the span $\xi \in [0, T] = [0, 2h, \dots, Mh = T]$, for h step size, then $[0, T] = [\xi_0 = 0, \xi_1, \dots, \xi_M = T]$ while the inputs $\xi_m = mh$ for $m = 0, 1, 2, \dots, M$.

Accordingly, Eq. (26) is represented in its discrete form as follows:

$$y(\xi_m) + \sum_{j=1}^m (-1)^j \frac{\Gamma(q+1)}{\Gamma(q-j+1)j!} y(\xi_m-jh) = h^{-q} x(y(\xi_m), \xi_m), \quad m = 0, 1, 2, \dots, M. \quad (27)$$

Equivalently for $c_0^q = 1$, $c_j^q = (-1)^j \frac{\Gamma(q+1)}{\Gamma(q-j+1)j!} = \left(1 - \frac{1+q}{j}\right)^j c_{j-1}^q$, $j = 1, 2, \dots$

The fractional order equation is solved using the GL approach formulated as follows:

$$y(\xi_m) + \sum_{j=1}^m c_j^q y(\xi_m-jh) = h^{-q} x(y(\xi_m), \xi_m), \quad m = 0, 1, 2, \dots, M, \quad (28)$$

$$y(\xi_m) = x(y(\xi_m), \xi_m) h^{-q} - \sum_{j=1}^m c_j^q y(\xi_m-jh), \quad m = 0, 1, 2, \dots, M. \quad (29)$$

The framework detailed in this section serves to formulate a synthetic dataset across all cases and scenarios, facilitating the mathematical modeling of the nonlinear FCVP system.

3.3 Intelligent Computing of Nonlinear ARXNNs-LM Neuroarchitecture

The stochastic numerical computing with AI methodologies has been widely implemented by research scholars for addressing different applications of paramount implication arising in applied science and engineering. All these illustrations motivated us to investigate ARXNNs-LM networks for solving the nonlinear FCVP model. In the proposed ARXNNs-LM scheme, using multilayer autoregressive exogenous neural networks, proficiently optimized through the LM algorithm, is articulated for solving the nonlinear FCVP system in Eqs. (11)–(13). The network structure ARXNNs consists of three (input-hidden-output) layers; the networks capture temporal dependencies by relating current observations to past values of targeted time series. The neurostructural visualization of the nonlinear ARXNNs-LM framework is demonstrated in Fig. 4 in terms of the input layer (single), hidden layers with 20 neurons and tansigmoidal activation function, and output layer with a matrix of 21 outputs. The ARXNNs framework is built on an autoregressive exogenous model where $y(t)$ represents the current output that is predicted using both previous output values and external input signals. In the present case, the autoregressive part considered 4 past output values from $y(t-1)$ to $y(t-4)$, enabling the model to capture the effect of past system states on the present. The exogenous input denoted by $x(t)$ represents the computer virus propagation dynamics related system input. To model the nonlinear relationships the system uses 20 tansigmoid neurons in a single hidden layer, which helps in learning complex temporal dynamics followed by linear output layer with 21 final predictions. To learn the memory-dependent system behavior, the network uses a feedback process based on delayed output recursion. The hidden layer uses tansigmoid activation function to address the nonlinear time-dependent dependencies, while the output layer uses a linear activation function to generate final predictions to improve the system's accuracy in predicting the computer virus propagation.

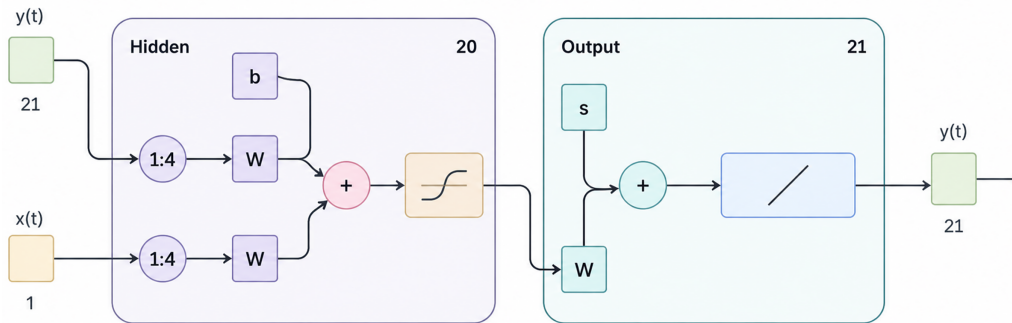


Figure 4: Neuro-structure of the nonlinear ARX networks.

The synthetic dataset of the fractional finite difference of the GL operator is the response outputs of nonlinear ARXNNs-LM to generate the solutions of the nonlinear FCVP model. The LM backpropagation algorithm is leveraged to iteratively tune the weights of the ARXNNs framework, enabling accurate solution of the FCVP system described in Eqs. (11)–(13). The neural networks optimization toolbox routines ‘narnet’, ‘ntstool’, and ‘train’ are employed for configuration and training of the ARXNNs-LM neuroarchitecture in the MATLABR2024b software package. The step-by-step architectural workflow of the employed ARXNNs-LM neuroarchitecture for solving the intricate temporal dynamics of the FCVP model is demonstrated in Fig. 5. The network structure ARXNNs consists of three (input-hidden-output) layers with the training regime specifically based on optimization scheme LM, loss function MSE, and terminal epochs criteria.

The networks capture temporal dependencies by relating current observations to past values of targeted time series.

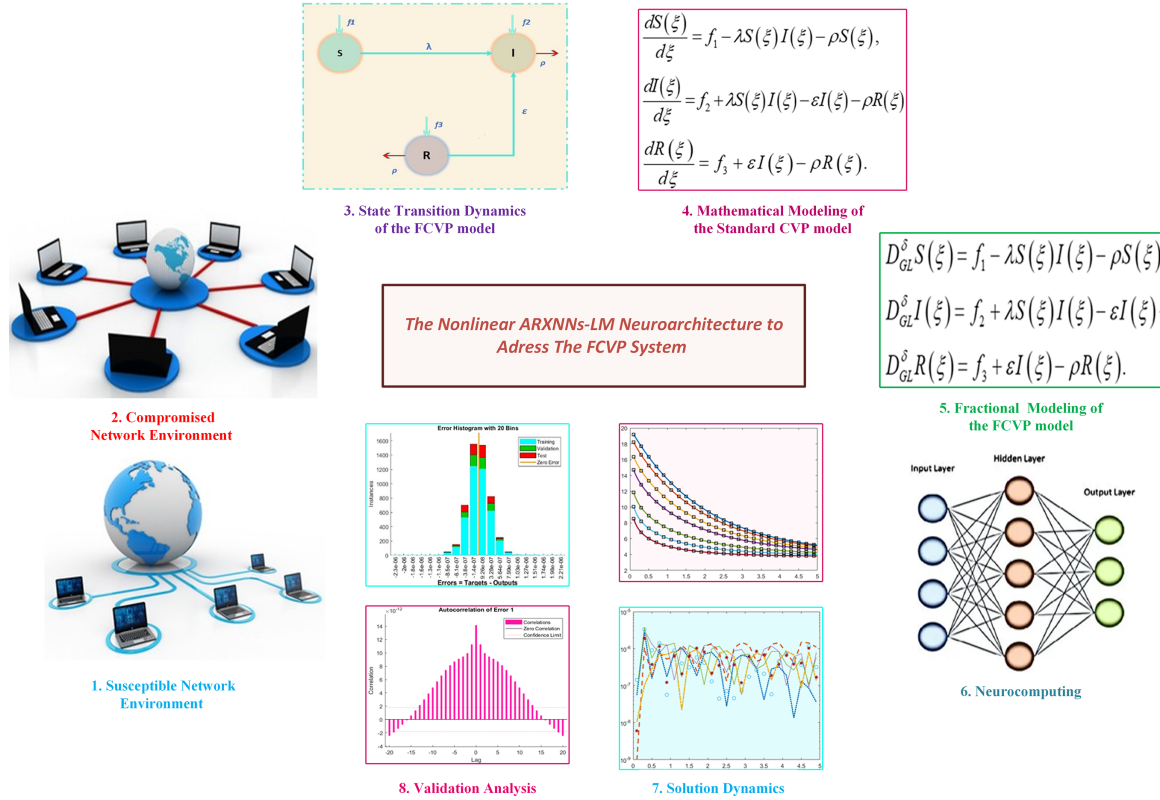


Figure 5: Workflow scheme of ARXNNs-LM algorithm for solving FCVP model.

4 Evolutional Scheme

The performance analysis for the outcomes of numerical experiments using the nonlinear ARXNNs-LM framework to address a nonlinear fractional epidemiological system for FCVP is conducted with the help of iterative convergence curves on the MSE-based fitness function, proximity analysis with the magnitude of absolute error, optimization controlling parameter nonlinear ARXNNs-LM for solving the nonlinear FCVP model, Time series illustrations with error, error-histogram analysis, autocorrelations of error, and correction of error and inputs. Additionally, three-dimensional analysis of the dynamics of the nonlinear FCVP model approximated with the nonlinear ARXNNs-LM scheme is also presented for better visual evaluation of the system model. The numerical and graphical illustration with necessary interpretation is provided in the next sections.

5 Result and Discussion

This study presents the outcomes of numerical experiments using the nonlinear ARXNNs-LM framework to address a nonlinear fractional epidemiological system for FCVP. The system includes fixed values for $f_1 = 2$, $f_2 = 3$, and $f_3 = 2$, which represent the respective connection rates of external computers, while the respective initial conditions are set at $S_0 = 20$, $I_0 = 15$, and $R_0 = 10$. The investigation considers three distinct scenarios by varying parameters: λ (the susceptibility rate), ε (the recovery rate of infected computers), and

ρ (the removal rate from the network). The analysis examines three scenarios, each with three different parameter sets, while keeping f_1 , f_2 , and f_3 constants.

Scenario-1: The influence of the infection rate on susceptible computers is analyzed by simulating the FCVP model across multiple λ values.

Scenario-2: The impact of removal mechanisms is investigated by simulating the FCVP model across varying ρ values, different rates of system cleansing.

Scenario-3: The influence of the recovery mechanism is investigated by simulating the FCVP model varying ε values, reflecting different rates of system restoration.

The study evaluates three parametric scenarios modifying λ , ρ , and ε with reference trajectories of $S(\xi)$, $I(\xi)$, and $R(\xi)$ computed through the Adams integration scheme (step size = 0.001 and terminal point on 5). Reference trajectories for $S(\xi)$, $I(\xi)$, and $R(\xi)$ obtained through the Adams method underpin the analysis. The nonlinear FCVP system is addressed using the supervised stochastic approach for computational analysis (SSACA) methodology in conjunction with 'ntstool', employing 20 hidden neurons and 501 predictors across the numerical domain [0, 5]. Dataset allocation follows a training (78%), validation (11%), and testing (11%), within a 20 hidden-layer neuron configuration. The network structure ARXNNs consists of three (input-hidden-output) layers with the training regime specifically based on optimization scheme LM, loss function MSE, and terminal epochs criteria. The networks capture temporal dependencies by relating current observations to past values of targeted time series. The subsequent discussion delivers stability characterization, convergence verification, and a defensible rationale for parameter selection.

Table 3 presents the comparative performance evaluation analysis based on MSE outcomes for the proposed ARXNNs-LM neuroarchitecture against the benchmarked techniques for scenario 1, case 1 of the FCVP model. We implemented and evaluated Recurrent Neural Network (RNN) models, specifically Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU), for time-series prediction. A sequence length (delay) of 5 was employed with a 78/11/11 train-validation-test split under a sequential data partitioning scheme. Each network consisted of a single hidden layer with 20 neurons, optimized using the Adam optimizer with a learning rate of 0.001 and mini-batch size = 64. We also implemented traditional models like decision tree, K-Nearest Neighbors, Support Vector Regression, Random Forest, Linear Regression, Extreme Gradient Boosting (XGBoost), Light Gradient Boosting Machine (LightGBM), Adaptive Boosting(AdaBoost), Lasso Regression, Ridge Regression, and Gradient Boosting. A higher MSE magnitude reveals their inadequate ability in capturing the intricate temporal dynamics inherent in the FCVP model. Additionally, the results of ARXNNs optimized with Bayesian regularization (BR), i.e., ARXNNs-BR, and scale conjugate gradient (SCG), i.e., ARXNNs-SCG, are also listed in Table 3 on the MSE metric. We also conducted the ARXNNs-LM vs. RNN/LSTM/GRU MSE for additional representative cases (e.g., Scenario-2 Case 4, Scenario-3 Case 2, Scenario-3 Case 5), but the results with similar observation and inferences as given in Table 3.

Table 3: Comparative performance evaluation analysis based on MSE outcomes for the ARXNNs-LM framework against the benchmark models for scenario-1 case 1 of the FCVP model.

Implemented Models	78/11/11—%Age			
	Neurons (Hidden Layer)	MSE (Training)	MSE (Validation)	MSE (Testing)
Decision Tree	20	0.00E+00	8.81E-02	5.88E-01
K-Nearest Neighbors	20	4.38E-05	8.90E-02	5.91E-01

(Continued)

Table 3 (continued)

Implemented Models	78/11/11—%Age			
	Neurons (Hidden Layer)	MSE (Training)	MSE (Validation)	MSE (Testing)
Support Vector Regression	20	5.05E−03	3.82E−02	2.12E−01
XGBoost	20	6.80E−06	1.24E−01	1.83E+00
Random Forest	20	6.40E−06	1.06E−01	1.02E+00
LightGBM	20	2.53E−04	1.56E−01	3.83E+00
AdaBoost	20	8.28E−03	2.47E−01	9.81E−01
Lasso Regression	20	2.00E−02	2.90E−02	6.47E−02
Ridge Regression	20	1.60E−04	4.67E−04	2.15E−03
Linear Regression	20	2.33E−11	4.81E−08	3.83E−06
Elastic Net	20	9.30E−03	1.90E−02	4.99E−02
Gradient Boosting	20	6.38E−05	1.31E−01	7.88E−01
GRU	20	4.59E−04	4.90E−04	1.63E−02
RNN	20	1.16E−04	2.98E−04	8.67E−03
LSTM	20	5.22E−05	5.36E−04	1.27E−02
ARXNNs-BR	20	7.19E−10	–	1.01E−09
ARXNNs-SCG	20	1.68E−04	1.73E−04	1.25E−04
ARXNNs-LM	20	7.72E−12 ↑	7.82E−12 ↑	8.44E−12 ↑

Table 4 provides the details for MSE values across various scenarios, including training, testing, performance grids, closing epoch, Mu grids, gradient, and time, for outcomes of ARXNNs-LM for all five cases of distinct scenarios of the nonlinear FCVP system. While outcomes for selected cases are portrayed graphically in Figs. 6–11. As illustrated in these graphs, the SSACA method effectively addresses nonlinear FCVP by using input and output values to generate performance learning plots, cross and autocorrelation plots, fitness metrics, error distribution plots, and training state trajectories, providing a comprehensive view of convergence, generalization capability, and training stability. The ARXNNs-LM approach provides accurate approximations of the dynamics of the nonlinear FCVP model with reasonably small values of AE that endorsed the effectiveness and accurateness SSACA methodologies.

Table 4: Outcomes of the ARXNNs-LM to solve the FCVP model.

Index (Scenarios)	Index (Cases)	Training (MSE)	Testing (MSE)	Validation (MSE)	Gradient Magnitude	Mu	Final Epoch	Time (s)
1	1	7.7204E−12	7.8278E−12	8.4492E−12	3.7205E−05	1E−11	1000	230
	2	9.0979E−12	4.2292E−12	5.5997E−12	1.5151E−07	1E−09	1000	220
	3	2.2580E−12	6.1377E−12	5.8873E−12	3.7908E−05	1E−12	1000	254
	4	3.5634E−11	3.4578E−11	3.6591E−11	2.0466E−07	1E−08	1000	267
	5	7.6659E−12	2.3497E−10	9.7469E12	2.7643E−06	1E−09	1000	261

(Continued)

Table 4 (continued)

Index (Scenarios)	Index (Cases)	Training (MSE)	Testing (MSE)	Validation (MSE)	Gradient Magnitude	Mu	Final Epoch	Time (s)
2	1	8.9155E-13	1.5688E-11	9.6840E-13	2.7915E-06	1E-10	1000	277
	2	6.5255E-12	1.1867E-12	2.0461E-12	2.2337E-07	1E-09	970	330
	3	2.4904E-12	1.0501E-11	2.1323E-12	4.0359E-06	1E-10	990	396
	4	4.1818E-14	1.1120E-08	3.8859E-14	1.1955E-07	1E-11	880	245
	5	1.2633E-11	1.0903E-07	9.8616E-12	1.8775E06	1E-09	913	274
3	1	6.2129E-09	1.1548E-08	4.1036E-13	4.0547E-06	1E-11	858	356
	2	8.5541E-12	1.0117E-07	1.3342E-12	1.1511E-07	1E-09	1000	317
	3	1.2516E-12	1.0274E-08	1.0672E-12	2.3639E-06	1E-10	922	3178
	4	6.1541E-12	3.7777E-12	5.5997E-12	1.4673E-07	1E-09	1000	3921
	5	3.0431E-12	2.2556E-11	3.4937E-12	1.8076E-05	1E-10	985	2041

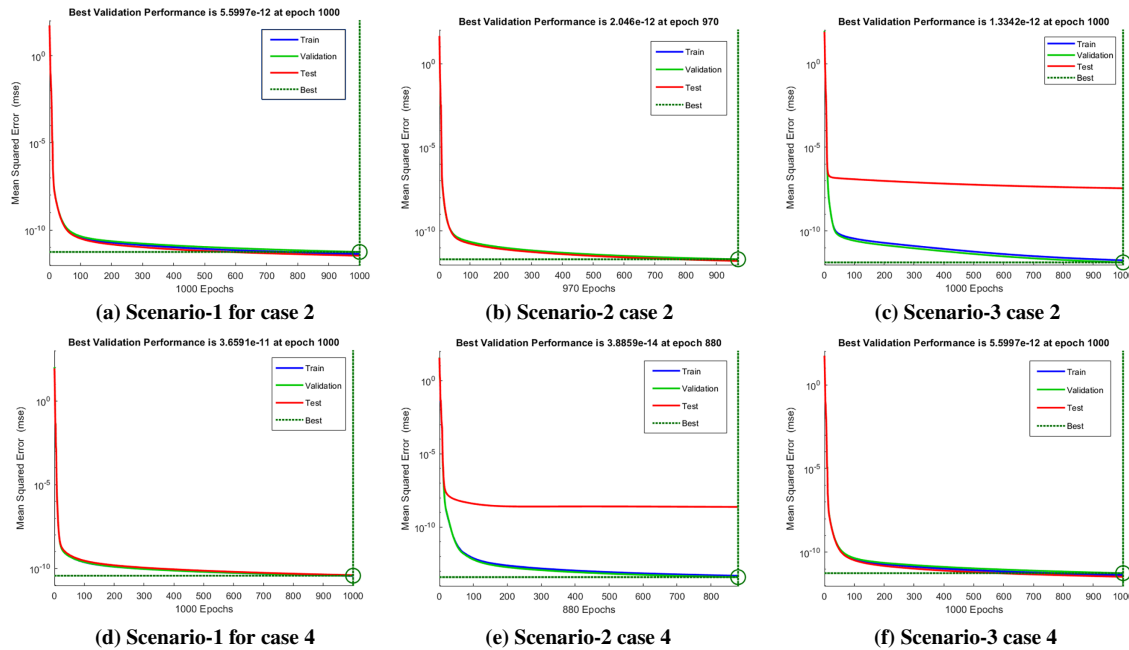


Figure 6: Performance in terms of learning curves of nonlinear ARXNNs-LM for solving the nonlinear FCVP model.

