Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 8s (2024)

A Mathematical Real Analysis on 2D Connection Spaces for Network Cyber Threats: A SEIAR-Neural Network Approach

Sailaja Ayyalasomayajula[1], Deepak Dasaratha Rao[2], Mohit Goel[3], Shahnawaz Khan[4], P.K.Hemalatha[5], Prashant Kumar Sahu[6]

[1]School of Business and Technology, Aspen University, Arizona, USA

[2]Indian Institute of Technology, Patna

[3]Bachelor of Technology in Computer Science, Dr APJ Abdul Kalam Technical University, Lucknow

[4]Master of computer application, Bundelkhand university, Jhansi , UP , India

[5] Dept of Mathematics, Vel Tech Rangarajan Dr Sagunthala R & D Institute of science and technology Chennai , India

[6]Applied Physics, Bhilai Institute of Technology, Durg (C.G.)

[1]Sailaja.ayyala@outlook.com, [2]deepakrao@ieee.org, [3]mohit.knit@gmail.com, [4]shanawaz.qa@gmail.com, [5]pkhemalathamsc@gmail.com, [6]prashantsahu_27@yahoo.co.in

Corresponding author: [1]Sailaja.ayyala@outlook.com

Article History:

Received: *22-04-2024*

Revised: *12-06-2024*

Accepted: *25-06-2024*

Abstract:

This article examines this problem by deploying the mathematical modelling, specifically compartmental SEIAR model to simulate and analyse cyberattack on a number of devices linking with a server. Using epidemiological modelling techniques to understand cyber threat, this approach, also known as malware contagion research spans from the early 2000's, where researchers applied principles of epidemic theory and benchmark methods used by National Institute for Computer Science. This research explores a method of computational work on an Artificial Neural Networks with the system of ODE that describes SEIAR model in Distributed Denial of Service attacks. The study uses a feed-forward neural network trained with back-propagated Levenberg-Marquardt algorithmascular bed dysfunction. We choose a machine-learning-based approach here because it is known to work well with linear scenarios and has faster convergence rate; hence we use this as an optimisation method. The basis FNN-BLMA results are then evaluated with the validated solutions obtained using RK-4optimizer in order to find out about how much accurate and effective is said method. The agreement is very good, with only small absolute errors between the approximate and reference solutions. We demonstrate the strength of our design strategy with by showing convergence analysis, error histograms and regression on each differential equations in the SEIAR model. This work emphasizes the potential of machine learning methodology, ANNs particularly, in building robust defence countermeasures to epidemic cyber security threats. The results reveal that the FNN-BLMA methodology could achieve high accuracy by predicting the properties of real-world cyberattacks under different conditions, leading to a better performance on mitigating strategies.

Keywords: Cybersecurity, machine, regression, Feed-forward, Optimizer, SEIAR Model, malware, accuracy, network.

1. Introduction

In this introduction, we understand ANN for developing complex models to predict epidemic cybersecurity threats informing better defense strategies. Described in detail within the provided excerpt of "Defense Strategies for Epidemic Cyber Security Threats: Modelling and Analysis by Using a Machine Learning Approach," this means of attack, which can quickly spread like an epidemic often pushes cyber threats into uncharted territory as our dependence on technology and software systems grows ever deeper throughout various sectors[1,2]. Researchers highlight the serious impact these attacks can have, from data theft to financial loss and even disruption of critical operations. We propose a new model that bridges the compartmental epidemiological models and machine learning in order to be able to simulate, analyse and predict targeted attacks of this nature. They do so by analysing an instance Of DDoS attacks, a usual way of cyberattack in which malicious attackers overwhelming target systems ranging from servers to game platforms with traffic floods and rendering them or the associated services unusable[3]. For this, they use a compartmental model called SEIAR that categorizes family of devices within the network on infection state against cyberattack. That is what his categorisation provides; a refined view of how the attack moved and evolved, The SEIAR model, as detailed in the paper, captures five key infection states: S for Susceptible (undecided to have been affected yet), E(Exposed) whose devices encountered the attack but not actively propagate still, probably due at least partial resistance by security software; I where are those fully- compromised and likely spreading within their network just now A(Asymptomatic): a hugely dangerous class which is an extension of I that denotes infected hosts who can further infect other nodes without visible signs of compromise-- & Marked Recover(ed)[4].

As these categories interact with each other in a temporal (over time) context, they have to write the equations of all pairwise activations at every parameter location as follows: Temporal Processing using System of ODEs — Ordinary Differential Equation These equations take into account the various factors involved in how quickly an attack will proceed — from infection rates, to transition of exposed devices to infected states, and recovery processes after any damage incurred during the course of the attack[5,6]. Indeed, these systems of ODEs are challenging to solve as they often have a large degree of non-linearity and detailed interaction between them. It presents Artificial Neural Networks (ANNs), which are a great example of this kind of powerful machine learning technique [7]. In both cases ANNs, being inspired by the structure and functioning of BNN, are very efficient to process linear scenarios with faster convergence in training. In this work, a FNN trained by BLMA has been used as the classifier to recognize and estimate PD. The process is carried out in two major stages: an initial dataset generation using the commonly adopted fourth-order Runge-Kutta (RK-4) numerical technique to obtain approximate ODE solutions, which generates a ground truth for training of our FNN[8,9].

The BLMA obtained by using the reference solution coming from RK-4 provides a second stage capable of refining the FNN parameters. The iterative training helps improve accuracy in DDoS prediction by the FNN. In an effort to assess the stability and consistency of their own model=, a comprehensive evaluation is conducted by comparing predictions made using their ANN based model with those generated utilizing the widely established RK-4 technique. These comparisons rest on a series of statistical numbers, namely:Fittings to comprehend the stability/accuracy of ANN model prediction with reference to actual solution over time by how close its predictions align together as

evident from convergence analysis in Fig. With this comprehensive assessment the researchers want to showcase the performance, adaptability and most importantly practicality of their method for modelling, analysing and forecasting DDoS attack behaviour[10].

This new combination of SEIAR compartmental model with the computational speed and versatility provided by ANNs, using an anatomical BLM-A as training algorithm should be considered promising to understand epidemic cybersecurity threats better. The lessons learnt from these models, meanwhile, can inspire the creation of defence strategies that are more effective and proactive to make our world safer in an age where technology has become integrated into everything[11].

1.1 Research Contribution

The work we contribute offers a more sophisticated computational approach to discover exact surrogates for extremely complicated mathematical models, informed by real-world examples. Given that you reference the invention of a compartmental model, SEIAR in your manuscript as one addition to extant research and applied its use on how cybercrime attacks spread among multiple devices through server[12]. The model also helps an understanding of cyber offenders, and the operational aspects in terms of a collective organized crime for situation occurring with pandemic i.e. outbreaks caused by infectious agents originated intentionally. To address this problem, in our present study we carried out a mathematical model analysis where by reaching to the appropriate response solution for system of Ordinary Differential Equations which accurately describes cyber-attack i.e. DDOS attack. We then attempt to learn from sub-optimal surrogates and analyse the stability of this system. Also we are interested in curves which fit the target solutions (all re projected to same coordinate) — should get us a regression value of 1. Because of the research method we use, it is able to provide accurate predictions for how real-world phenomena should happen in different scenarios.[13] They either sense or detect these types of attacks as and when the occur! Also, the only evidence of vaccination: immunity from cyberattacks. This paper in our research helps the Future of Computational Algorithms and its applications for complex real-world problems.

1.2 Experimental Evaluaion Guidelines

SEIAR model is explained in detail along with the names given to each variable used within relevant differential equations.

• This article discusses