Fig. 6 illustrates the performance in terms of learning curves of nonlinear ARXNNs-LM for solving the nonlinear FCVP model. This systematic illustration allows for an in-depth evaluation of SSACA's performance in solving FCVP under different conditions. Remarkably, outstanding performance measures in terms of MSE are accomplished at levels 5.5997E-12, 3.6591E-11, 2.0461E-12, 3.8859E-14, 1.3342E-12, and 5.5997E-12 across 1000, 1000, 1000, 970, 880, and 1000, respectively, for cases two and four of three scenarios. The remaining scenarios exhibit analogous behavioral patterns, reinforcing the reliability and consistency of the proposed ARXNNs-LM technique.

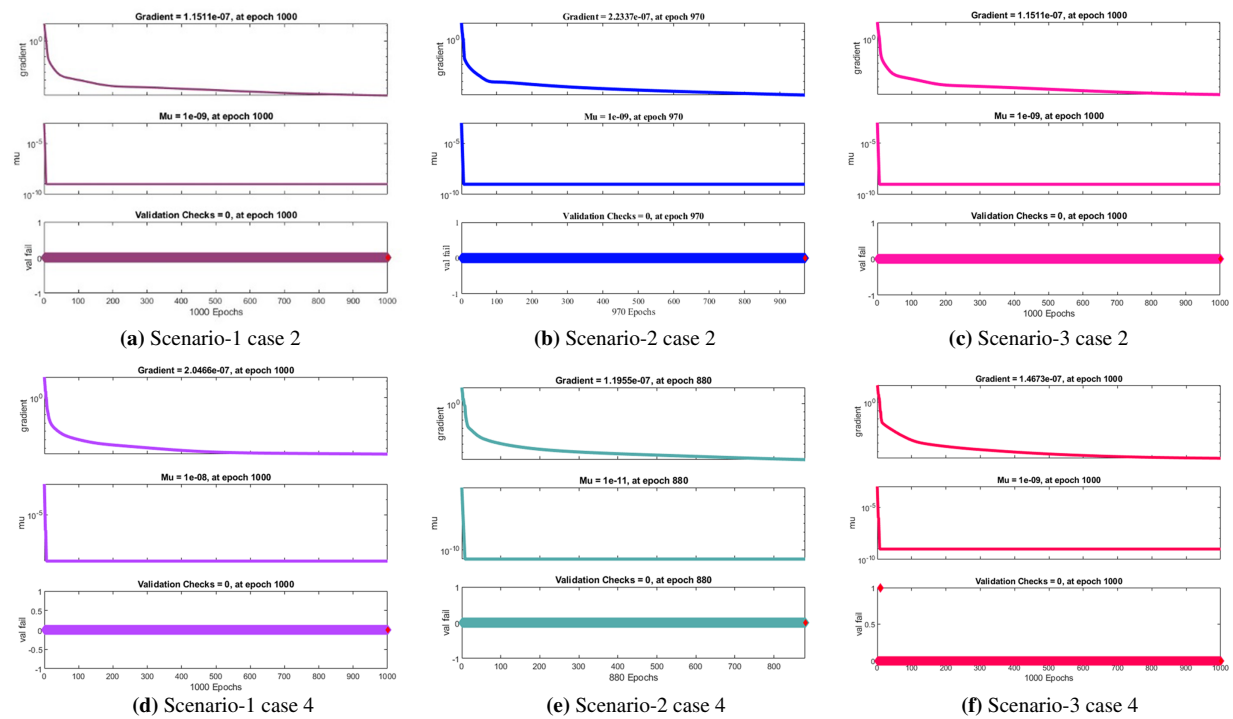


Figure 7: Optimization controlling parameter nonlinear ARXNNs-LM for solving the nonlinear FCVP model.

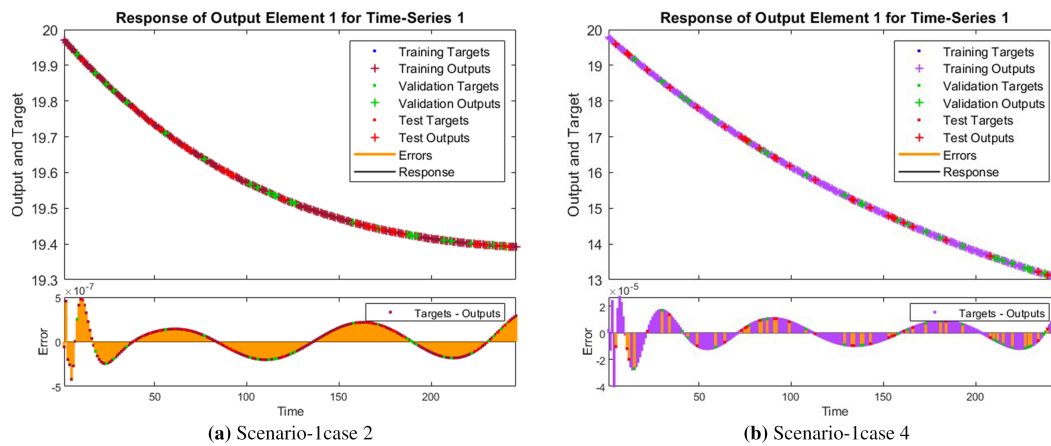


Figure 8: (Continued)

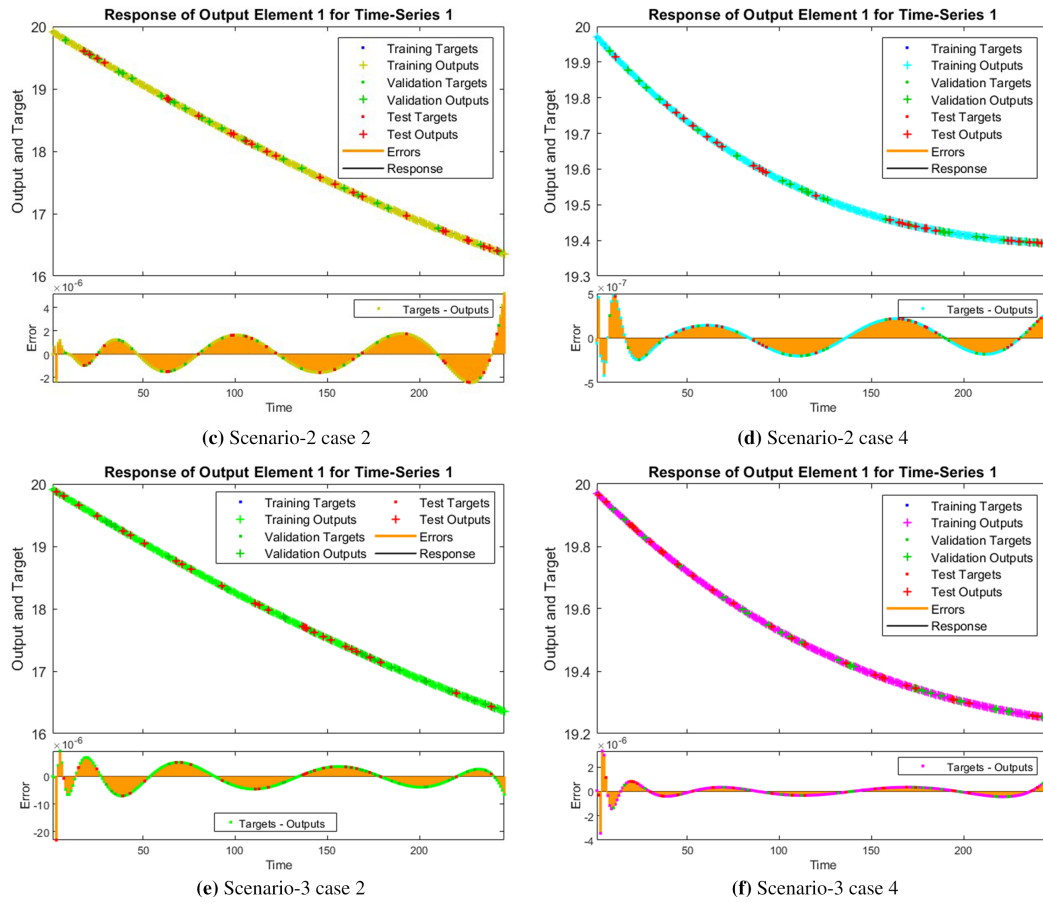


Figure 8: Time series illustrations with errors for the nonlinear ARXNNs-LM algorithm to solve the nonlinear FCVP model.

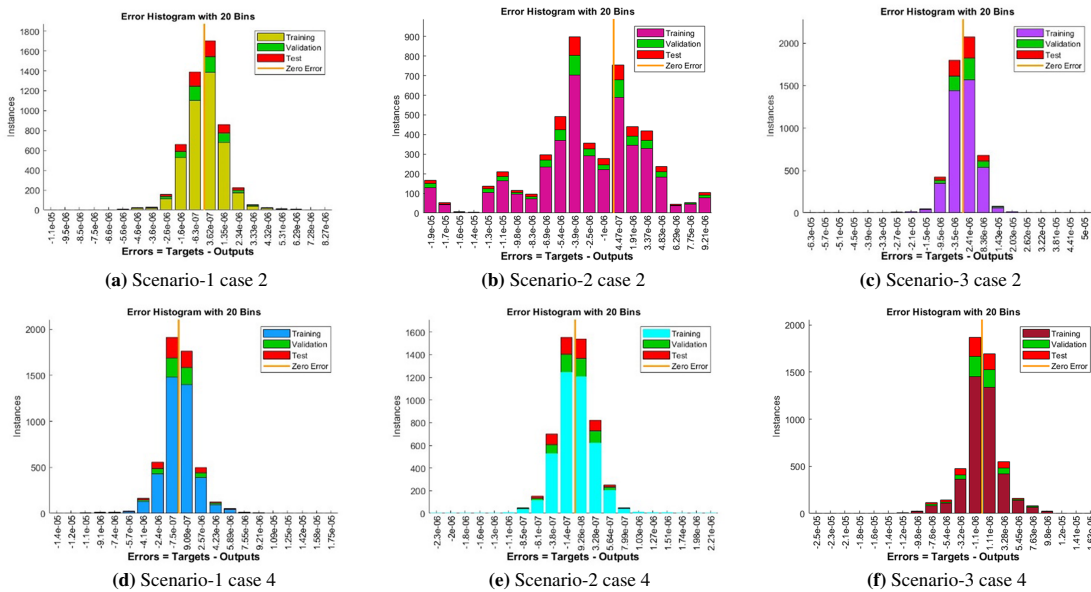


Figure 9: Error-histogram analysis of nonlinear ARXNNs-LM to solve the nonlinear FCVP model.

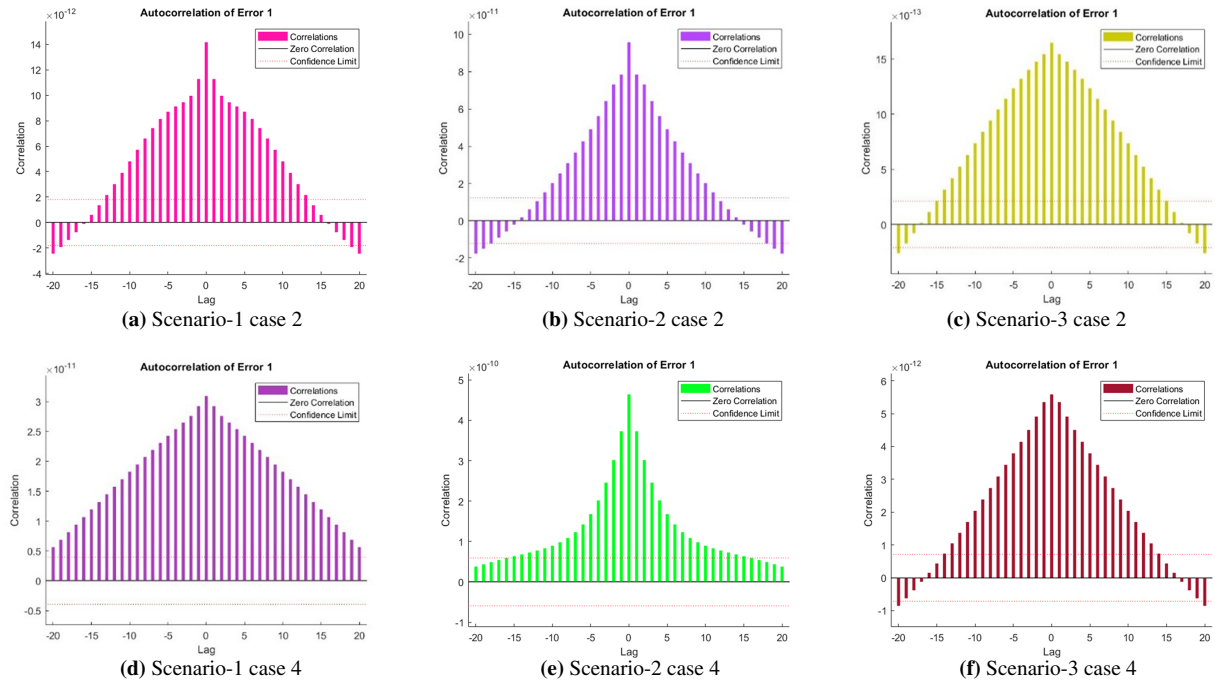


Figure 10: Autocorrelations of errors for nonlinear ARXNNs-LM to solve the nonlinear FCVP model.

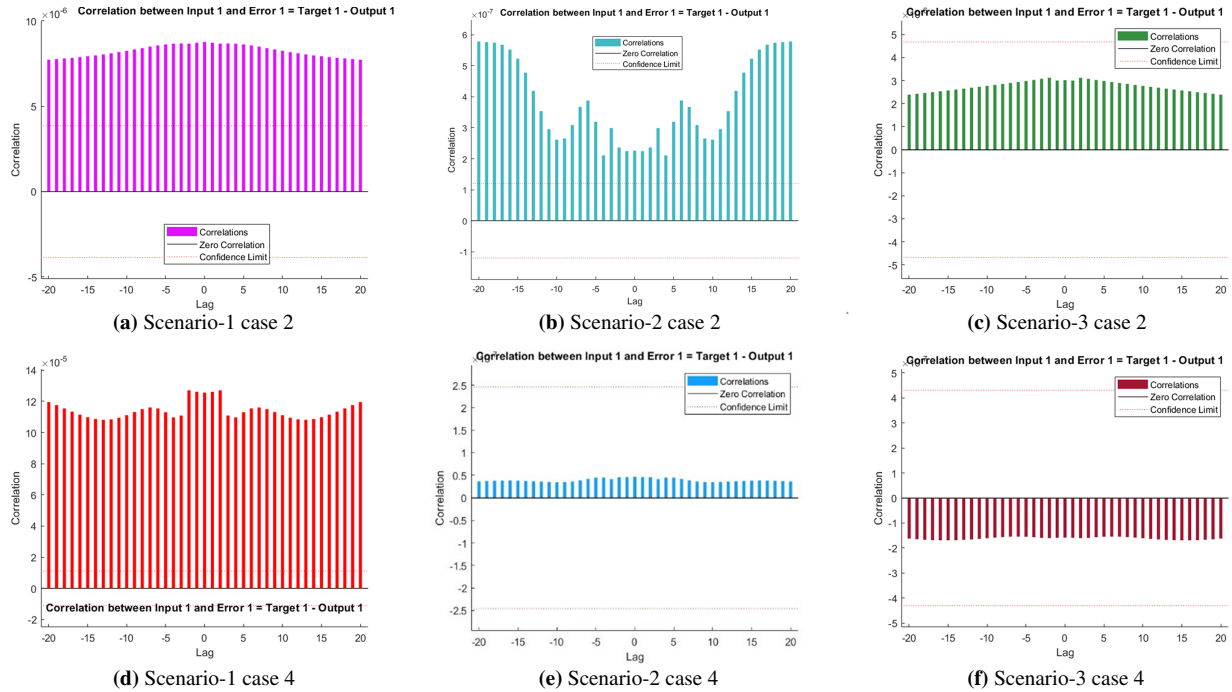


Figure 11: Correlation between error and inputs for nonlinear ARXNNs-LM to solve the nonlinear FCVP model.

The performance of the proposed SSACA in addressing the FCVP model for cases two and four of all three scenarios is measured through the optimization configuration parameters of the LM algorithm scheme as portrayed in Fig. 7. These graphs provide an assessment of the model's efficacy and highlight its adaptability

and comparative performance analysis for the selected cases across the scenarios. Fig. 8 displays the system's time-series responses alongside the corresponding error curves produced by the nonlinear ARXNNs-LM framework. The results reveal the algorithm's adaptive behavior and confirm that SSACA attains a precise approximation of the FCVP system with marginal errors. Fig. 9 provides a comprehensive analysis of the error frequency histograms of the nonlinear ARXNNs-LM technique, demonstrating the distribution of error behavior in different bins for cases 2 and 4 of all three scenarios.

Fig. 10 showcases the autocorrelation of the error for the ARXNNs-LM technique to address the temporal dynamics of the FCVP model. The graphical representation provides a comprehensive visualization of the solution generated by the proposed algorithm, offering insight into autocorrelation curves. Fig. 11 shows the relationship between input data and prediction errors in the ARXNNs-LM framework. The accompanying correlation graphs depict a comprehensive analysis of deviation between the predicted and actual values, allowing a thorough evaluation of SSACA's performance in solving the nonlinear FCVP model under varied conditions.

Fig. 12 portrayed the outcomes of ARXNNs-LM neuroarchitecture for the solutions for $S(t)$ of nonlinear epidemiological model of FCVP for all five cases $\lambda = 0.001$ Fig. 12a, $\lambda = 0.003$ Fig. 12b, $\lambda = 0.005$ Fig. 12c, $\lambda = 0.007$ Fig. 12d, and $\lambda = 0.009$ Fig. 12e of scenario-1 along with the reference GL numerical solutions for fractional order $q_0 = 1, q_1 = 0.99, q_2 = 0.97, q_3 = 0.95, q_4 = 0.91, q_5 = 0.88$ and $q_6 = 0.85$. To assess the accuracy or precision of the ARXNNs-LM scheme, the study on AE is conducted, and results are presented in Fig. 13 over the complete set of nonlinear FCVP scenarios, each examined under five different configurations of λ and seven fractional orders q . The range of AE are found 10^{-5} to 10^{-8} for $\lambda = 0.001$ Fig. 13a, 10^{-5} to 10^{-8} for $\lambda = 0.003$ Fig. 13b, 10^{-5} to 10^{-8} for $\lambda = 0.005$ Fig. 13c, 10^{-5} to 10^{-8} for $\lambda = 0.007$ Fig. 13d, and 10^{-5} to 10^{-8} for $\lambda = 0.009$ Fig. 13e. The ARXNNs-LM approach demonstrates consistently accurate performance, closely matching the reference results for scenario-1 of the FCVP system.

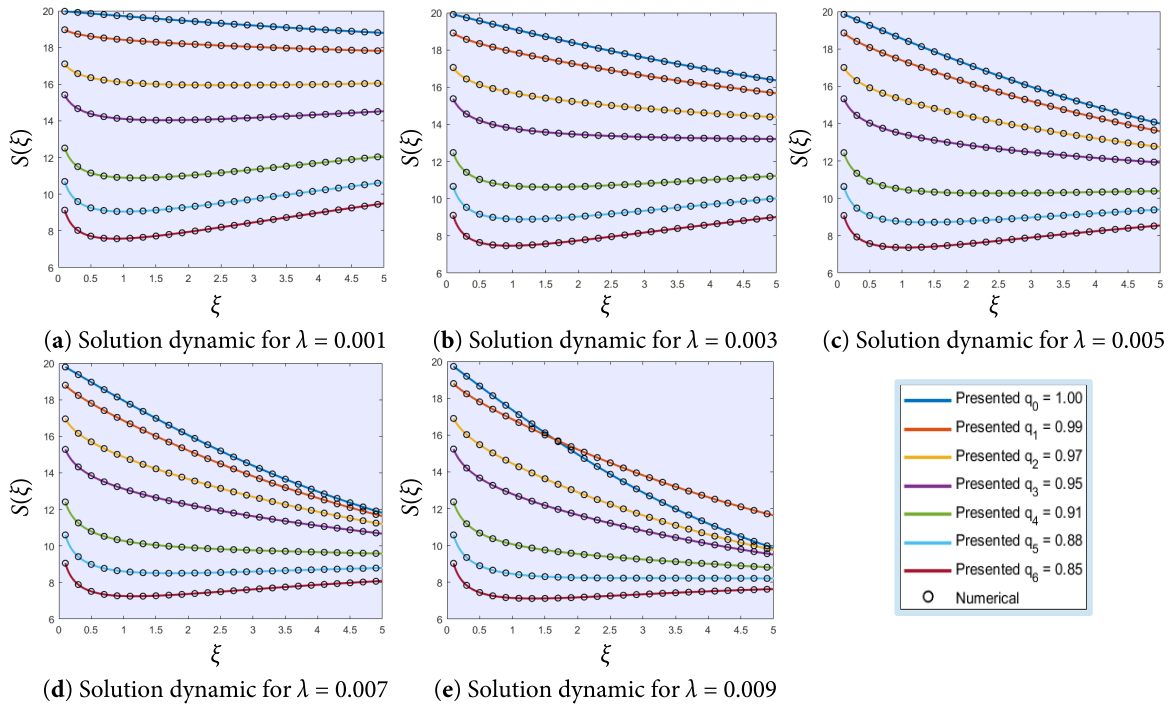


Figure 12: The numerical analysis of the nonlinear ARXNNs-LM framework for $S(\xi)$ state parameter of the nonlinear FCVP system for scenario-1.

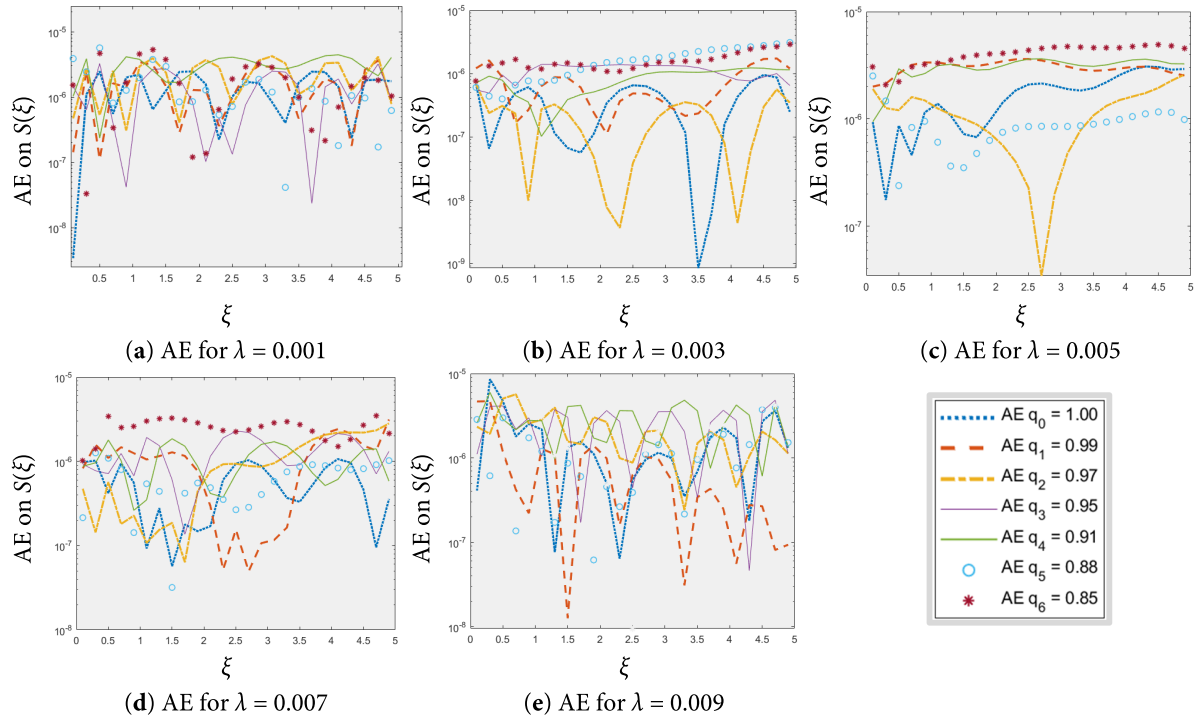


Figure 13: Comparison of AE for nonlinear ARXNNs-LM for $S(\xi)$ state parameter of the nonlinear FCVP system for scenario-1.

Fig. 14 portrayed the outcomes of ARXNNs-LM neuroarchitecture to solve the $I(t)$ of nonlinear epidemiological system for FCVP over five different configuration of $\lambda = 0.001$ Fig. 14a, $\lambda = 0.003$ Fig. 14b, $\lambda = 0.005$ Fig. 14c, $\lambda = 0.007$ Fig. 14d, and $\lambda = 0.009$ Fig. 14e of scenario-1 along with the reference GL numerical solutions for fractional order $q_0 = 1, q_1 = 0.99, q_2 = 0.97, q_3 = 0.95, q_4 = 0.91, q_5 = 0.88$ and $q_6 = 0.85$. To assess the accuracy or precision of the ARXNNs-LM scheme, the analysis of AE is conducted, and the results are presented in Fig. 15 for the nonlinear FCVP model with five variations of λ and q seven fractional values. The range of AE are found 10^{-5} to 10^{-7} for $\lambda = 0.001$ Fig. 15a, 10^{-5} to 10^{-8} for $\lambda = 0.003$ Fig. 15b, 10^{-5} to 10^{-8} for $\lambda = 0.005$ Fig. 15c, 10^{-5} to 10^{-8} for $\lambda = 0.007$ Fig. 15d, and 10^{-5} to 10^{-8} for $\lambda = 0.009$ Fig. 15e. Scenario-1 demonstrates that the ARXNNs-LM framework achieves a strong and stable correspondence with the benchmark solution, indicating reliable approximation performance.

Fig. 16 portrayed the outcomes of the ARXNNs-LM neuroarchitecture to solve $R(t)$ of nonlinear epidemiological system for FCVP over 5 different configurations of $\lambda = 0.001$ Fig. 16a, $\lambda = 0.003$ Fig. 16b, $\lambda = 0.005$ Fig. 16c, $\lambda = 0.007$ Fig. 16d, and $\lambda = 0.009$ Fig. 16e of scenario-1 along with the reference GL numerical solutions for fractional order $q_0 = 1, q_1 = 0.99, q_2 = 0.97, q_3 = 0.95, q_4 = 0.91, q_5 = 0.88$ and $q_6 = 0.85$.

To assess the accuracy or precision of the ARXNNs-LM framework, the analysis of AE is conducted, and results are presented in Fig. 17 for all the cases of the nonlinear FCVP model for five variations of λ , and fractional order values of q . The range of AE are found 10^{-5} to 10^{-8} for $\lambda = 0.001$ Fig. 17a, 10^{-5} to 10^{-8} for $\lambda = 0.003$ Fig. 17b, 10^{-5} to 10^{-7} for $\lambda = 0.005$ Fig. 17c, 10^{-5} to 10^{-9} for $\lambda = 0.007$ Fig. 17d, and 10^{-5} to 10^{-7} for $\lambda = 0.009$ Fig. 17e. Scenario-1 demonstrates that the ARXNNs-LM framework achieves a strong and stable correspondence with the benchmark solution, indicating reliable approximation performance. In-depth analysis of the dynamics is portrayed with the help of 3D graphs to envision the complex interactions or relations between multiple variables instantaneously for scenario-1 of the nonlinear FCVP model, as shown in Fig. 18.

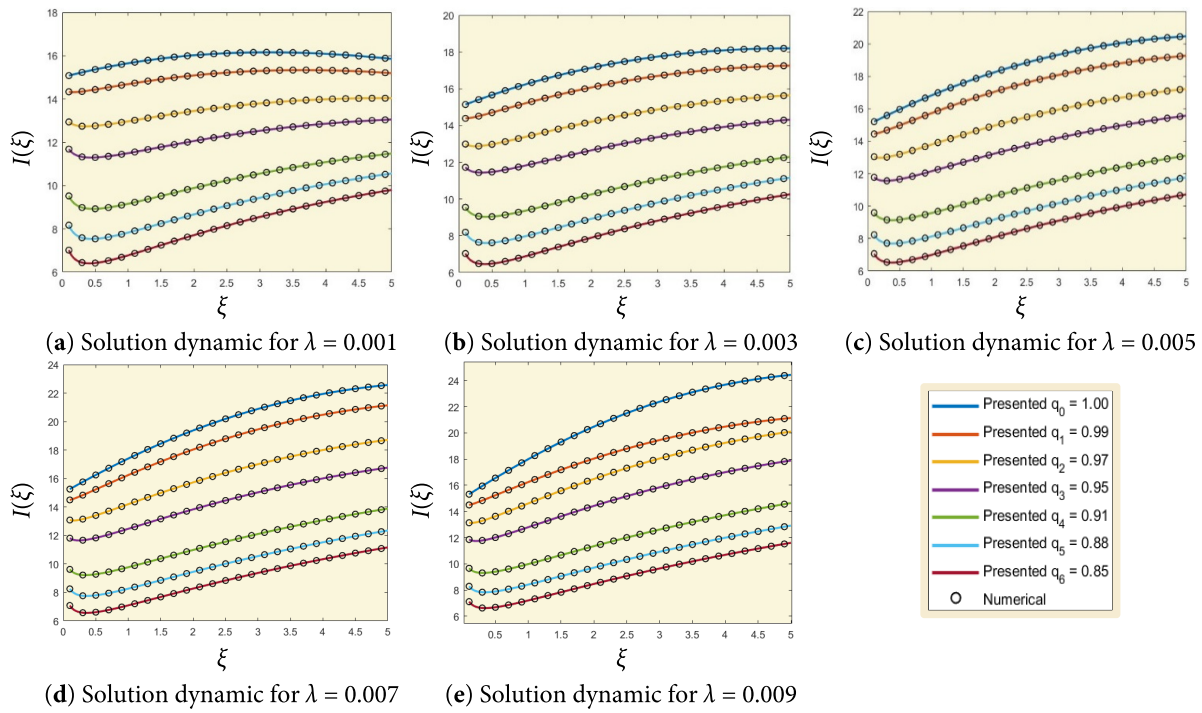


Figure 14: The numerical analysis of the nonlinear ARXNNs-LM framework for $I(\xi)$ state parameter of the nonlinear FCVP system for scenario-1.

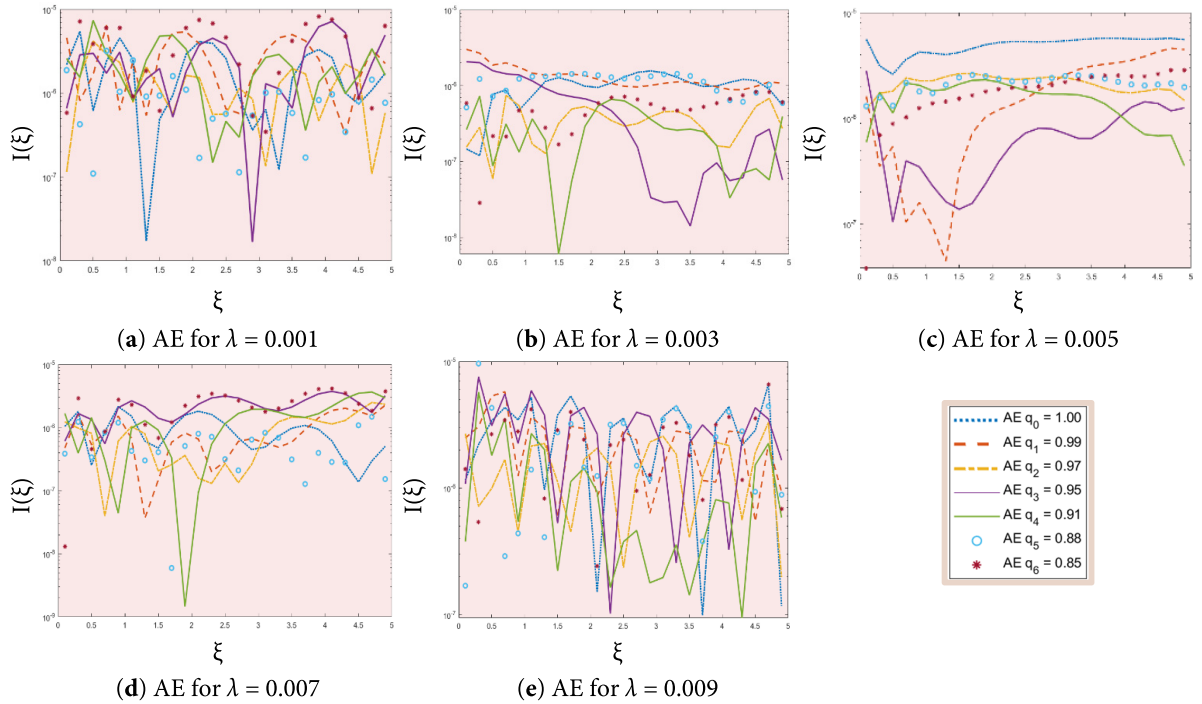


Figure 15: Comparison of AE for nonlinear ARXNNs-LM for $I(\xi)$ state parameter of the nonlinear FCVP system for scenario-1.

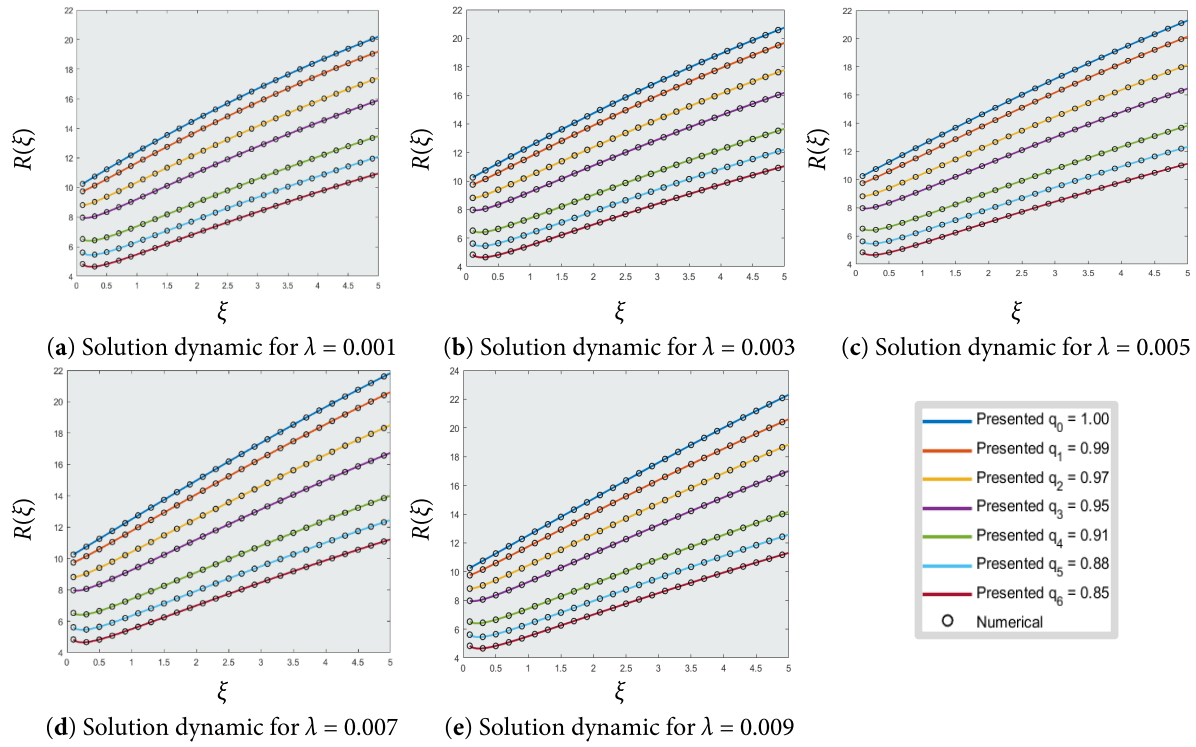


Figure 16: The numerical analysis of the nonlinear ARXNNs-LM framework for $R(\xi)$ state parameter of the nonlinear FCVP system for scenario-1.

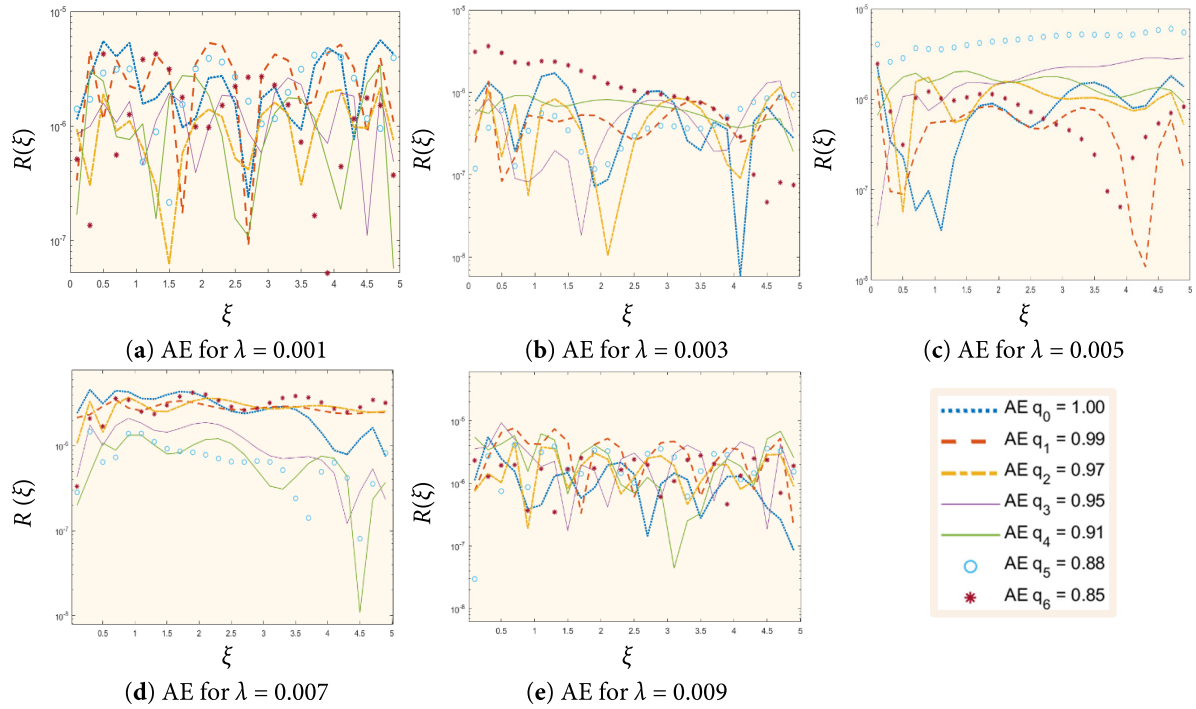


Figure 17: Comparison of AE for nonlinear ARXNNs-LM for $R(\xi)$ state parameter of the nonlinear FCVP system for scenario-1.

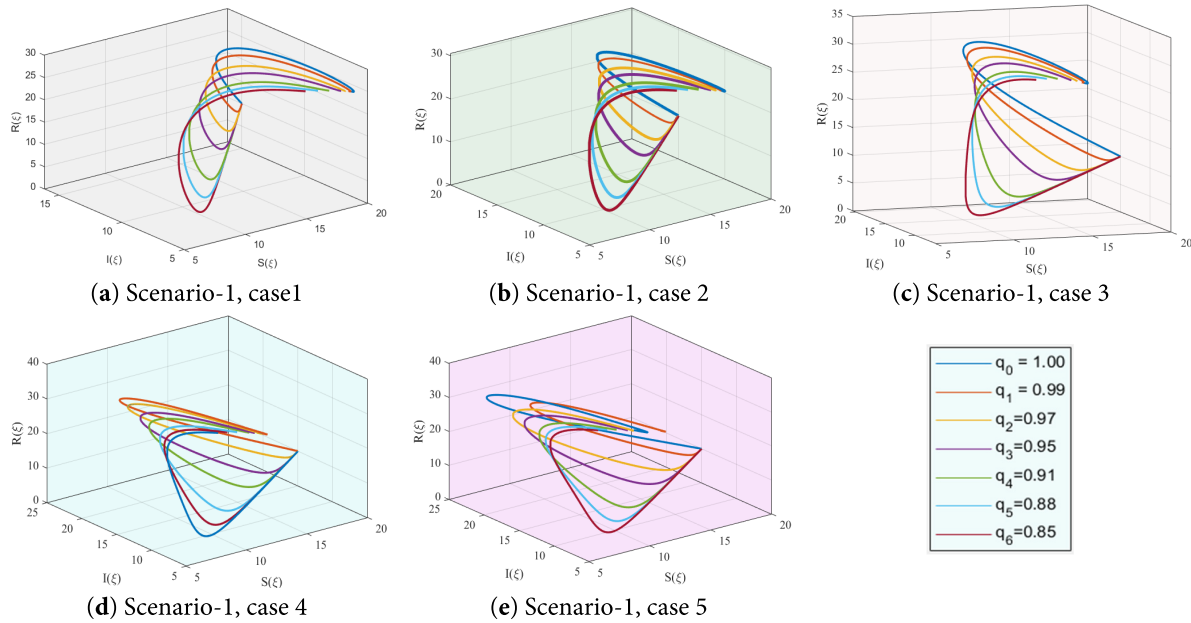


Figure 18: The three-dimensional analysis of the dynamics of the nonlinear FCVP model approximated with the nonlinear ARXNNs-LM scheme for scenario-1.

By plotting three variables $S(\xi)$, $I(\xi)$, and $R(\xi)$ in a three-dimensional space, these graphs provide a complete interpretation of their interactions by varying λ (the rate of susceptibility), ρ (the removal rate from the network), and ε (the recovery rate of infected computers) for all 6 fractional orders along with integer orders. They capture dynamic changes over time, effectively providing insight into how the system evolves. Fig. 19 portrayed the outcomes of ARXNNs-LM neuroarchitecture to solve $S(t)$ of nonlinear epidemiological system for FCVP for all five cases $\rho = 0.1$ Fig. 19a, $\rho = 0.2$ Fig. 19b, $\rho = 0.3$ Fig. 19c, $\rho = 0.4$ Fig. 19d, and $\rho = 0.5$ Fig. 19e of scenario-2 along with the reference GL numerical solutions for fractional order $q_0 = 1$, $q_1 = 0.99$, $q_2 = 0.97$, $q_3 = 0.95$, $q_4 = 0.91$, $q_5 = 0.88$ and $q_6 = 0.85$.

To assess the accuracy or precision of the ARXNNs-LM framework, the analysis of AE is conducted, and results are presented in Fig. 20 for the nonlinear FCVP model for five variations of ρ and seven fractional values of q . The range of AE are found 10^{-5} to 10^{-8} for $\rho = 0.001$ Fig. 20a, 10^{-5} to 10^{-9} for $\rho = 0.2$ Fig. 20b, 10^{-5} to 10^{-9} for $\rho = 0.3$ Fig. 20c, 10^{-5} to 10^{-9} for $\rho = 0.4$ Fig. 20d, and 10^{-4} to 10^{-9} for $\rho = 0.5$ Fig. 20e. Scenario-2 demonstrates that the ARXNNs-LM framework achieves a strong and stable correspondence with the benchmark solution, indicating reliable approximation performance. Fig. 21 portrayed the outcomes of ARXNNs-LM neuroarchitecture to solve $I(t)$ of nonlinear epidemiological system for FCVP over different configurations of $\rho = 0.1$ Fig. 21a, $\rho = 0.2$ Fig. 21b, $\rho = 0.3$ Fig. 21c, $\rho = 0.4$ Fig. 21d, and $\rho = 0.5$ Fig. 21e of scenario-2 along with the reference GL numerical solutions for fractional order $q_0 = 1$, $q_1 = 0.99$, $q_2 = 0.97$, $q_3 = 0.95$, $q_4 = 0.91$, $q_5 = 0.88$, and $q_6 = 0.85$. To assess the accuracy or precision of the ARXNNs-LM scheme, scrutiny on AE is conducted, and results are presented in Fig. 22 for all the cases of the nonlinear FCVP model for five variations of ρ and seven differential orders q .

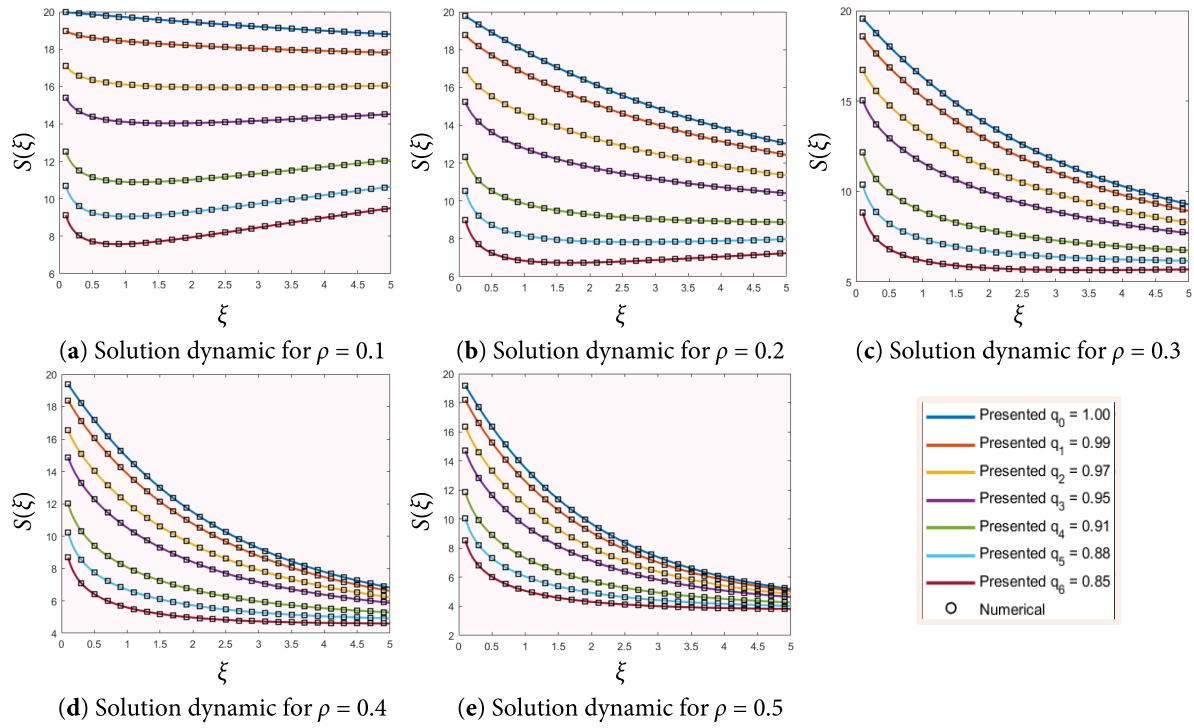


Figure 19: The numerical analysis of the nonlinear ARXNNs-LM framework for $S(\xi)$ state parameter of the nonlinear FCVP system for scenario-2.

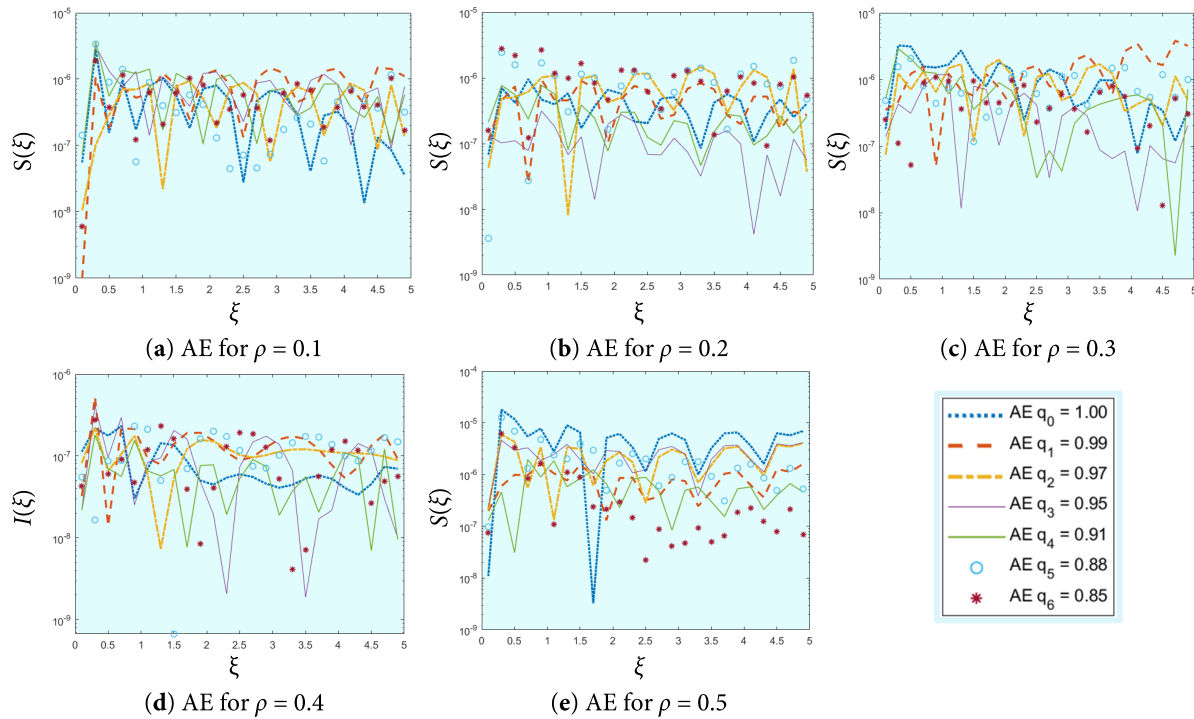


Figure 20: Comparison of AE for nonlinear ARXNNs-LM for $S(\xi)$ state parameter of the nonlinear FCVP system for scenario-2.

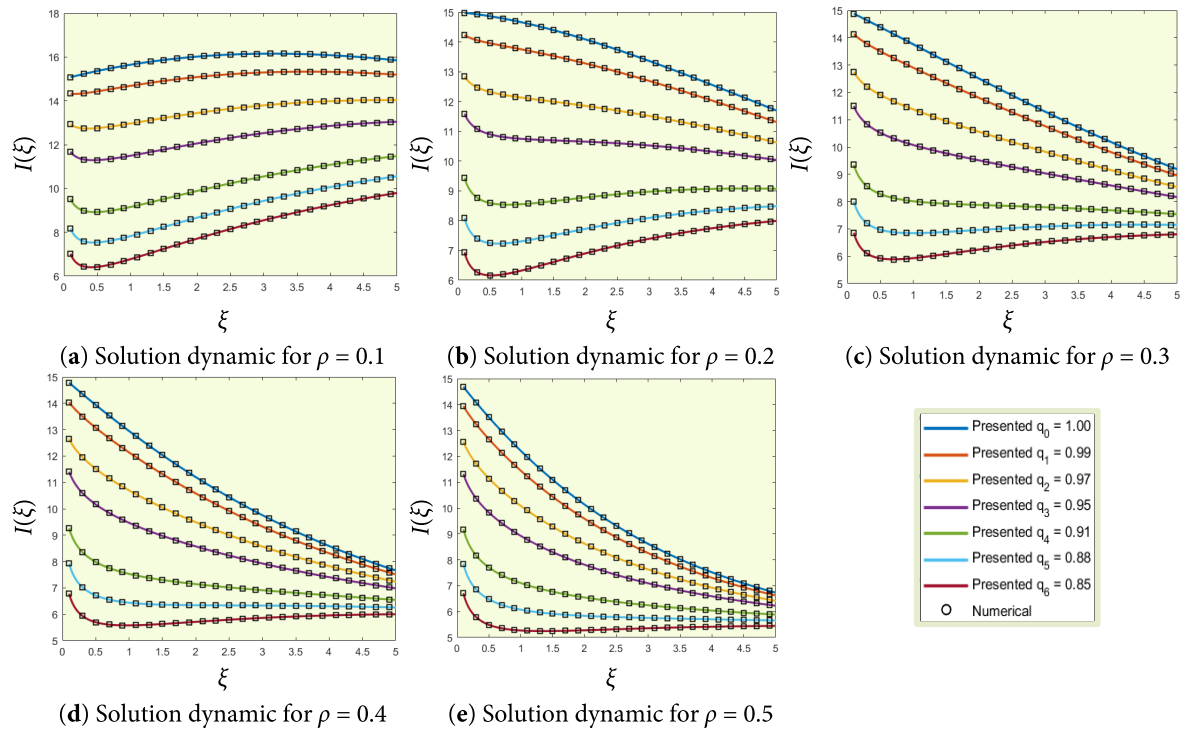


Figure 21: The numerical analysis of the nonlinear ARXNNs-LM framework for $I(\xi)$ state parameter of the nonlinear FCVP system for scenario-2.

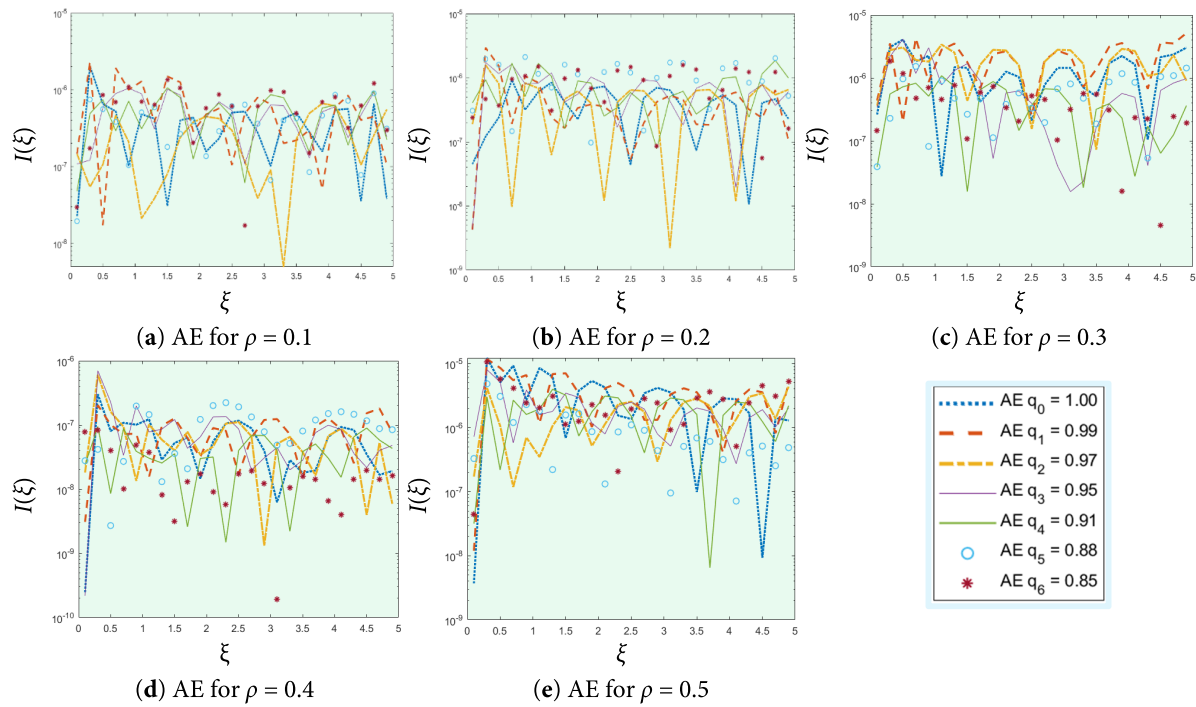


Figure 22: Comparison of AE for nonlinear ARXNNs-LM for $I(\xi)$ state parameter of the nonlinear FCVP system for scenario-2.

The range of AE are found 10^{-5} to 10^{-9} for $\rho = 0.001$ Fig. 22a, 10^{-5} to 10^{-9} for $\rho = 0.2$ Fig. 22b, 10^{-5} to 10^{-9} for $\rho = 0.3$ Fig. 22c, 10^{-6} to 10^{-9} for $\rho = 0.4$ Fig. 22d, and 10^{-4} to 10^{-9} for $\rho = 0.5$ Fig. 22e. Scenario-2 demonstrates that the ARXNNs-LM framework achieves a strong and stable correspondence with the benchmark solution, indicating reliable approximation performance. Fig. 23 portrayed the outcomes of ARXNNs-LM neuroarchitecture to solve $R(t)$ of nonlinear epidemiological system for FCVP across different configurations of $\rho = 0.1$ Fig. 23a, $\rho = 0.2$ Fig. 23b, $\rho = 0.3$ Fig. 23c, $\rho = 0.4$ Fig. 23d, and $\rho = 0.5$ Fig. 23e of scenario-2 along with the reference GL numerical solutions for fractional order $q_0 = 1, q_1 = 0.99, q_2 = 0.97, q_3 = 0.95, q_4 = 0.91, q_5 = 0.88, \text{ and } q_6 = 0.85$. To assess the accuracy or precision of the ARXNNs-LM framework, the analysis of AE is conducted, and results are presented in Fig. 24 for all the cases of the nonlinear FCVP model for five variations of ρ and seven fractional values q . The range of AE are found 10^{-5} to 10^{-9} for $\rho = 0.001$ Fig. 24a, 10^{-5} to 10^{-9} for $\rho = 0.2$ Fig. 24b, 10^{-5} to 10^{-9} for $\rho = 0.3$ Fig. 24c, 10^{-6} to 10^{-9} for $\rho = 0.4$ Fig. 24d, and 10^{-4} to 10^{-9} for $\rho = 0.5$ Fig. 24e. Scenario-2 demonstrates that the ARXNNs-LM framework achieves a strong and stable correspondence with the benchmark solution, indicating reliable approximation performance.

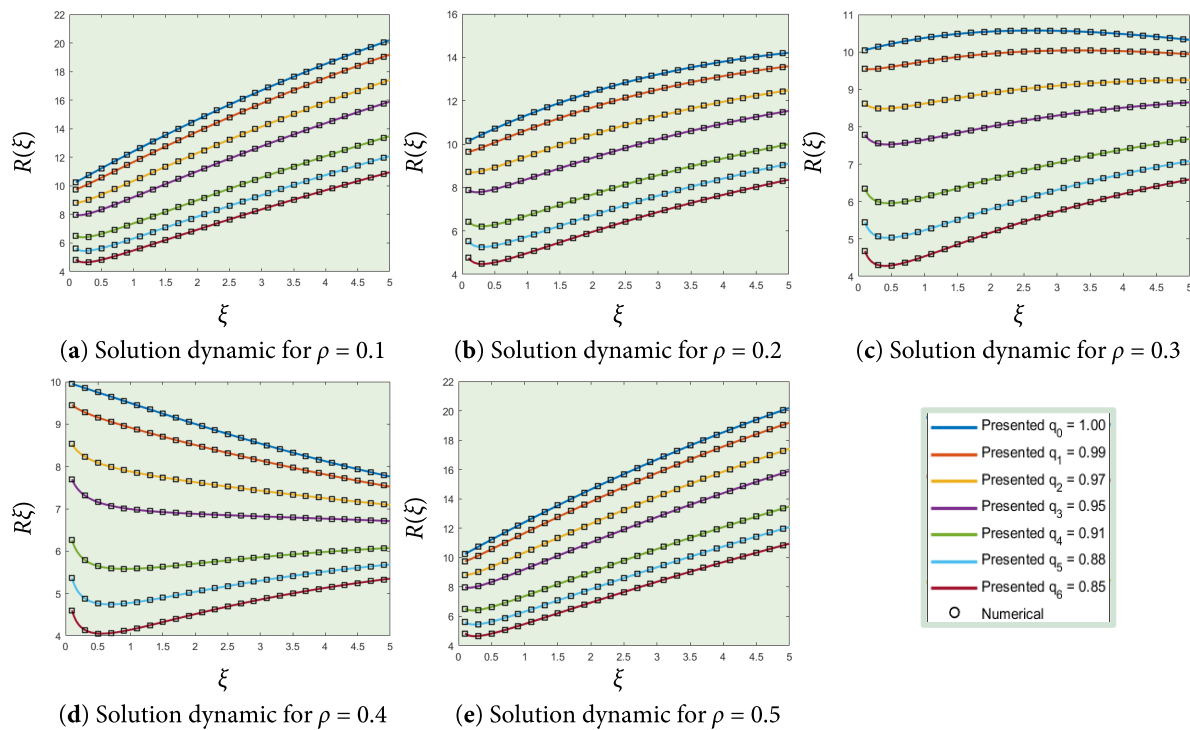


Figure 23: The numerical analysis of the nonlinear ARXNNs-LM framework for $R(\xi)$ state parameter of the nonlinear FCVP system for scenario-2.

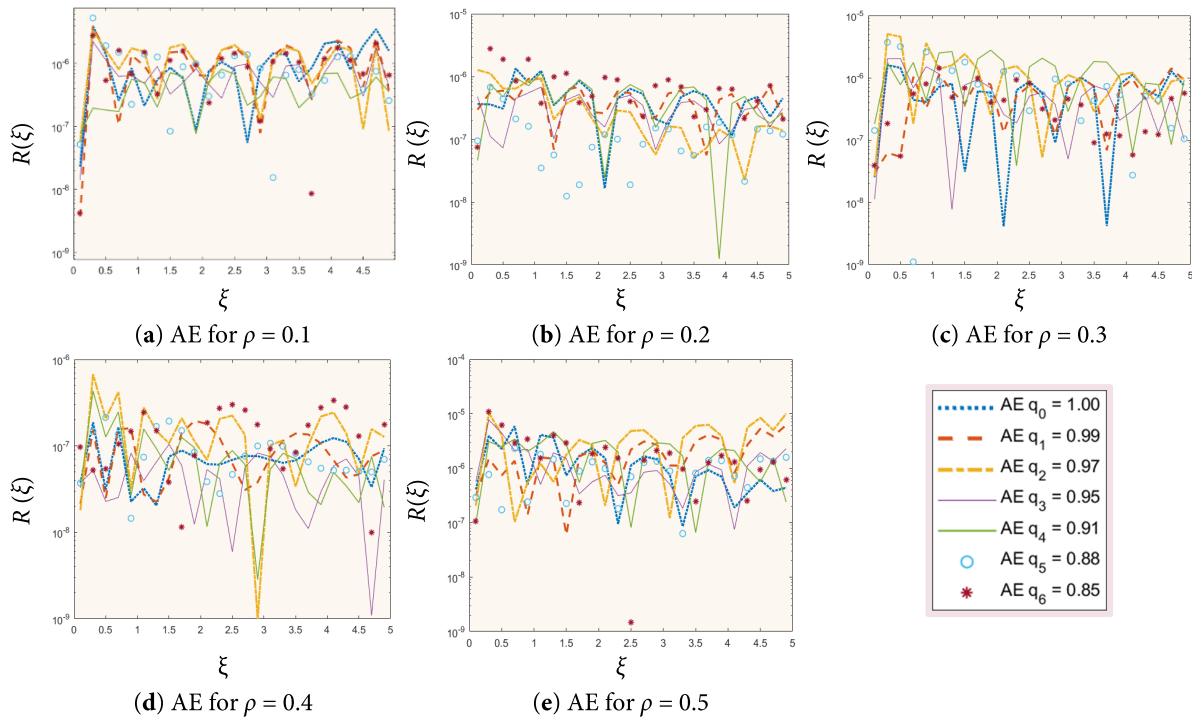


Figure 24: Comparison of AE for nonlinear ARXNNs-LM for $R(\xi)$ state parameter of the nonlinear FCVP system for scenario-2.

In-depth analysis of the dynamics is portrayed with the help of 3D graphs to visualize the intricate interactions or relations between multiple variables instantaneously for scenario-2 of the nonlinear FCVP model, as shown in Fig. 25. By plotting three variables $S(\xi)$, $I(\xi)$, and $R(\xi)$ in a three-dimensional space, these graphs provide a complete interpretation of their interactions by varying λ (the rate of susceptibility) and ρ (the removal rate from the network). and ε (the recovery rate of infected computers) for all 6 fractional orders, along with integer order. They capture dynamic changes over time, effectively providing insight into how the system evolves. Fig. 26 portrayed the outcomes of ARXNNs-LM framework to solve $S(t)$ of nonlinear epidemiological system for FCVP across different configurations of $\varepsilon = 0.1$ Fig. 26a, $\varepsilon = 0.2$ Fig. 26b, $\varepsilon = 0.3$ Fig. 26c, $\varepsilon = 0.4$ Fig. 26d, and $\varepsilon = 0.5$ Fig. 26e of scenario-3 along with the reference GL numerical solutions for fractional order $q_0 = 1$, $q_1 = 0.99$, $q_2 = 0.97$, $q_3 = 0.95$, $q_4 = 0.91$, $q_5 = 0.88$ and $q_6 = 0.85$. To assess the accuracy or precision of the ARXNNs-LM framework, the analysis of AE is conducted, and results are presented in Fig. 27 for all the cases of the nonlinear FCVP model for five variations of ε and fractional values of q . The range of AE are found 10^{-5} to 10^{-8} for $\varepsilon = 0.001$ Fig. 27a, 10^{-5} to 10^{-9} for $\varepsilon = 0.2$ Fig. 27b, 10^{-5} to 10^{-9} for $\varepsilon = 0.3$ Fig. 27c, 10^{-5} to 10^{-9} for $\varepsilon = 0.4$ Fig. 27d, and 10^{-4} to 10^{-9} for $\varepsilon = 0.5$ Fig. 27e Scenario-3 demonstrates that the ARXNNs-LM frame work achieves a strong and stable correspondence with the benchmark solution, indicating reliable approximation performance. Fig. 28 portrayed the outcomes of ARXNNs-LM neuroarchitecture to solve $I(t)$ of nonlinear epidemiological system for FCVP across different configurations of $\varepsilon = 0.1$ Fig. 28a, $\varepsilon = 0.2$ Fig. 28b, $\varepsilon = 0.3$ Fig. 28c, $\varepsilon = 0.4$ Fig. 28d, and $\varepsilon = 0.5$ Fig. 28e of scenario-3 along with the reference GL numerical solutions for fractional order $q_0 = 1$, $q_1 = 0.99$, $q_2 = 0.97$, $q_3 = 0.95$, $q_4 = 0.91$, $q_5 = 0.88$ and $q_6 = 0.85$. To assess the accuracy or precision of the ARXNNs-LM framework, the analysis of AE is conducted, and results are presented in Fig. 29 for all the cases of the nonlinear FCVP model for five variations of ε and seven differential orders q . The range of AE are found 10^{-5} to 10^{-8} for $\varepsilon = 0.1$ Fig. 29a, 10^{-5} to 10^{-9} for $\varepsilon = 0.2$ Fig. 29b, 10^{-5} to 10^{-9} for $\varepsilon = 0.3$ Fig. 29c, 10^{-5} to 10^{-9}

for $\varepsilon = 0.4$ Fig. 29d, and 10^{-4} to 10^{-9} for $\varepsilon = 0.5$ Fig. 29e. Scenario-3 demonstrates that the ARXNNs-LM framework achieves a strong and stable correspondence with the benchmark solution, indicating reliable approximation performance.

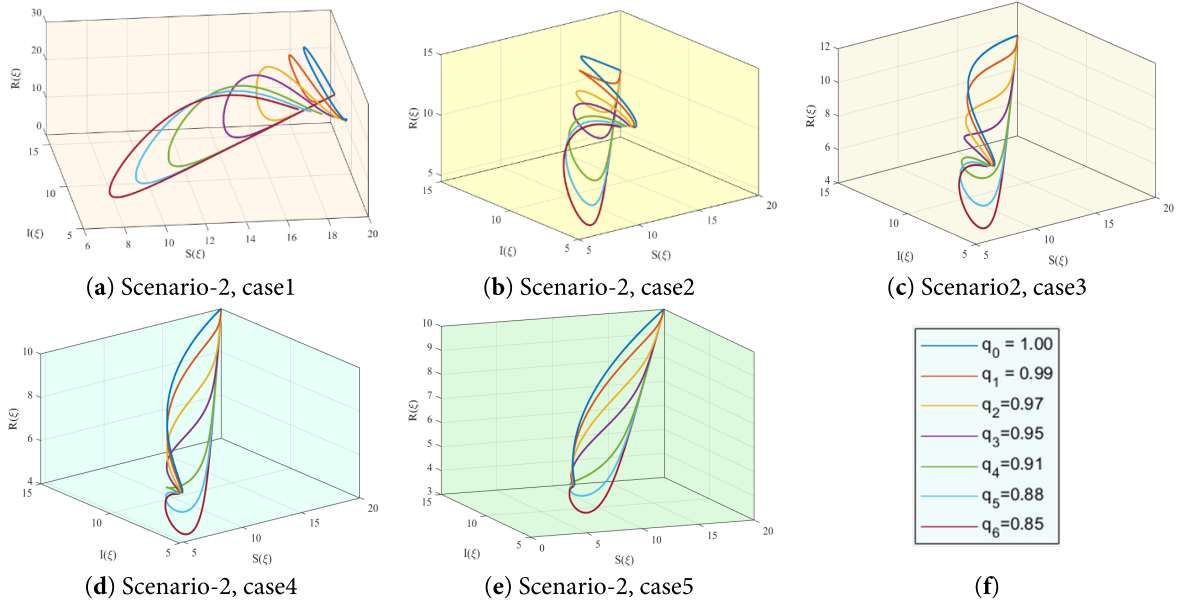


Figure 25: The three-dimensional analysis of the dynamics of the nonlinear FCVP model approximated with the nonlinear ARXNNs-LM scheme for scenario-2.

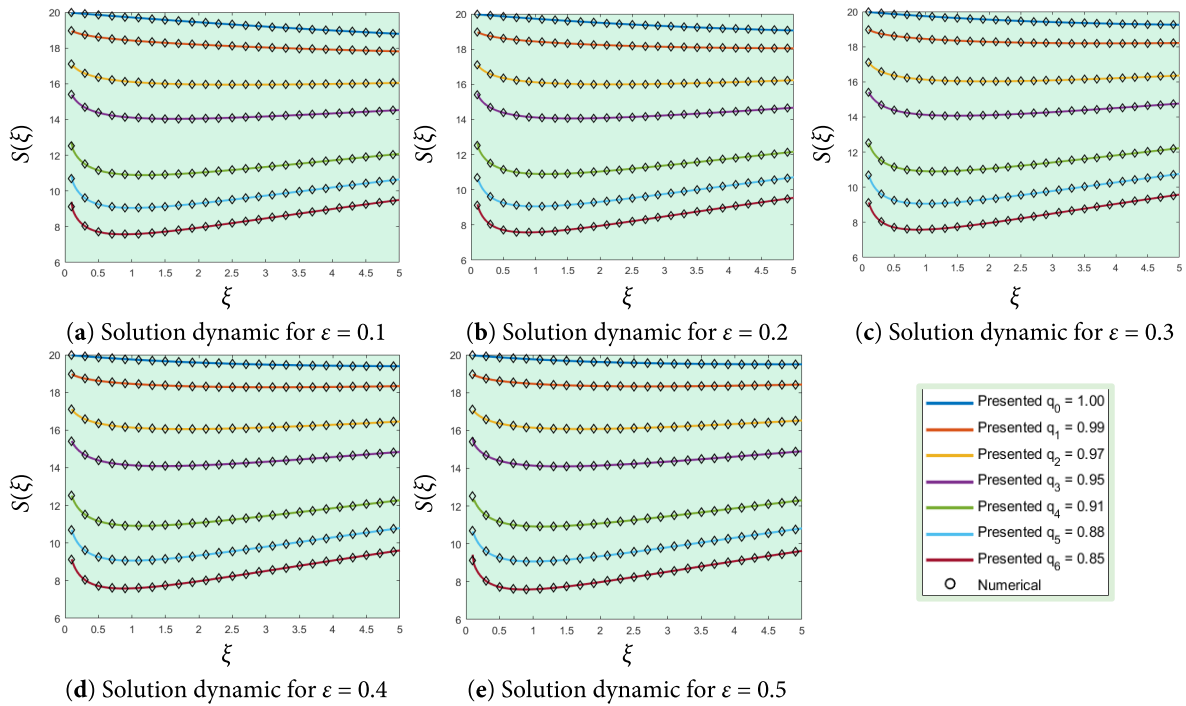


Figure 26: The numerical analysis of the nonlinear ARXNNs-LM framework for the $S(\xi)$ state parameter of the nonlinear FCVP system for scenario-3.

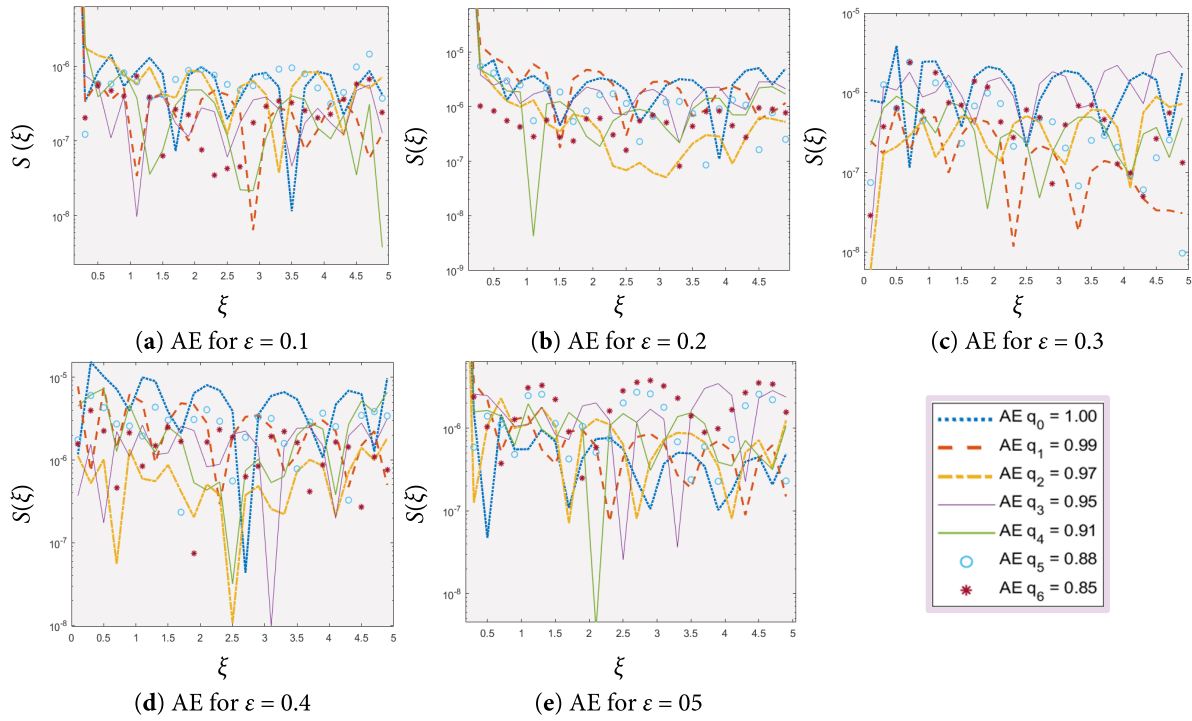


Figure 27: Comparison of AE for nonlinear ARXNNs-LM for $S(\xi)$ state parameter of the nonlinear FCVP system for scenario-3.

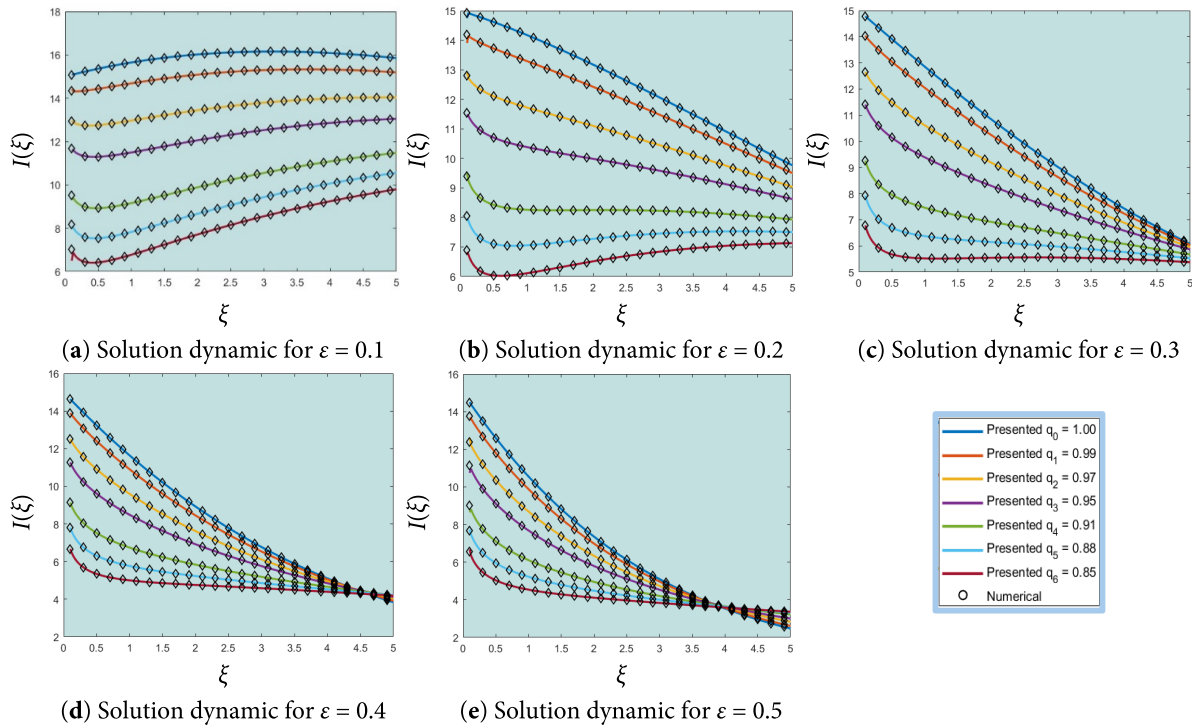


Figure 28: The numerical analysis of the nonlinear ARXNNs-LM framework for $I(\xi)$ state parameter of the nonlinear FCVP system for scenario-3.

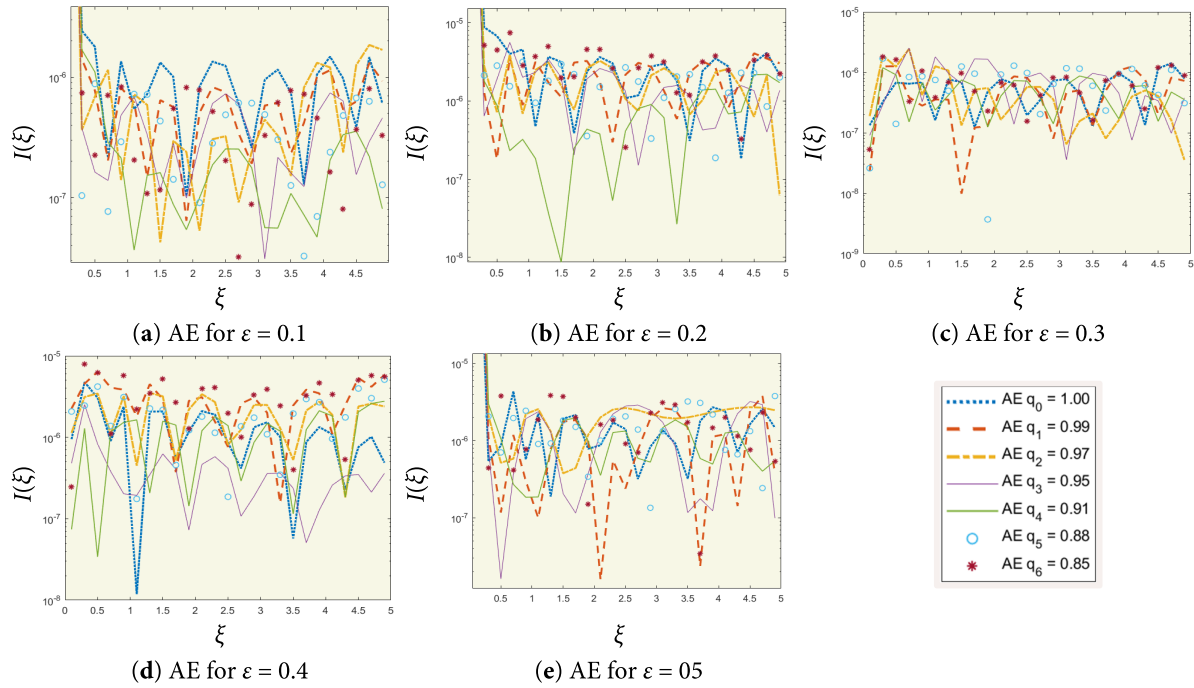


Figure 29: Comparison of AE for nonlinear ARXNNs-LM for $I(\xi)$ state parameter of the nonlinear FCVP system for scenario-3.

Fig. 30 portrayed the outcomes of ARXNNs-LM neuroarchitecture to solve $R(t)$ of nonlinear epidemiological system for FCVP across different configurations of $\varepsilon = 0.1$ Fig. 30a, $\varepsilon = 0.2$ Fig. 30b, $\varepsilon = 0.3$ Fig. 30c, $\varepsilon = 0.4$ Fig. 30d, and $\varepsilon = 0.5$ Fig. 30e of scenario-3 along with the reference GL numerical solutions for fractional order $q_0 = 1, q_1 = 0.99, q_2 = 0.97, q_3 = 0.95, q_4 = 0.91, q_5 = 0.88$ and $q_6 = 0.85$. To assess the accuracy or precision of the ARXNNs-LM framework, the analysis of AE is conducted, and results are presented in Fig. 31 for all the cases of the nonlinear FCVP model for five variations of ε and q fractional order values. The range of AE are found 10^{-2} to 10^{-10} for $\varepsilon = 0.1$ Fig. 31a, 10^{-4} to 10^{-12} for $\varepsilon = 0.2$ Fig. 31b, 10^{-5} to 10^{-9} for $\varepsilon = 0.3$ Fig. 31c, 10^{-5} to 10^{-8} for $\varepsilon = 0.4$ Fig. 31d, and 10^{-4} to 10^{-12} for $\varepsilon = 0.5$ Fig. 31e. Scenario-3 demonstrates that the ARXNNs-LM framework achieves a strong and stable correspondence with the benchmark solution, indicating reliable approximation performance.

In-depth analysis of the dynamics is portrayed with the help of 3D graphs to envision the complex interactions or relations between multiple variables instantaneously for scenario-3 of the nonlinear FCVP model, as shown in Fig. 32. By plotting three variables $S(\xi)$, $I(\xi)$, and $R(\xi)$ in a three-dimensional space, these graphs provide a complete interpretation of their interactions by varying λ (the rate of susceptibility), ρ (the removal rate from the network), and ε (the recovery rate of infected computers) for all 6 fractional orders along with integer orders. They capture dynamic changes over time, effectively providing insight into how the system evolves.

The analysis of variance (ANOVA) test is employed by leveraging ARXNNs to examine the group-level differences, aided with different optimization algorithms, LM, Bayesian regularization (BR), and scaled conjugate gradient (SCG) for state parameters $S(\xi)$, $I(\xi)$, and $R(\xi)$ of the FCVP model. The ANOVA outcomes for scenario-1 case1 are tabulated in Table 5, analysis reports SS, df, MS, F-statistics, and p -values (Prob > F). A consistent pattern of low SS variability is monitored for ARXNNs-LM, ARXNNs-BR, and ARXNNs-SCG, while ARXNNs-SCG demonstrates relatively larger dispersion.

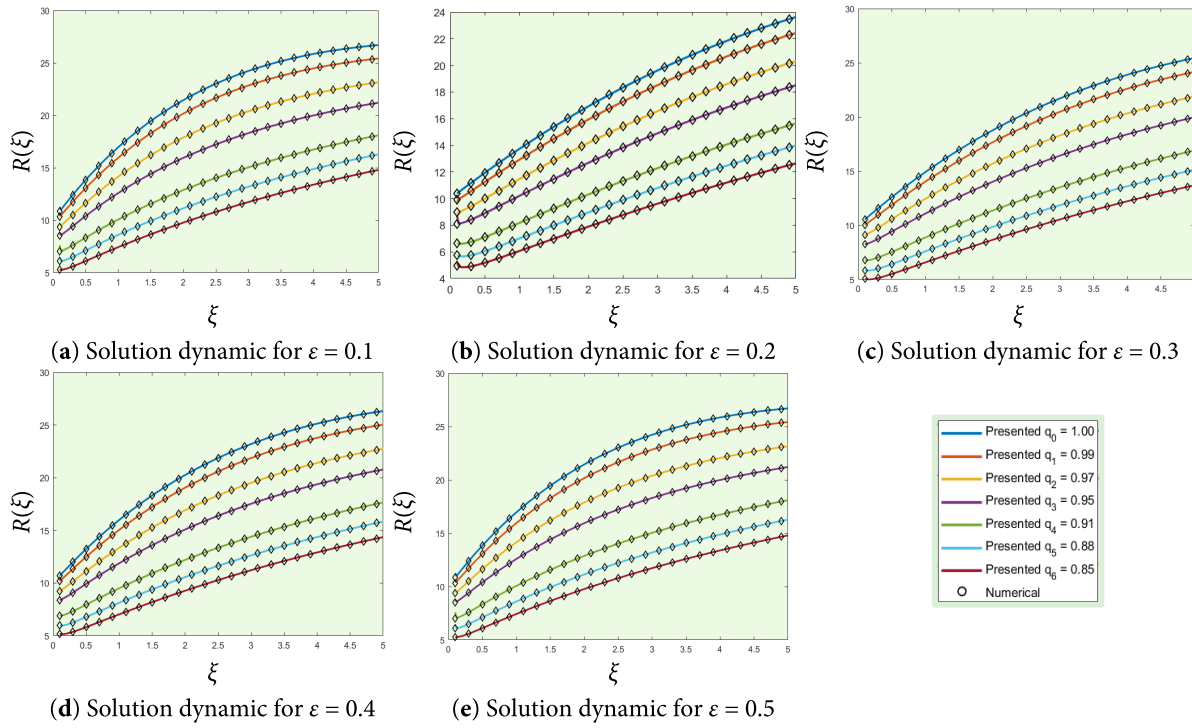


Figure 30: The numerical analysis of the nonlinear ARXNNs-LM framework for $R(\xi)$ state parameter of the nonlinear FCVP system for scenario-3.

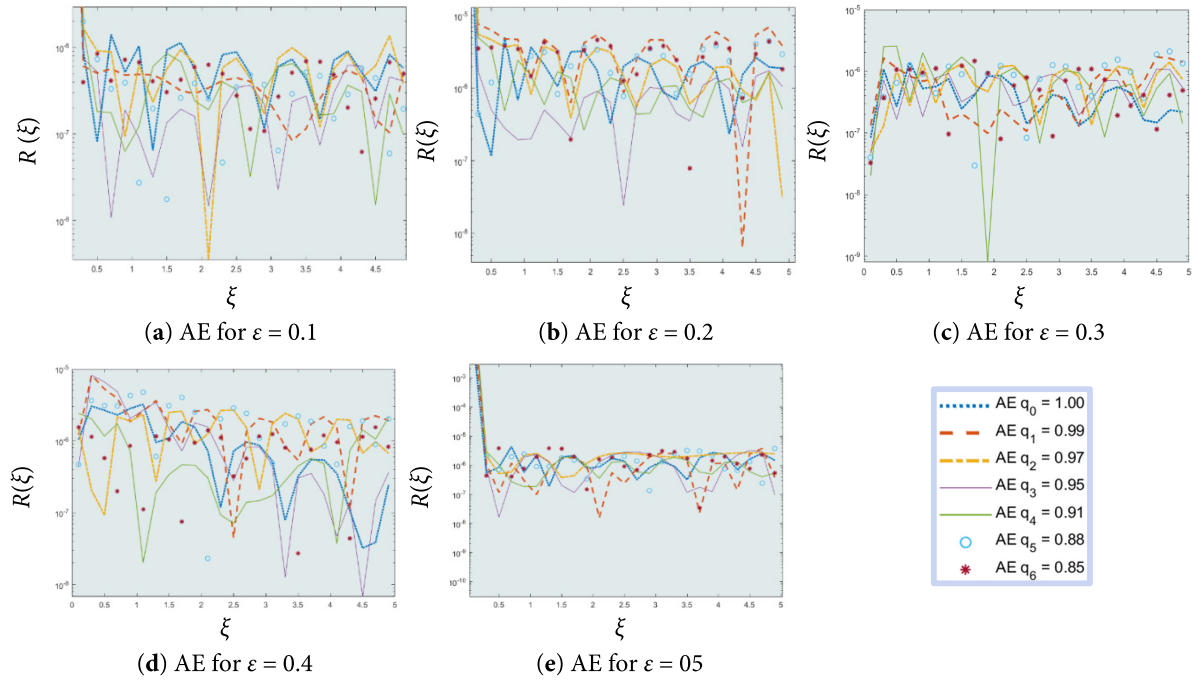


Figure 31: Comparison of AE for nonlinear ARXNNs-LM for $R(\xi)$ state parameter of the nonlinear FCVP system for scenario-3.

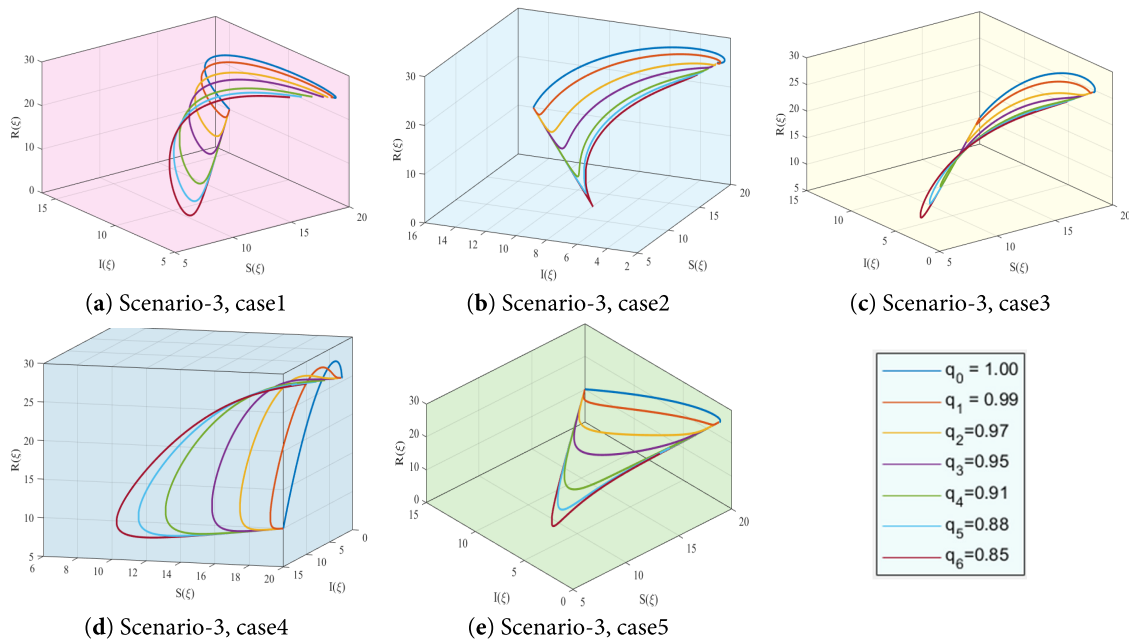


Figure 32: The three-dimensional analysis of the dynamics of the nonlinear FCVP model approximated with the nonlinear ARXNNs-LM scheme for scenario-3.

Table 5: Comparison analysis of different optimization algorithms on ANOVA test for scenario-1 case 1 of FCVP model.

Index	Method	Source	Analysis on Metrics				
			SS	df	MS	F	Prob > F
S_{ξ}	ARXNNs-LM	Groups	7.80E-10	2	3.90E-10	1.29	0.283
		Error	1.72E-08	57	3.02E-10		
		Total	1.80E-08	59			
	ARXNNs-BR	Groups	3.29E-08	2	1.65E-08	1.47	0.238
		Error	6.38E-07	57	1.12E-08		
		Total	6.71E-07	59			
	ARXNNs-SCG	Groups	0.014104	2	0.007052	1.16	0.321
		Error	0.346819	57	0.006085		
		Total	0.360922	59			
I_{ξ}	ARXNNs-LM	Groups	2.58E-10	2	1.29E-10	0.51	0.600
		Error	1.43E-08	57	2.51E-10		
		Total	1.46E-08	59			
	ARXNNs-BR	Groups	3.72E-08	2	1.86E-08	1.28	0.284
		Error	8.25E-07	57	1.45E-08		
		Total	8.62E-07	59			
	ARXNNs-SCG	Groups	0.000254	2	0.000127	0.05	0.947
		Error	0.132856	57	0.002331		
		Total	0.13311	59			

(Continued)

Table 5 (continued)

Index	Method	Source	Analysis on Metrics				
			SS	df	MS	F	Prob > F
R_ξ	ARXNNs-LM	Groups	5.21E-08	2	2.60E-08		
		Error	1.13E-06	57	1.98E-08	1.31	0.276
		Total	1.18E-06	59			
	ARXNNs-BR	Groups	3.73E-06	2	1.87E-06		
		Error	0.000166	57	2.91E-06	0.64	0.530
		Total	0.000169	59			
	ARXNNs-SCG	Groups	0.002395	2	0.001198		
		Error	0.070198	57	0.001232	0.97	0.384
		Total	0.072593	59			

Identical degrees of freedom are observed across all learning algorithms. Comparative analysis of MS values reveals that ARXNNs-LM outperforms other methods in scenario-1 case 1. Notably, the consistently high p -values (Prob > 0.05) and F-statistics indicate that the observed differences among group means are statistically insignificant. The ANOVA-based graphical visualization is presented in Fig. 33 for state parameters $S(\xi)$, $I(\xi)$, and $R(\xi)$ of the FCVP model, which provides a qualitative assessment of group-level differences of ARXNNs-LM, ARXNNs-BR, and ARXNNs-SCG methods. The marginal differences in mean absolute error (MAE) and overlapping errors suggest negligible intergroup variation and indicate comparable predictive accuracy.

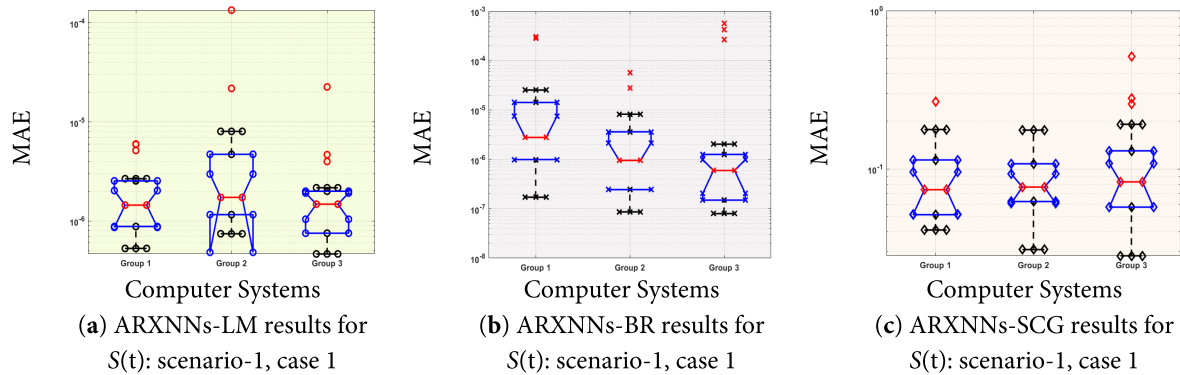


Figure 33: (Continued)

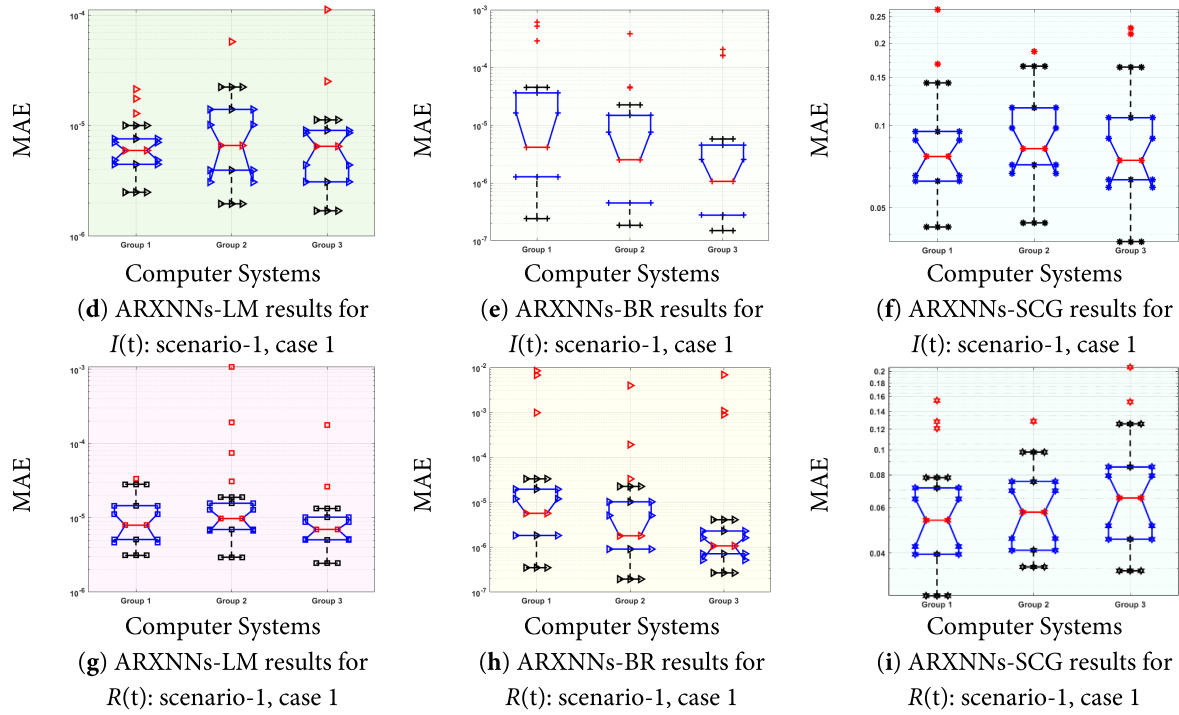


Figure 33: ANOVA-based assessment of accuracy metrics for the ARXNNs framework across multiple optimization algorithms in the FCVP model for scenario-1, case 1.

The MAE-based trajectories depicted in Fig. 34 provide a visual assessment of the proposed ARXNNs performance across 20 independent executions for three state variables, S , I , and R , under group-level configuration (G1, G2, G3) with LM, BR, and SCG algorithms. Distinct trajectories corresponding to individual variable and configuration pairs, with markers and colors identifying state variables and line styles differentiating experimental setups.

The observed patterns demonstrate consistent and stable performance of the proposed ARXNNs-LM technique under varying conditions, underscoring its predictive accuracy and generalization ability. The state-wise MAE-based performance assessment Heatmaps visualization for ARXNNs-LM, ARXNNs-BR, and ARXNNs-SCG frameworks in scenario-1, case 1, is depicted in Fig. 35. The consistently lower values of MAE are observed for the ARXNNs-LM neuroarchitecture across all compartments, aligned with the ANOVA findings, reinforcing the robustness and accuracy of the proposed framework. The jitter plots in Fig. 36 visualized the distribution of MAE values across the 20 independent runs for each experimental configuration of ARXNNs-LM, ARXNNs-BR, and ARXNNs-SCG frameworks in scenario-1, case 1.

The dense clustering and substantial overlap of lower MAE values across ARXNNs-LM configuration indicate limited inter-group variability, visually supporting the ANOVA findings, which report no statistically significant differences among group means. The MAE-based scatter matrix is presented in Fig. 37, which illustrates coherent pairwise relationships among MAE values corresponding to each state variable S , I , and R for ARXNNs-LM, ARXNNs-BR, and ARXNNs-SCG frameworks in scenario-1, case 1, indicating stable and correlated error dynamics. The patterns for the ARXNNs-LM technique indicate that lower prediction errors remain uniformly bound across variables, complementing the ANOVA analysis by confirming both distributional similarity and predictive consistency across heterogeneous conditions.

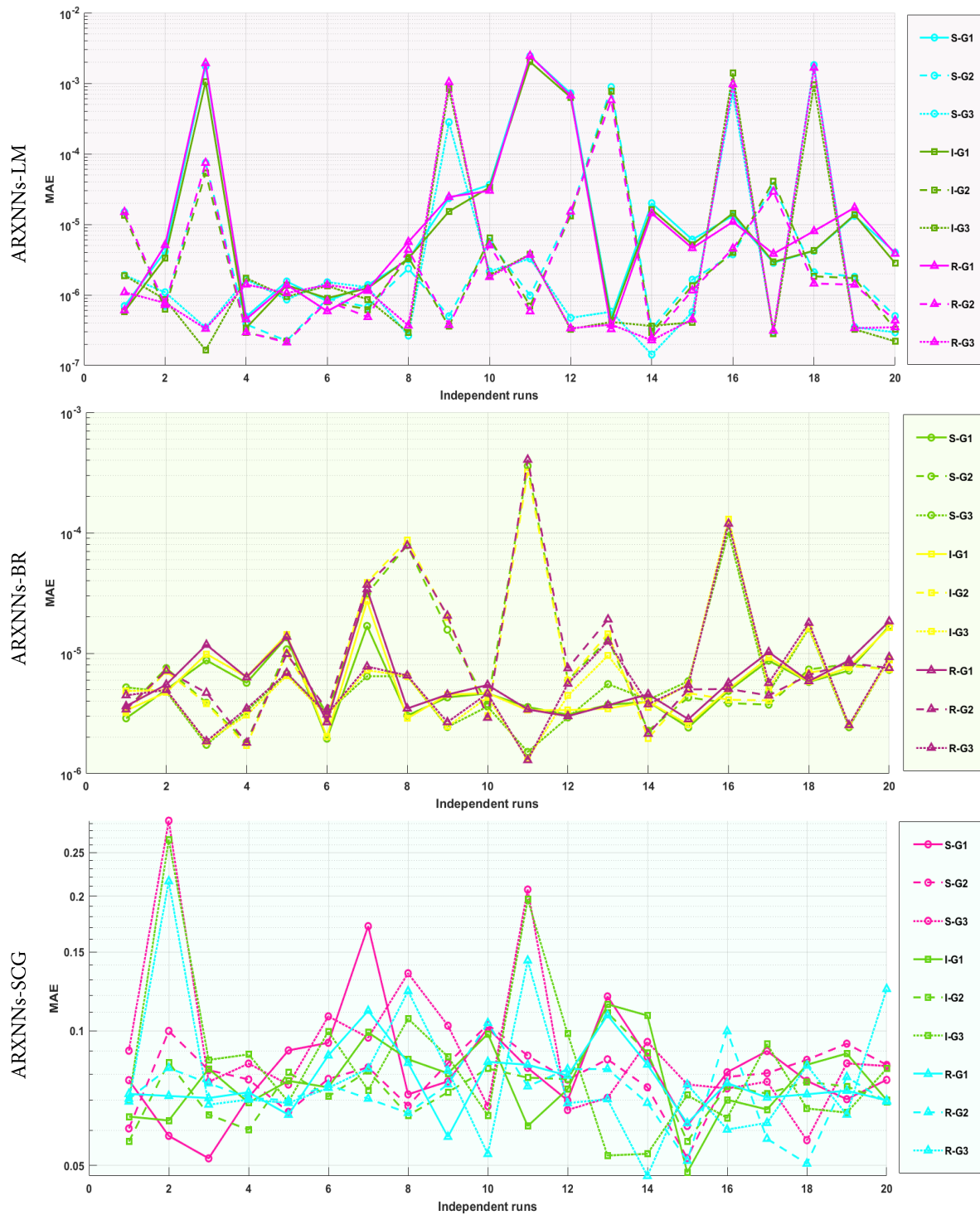


Figure 34: Comparison of MAE distribution over 20 independent runs for state variables S , I , and R across three experimental setups (G1, G2, G3) in scenario-1, case 1, visually supporting the ANOVA findings of statistically comparable performance.

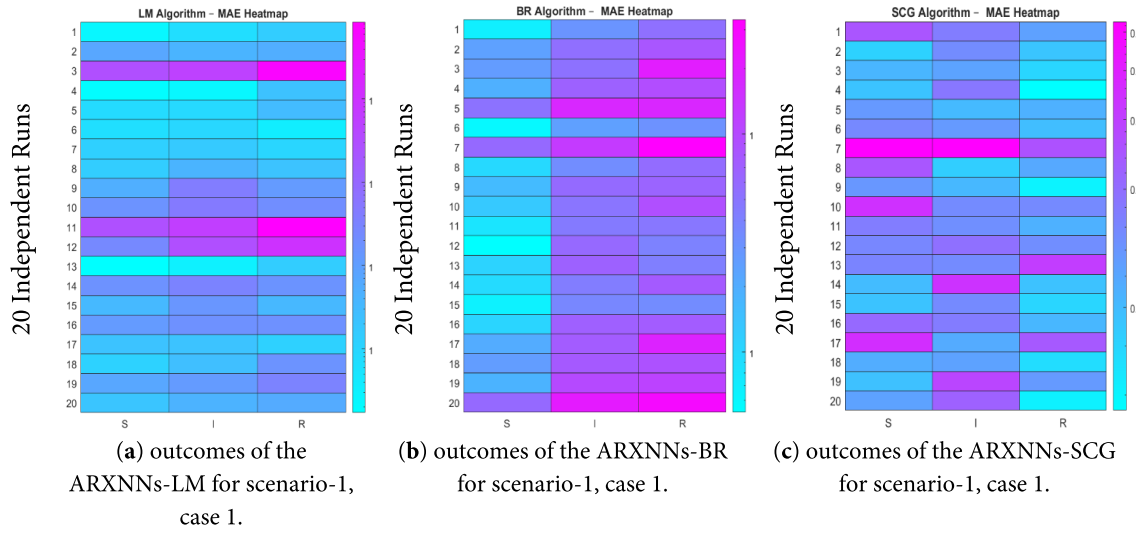


Figure 35: Heatmap comparison analysis of MAE-based performance assessment across S , I , and R state parameters for the ARXNNs trained with LM, BR, and SCG algorithms for scenario-1, case 1 color, and intensity represents relative error levels.

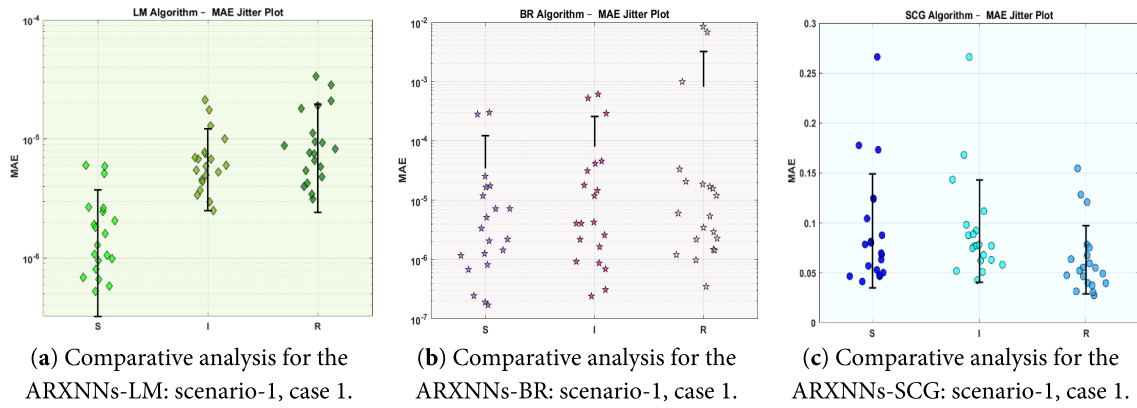


Figure 36: Comparative analysis of MAE-based evaluation via jitter plots across S , I , and R state parameters for the ARXNNs trained with LM, BR, and SCG algorithms for scenario-1, case 1.

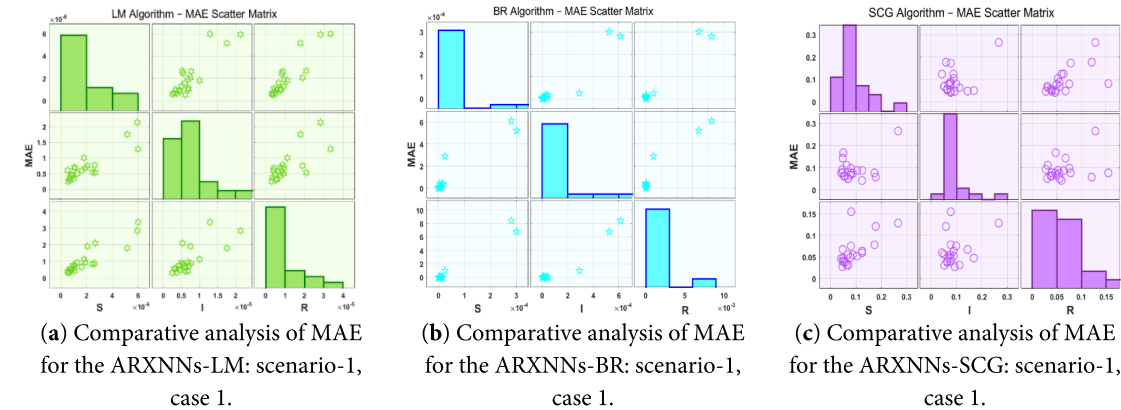


Figure 37: Comparative analysis of MAE-based evaluation via scatter matrix across S , I , and R state parameters for the ARXNNs trained with LM, BR, and SCG algorithms for scenario-1, case 1.

6 Conclusions

This study validates the effectiveness of the ARXNNs architecture optimized with the LM backpropagation in accurately capturing the nonlinear dynamics of the FCVP system across diverse scenarios and test cases, establishing its suitability for broad application in epidemiological cyber-threat analysis. The synthetic datasets generated through numerical procedure are employed to train the nonlinear ARXNNs-LM neuroarchitecture, enabling it to precisely capture and replicate the dynamic behavior of susceptible $S(\xi)$, infected $I(\xi)$, and recovered $R(\xi)$ computer states. The impact on the dynamics of the nonlinear FCVP model is observed to consolidate variations in λ (the rate of susceptibility), ρ (the removal rate from the network), and ε (the recovery rate of infected computers) while keeping the fixed external computer connection rate f_1 , f_2 , and f_3 for integer-order and fractional-order system scenarios. The ARXNNs-LM framework is trained using a synthetic dataset partitioned into training (78%), testing (11%), and validation (11%) subsets, ensuring optimal learning performance and minimal MSE. Exhaustive simulations exhibit that the ARXNNs-LM framework provide precise, stable, robust and convergent results that endorsed via MSE analysis with error magnitude of 10^{-9} to 10^{-13} , negligible deviation from the reference solution, with AE on the order of 10^{-4} to 10^{-10} , high fidelity cross and autocorrelation, and error distributions exhibiting maximum frequency at zero error, indicating high prediction accuracy. The precision of the presented hybrid ARXNNs-LM framework is further validated through the ANOVA assessment across multiple optimization algorithms applied to the FCVP system.

Limitations: The proposed ARXNNs-LM neuroarchitecture has some limitations. The employed framework is primarily trained using a synthetic dataset generated from the GL numerical solution of the FCVP model rather than real-world information due to the limited availability of labeled, high-resolution real-world datasets for computer virus propagation. The GL differentiation operator provides a controlled numerical analysis of computer virus propagation dynamics and memory-dependent cyber behaviors. This may limit the direct generalization, real-time implementation, and validation. The proposed model strongly emphasizes the range of fractional orders, but in realistic cyber scenarios, the memory effects vary dynamically, and computational complexity may increase in the critical networks. The ARXNNs-LM framework is employed in the heterogeneous networks to address the complex temporal dynamics of the FCVP system and show high-fidelity in prediction accuracy achieving an MSE value of 10^{-9} to 10^{-13} , these compartmental systems still face challenges in real-world scenarios. However, their effectiveness in the real-world cybersecurity environment may be limited when dealing with the broader real-world cyberattack scenarios that involve complex interactions, noisy traffic patterns, and diversity may affect the generalization ability and robustness of the proposed neuroarchitecture, but prediction accuracy can still be achieved by further fine-tuning of the parameters within the ARXNNs-LM framework, which enables improved learning accuracy.

Future directions: Future research should explore the application of the proposed methodology to diverse cybersecurity frameworks, particularly in sensor networks, node-based architectures, and other complex network topologies. Its extension to social communication systems could provide valuable insights into threat propagation, vulnerability assessment, and the development of robust mitigation strategies. In the future, we will also extend this hybrid AI-based predictive model to real-world computer virus spread data with the collaboration of the cybersecurity department of relevant organizations. A neural network trained on numerically simulated FCVP trajectories can serve as a better starting point and may provide better generalization when inferred with new data. Furthermore, these neural networks can be finetuned to appropriate real-world virus propagation data.

Acknowledgement: The authors would like to acknowledge the support of the National Science and Technology Council (NSTC), Taiwan.

Funding Statement: The authors would like to acknowledge the support of the National Science and Technology Council (NSTC), Taiwan, under grant no. 114-2221-E-224-019.

Author Contributions: Conceptualization, Muhammad Asif Zahoor Raja; writing—original draft, Kiran Asma; writing—review and edit, Muhammad Asif Zahoor Raja; validation, Muhammad Asif Zahoor Raja; formal analysis, Kiran Asma; supervision, Muhammad Asif Zahoor Raja; project administration, Muhammad Asif Zahoor Raja. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: The datasets generated and analyzed during the current study are available from the corresponding author on reasonable request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

Nomenclature

S	Susceptible computers
I	Infected computers
R	Recovered computers
λ	Infection rate of susceptible computers
ρ	Removal rate of computers from the network
ε	Recovery rate of infected computers
f_1, f_2 and f_3	External computers connecting rate to the network
ARXNNs	Autoregressive exogenous networks
LM	Levenberg-Marquardt method
MSE	Mean square errors
FCVP	Fractional computer virus propagation
GL	Grünwald–Letnikov
ANOVA	Analysis of variance
SSACA	Supervised stochastic approach for computational analysis

References

1. Almutairi N, Messaoudi M, Almalki FMK, Saber S. A deterministic and stochastic fractional-order model for computer virus propagation with Caputo-Fabrizio derivative: analysis, numerics, and dynamics. *Comput Model Eng Sci.* 2026;146(3):1–10. doi:10.32604/cmes.2026.076371.
2. Raza A, Shoaib Arif M, Rafiq M, Bibi M, Naveed M, Usman Iqbal M, et al. Numerical treatment for stochastic computer virus model. *Comput Model Eng Sci.* 2019;120(2):445–65. doi:10.32604/cmes.2019.06454.
3. Manohara G, Kumbinarasaiah S. Numerical solution of a modified epidemiological model of computer viruses by using Fibonacci wavelets. *J Anal.* 2024;32(1):529–54. doi:10.1007/s41478-023-00663-7.
4. Ayofe A, Oluwafemi O. Taxonomy, techniques and tools. In: *Computer viruses: from theory to applications*. Paris, France: Springer; 2006. p. 81–149. doi:10.1007/2-287-28099-5_4.
5. Joshi MJ, Patil BV. Computer virus: their problems & major attacks in real life. *J Adv Comput Sci Technol.* 2012;1(4):206–9. doi:10.14419/jacst.v1i4.318.
6. Kamal SU, Ali RJ, Alani HK, Abdulmajed ES. Survey and brief history on malware in network security case study: viruses, worms and bots. *ARPN J Eng Appl Sci.* 2016;11(1):683–98.
7. Haber M. Malware. In: *Attack vectors*. Berkeley, CA, USA: Apress; 2025. p. 83–92. doi:10.1007/979-8-8688-1709-0_4.

8. Pilania S, Kunwar RS. Zeus: in-depth malware analysis of banking trojan malware. In: *Advanced techniques and applications of cybersecurity and forensics*. Boca Raton, FL, USA: Chapman and Hall/CRC; 2024. p. 167–95. doi:10.1201/9781003386926-9.
9. Peng M, He X, Huang J, Dong T. Modeling computer virus and its dynamics. *Math Probl Eng*. 2013;2013(17):842614. doi:10.1155/2013/842614.
10. Gao K, Zhang L, Yao Y, Yang Y, Nian F. Effect of terminal boundary protection on the spread of computer viruses: modeling and simulation. *Front Inf Technol Electron Eng*. 2025;26(9):1637–48. doi:10.1631/fitee.2400236.
11. Zhu Q, Yang X, Ren J. Modeling and analysis of the spread of computer virus. *Commun Nonlinear Sci Numer Simul*. 2012;17(12):5117–24. doi:10.1016/j.cnsns.2012.05.030.
12. Ayaz A, Rehamn MAU, Rafiq M, Iqbal Z, Ahmed N, Akgül A, et al. Stochastic fractional order model for the computational analysis of computer virus. *Sci Rep*. 2025;15(1):33951. doi:10.1038/s41598-025-10330-5.
13. Iqbal Z, Rehman MA, Imran M, Ahmed N, Fatima U, Akgül A, et al. A finite difference scheme to solve a fractional order epidemic model of computer virus. *AIMS Math*. 2022;8(1):2337–59. doi:10.3934/math.2023121.
14. Tang W, Yang H, Pi J. Dynamics and control strategies for SLBRS model of computer viruses based on complex networks. *Int J Intell Syst*. 2024;2024(5):3943882. doi:10.1155/2024/3943882.
15. Wang J, Chang X, Zhong L. A SEIQRS computer virus propagation model and impulse control with two delays. *Math Methods App Sciences*. 2025;48(6):6851–65. doi:10.1002/mma.10721.
16. Zhang Z, Bi D. Bifurcation analysis in a delayed computer virus model with the effect of external computers. *Adv Differ Eq*. 2015;2015(1):317. doi:10.1186/s13662-015-0652-y.
17. Dong NP, Long HV, Giang NL. The fuzzy fractional SIQR model of computer virus propagation in wireless sensor network using Caputo Atangana-Baleanu derivatives. *Fuzzy Sets Syst*. 2022;429(3):28–59. doi:10.1016/j.fss.2021.04.012.
18. Liu J, Saeed T, Zeb A. Delay effect of an e-epidemic SEIRS malware propagation model with a generalized non-monotone incidence rate. *Results Phys*. 2022;39:105672. doi:10.1016/j.rinp.2022.105672.
19. del Rey AM, Vara RC, González SR. A computational propagation model for malware based on the SIR classic model. *Neurocomputing*. 2022;484:161–71. doi:10.1016/j.neucom.2021.08.149.
20. Asma K, Raja MA, Chang CY. Expedition of deterministic numerical solvers for computer virus spread: explicit Runge-Kutta and backward differential methods. *J Innov Technol*. 2025;7(1):33–49. doi:10.29424/JIT.202503_7(1).0004.
21. Wu G, Zhang Y, Zhang H, Yu S, Yu S, Shen S. SIHQR model with time delay for worm spread analysis in IIoT-enabled PLC network. *Ad Hoc Netw*. 2024;160(7):103504. doi:10.1016/j.adhoc.2024.103504.
22. Asma K, Raja MAZ, Chang CY, Ali Asif Raja MJ, Shoaib M, Shu CM. A machine learning approach using nonlinear ARX neural networks with Bayesian regularization for epidemic malware dynamics in critical network infrastructures. *Int J Inf Secur*. 2025;24(5):191. doi:10.1007/s10207-025-01104-1.
23. Yang F, Zhang Z, Zeb A. Hopf bifurcation of a VEIQS worm propagation model in mobile networks with two delays. *Alex Eng J*. 2021;60(6):5105–14. doi:10.1016/j.aej.2021.03.055.
24. Frutos-Bernal E, Rodríguez-Rosa M, Anciones-Polo M, Martín-del Rey Á. Analyzing malware propagation on wireless sensor networks: a new approach using queueing theory and HJ-biplot with a SIRS model. *Mathematics*. 2024;12(1):135. doi:10.3390/math12010135.
25. Asma K, Raja MAZ, Chang CY, Ali Asif Raja MJ, Shoaib M. Machine learning-driven exogenous neural architecture for nonlinear fractional cybersecurity awareness model in mobile malware propagation. *Chaos Solitons Fractals*. 2025;192(2):115948. doi:10.1016/j.chaos.2024.115948.
26. Wu G, Xie L, Zhang H, Wang J, Shen S, Yu S. STSIR: an individual-group game-based model for disclosing virus spread in Social Internet of Things. *J Netw Comput Appl*. 2023;214(3):103608. doi:10.1016/j.jnca.2023.103608.
27. Asma K, Raja MAZ, Chang CY, Ali Asif Raja MJ, Shu CM, Shoaib M. Machine learning knowledge driven investigation for immunity infused fractional industrial virus transmission in SCADA systems. *J Ind Inf Integr*. 2025;48(3):100940. doi:10.1016/j.jii.2025.100940.

28. Yang L, Song Q, Liu Y. Dynamics analysis of a new fractional-order SVEIR-KS model for computer virus propagation: stability and Hopf bifurcation. *Neurocomputing*. 2024;598(24):128075. doi:10.1016/j.neucom.2024.128075.
29. He J, Li Y, Tang J, Wang H, Yang G, Li T, et al. An immune-knowledge-driven SCADA-based industrial virus propagation model. *IEEE Internet Things J*. 2024;11(18):29956–70. doi:10.1109/JIOT.2024.3407768.
30. Ying X, Pan M, Chen X, Zhou Y, Liu J, Li D, et al. Research on virus propagation network intrusion detection based on graph neural network. *Mathematics*. 2024;12(10):1534. doi:10.3390/math12101534.
31. Yu X, Zhang Z. A delayed malware propagation model for cloud computing security. *Fractals*. 2026;34(4):2540064. doi:10.1142/s0218348x2540064x.
32. Shen S, Wei S, Gao XZ. SIQR: stochastic games-assisted disclosure of malware propagation in industrial Internet of Things. *Ad Hoc Netw*. 2026;186(1):104191. doi:10.1016/j.adhoc.2026.104191.
33. Ghosh S, Kumar VA. Internet malware propagation: dynamics and control through SEIRV epidemic model with relapse and intervention. *arXiv:2603.03712*. 2026. doi:10.48550/arXiv.2603.03712.
34. Raza MM, Umair M, Choudhry IA, Qasim M, Naseem MT, Asghar MN, et al. Malware detection and AI integration: a systematic review of current trends and future directions. *Comput Model Eng Sci*. 2026;146(3):1–10. doi:10.32604/cmesci.2025.074164.
35. Devi M, Nandal P, Sehrawat H. Federated learning-enabled lightweight intrusion detection system for wireless sensor networks: a cybersecurity approach against DDoS attacks in smart city environments. *Intell Syst Appl*. 2025;27(5):200553. doi:10.1016/j.iswa.2025.200553.
36. Devi M, Nandal P, Sehrawat H. Cyberattack detection using a golden pelican search algorithm optimized three-tier deep learning approach. *Wirel Netw*. 2026;32(2):815–37. doi:10.1007/s11276-025-04083-2.
37. Arqub OA, Maayah B. Numerical solutions of integrodifferential equations of Fredholm operator type in the sense of the Atangana-Baleanu fractional operator. *Chaos Solitons Fractals*. 2018;117:117–24. doi:10.1016/j.chaos.2018.10.007.
38. Kamil Jassim H, Abed Shareef Hussain M. On approximate solutions for fractional system of differential equations with Caputo-Fabrizio fractional operator. *J Math Computer Sci*. 2020;23(2):58–66. doi:10.22436/jmcs.023.01.06.
39. Garrappa R. Grünwald-Letnikov operators for fractional relaxation in Havriliak-Negami models. *Commun Nonlinear Sci Numer Simul*. 2016;38(5):178–91. doi:10.1016/j.cnsns.2016.02.015.
40. Luchko Y. Fractional differential equations with the general fractional derivatives of arbitrary order in the Riemann-Liouville sense. *Mathematics*. 2022;10(6):849. doi:10.3390/math10060849.
41. Almeida R. A Caputo fractional derivative of a function with respect to another function. *Commun Nonlinear Sci Numer Simul*. 2017;44(5):460–81. doi:10.1016/j.cnsns.2016.09.006.
42. Butzer PL, Kilbas AA, Trujillo JJ. Fractional calculus in the Mellin setting and Hadamard-type fractional integrals. *J Math Anal Appl*. 2002;269(1):1–27. doi:10.1016/S0022-247X(02)00001-X.
43. Sanchez-Ortiz J, Lopez-Cresencio OU, Arciga-Alejandro MP, Ariza-Hernandez FJ. A random Riemann-Liouville integral operator. *Mathematics*. 2025;13(15):2524. doi:10.3390/math13152524.
44. AlBaidani MM, Ganie AH, Khan A, Aljuaydi F. An approximate analytical view of fractional physical models in the frame of the Caputo operator. *Fractal Fract*. 2025;9(4):199. doi:10.3390/fractalfract9040199.
45. Agrawal PN, Baxhaku B. Exponential sampling type neural network Kantorovich operators based on Hadamard fractional integral. *Fract Calc Appl Anal*. 2025;28(4):1887–922. doi:10.1007/s13540-025-00418-0.
46. Jornet M. Fractional Bateman equations in the Atangana-Baleanu sense. *Phys Scr*. 2025;100(2):025301. doi:10.1088/1402-4896/ada217.
47. ul Haq I, Ali N, Ahmad H, Sabra R, Albalwi MD, Ahmad I. Mathematical analysis of a coronavirus model with Caputo, Caputo-Fabrizio–Caputo fractional and Atangana-Baleanu–Caputo differential operators. *Int J Biomath*. 2025;18(1):2350085. doi:10.1142/s1793524523500857.
48. Gomolka Z, Zeslowska E, Olbrot L, Komsa M, Ćwiakała A. Fractional derivative in LSTM networks: adaptive neuron shape modeling with the Grünwald-Letnikov method. *Appl Sci*. 2025;15(24):13046. doi:10.3390/app152413046.

49. Gorenflo R, Abdel-Rehim EA. Convergence of the Grünwald-Letnikov scheme for time-fractional diffusion. *J Comput Appl Math.* 2007;205(2):871–81. doi:10.1016/j.cam.2005.12.043.
50. Ali Khan T, Chaudhary NI, Khan ZA, Mehmood K, Hsu CC, Raja MAZ. Design of Runge-Kutta optimization for fractional input nonlinear autoregressive exogenous system identification with key-term separation. *Chaos Solitons Fractals.* 2024;182(1):114723. doi:10.1016/j.chaos.2024.114723.
51. Ali Syed F, Fang KT, Kiani AK, Shih DH, Shoaib M, Zahoor Raja MA. Novel intelligent supervised neuro-structures for nonlinear financial crime differential systems. *Mod Phys Lett B.* 2025;39(1):2450399. doi:10.1142/s0217984924503998.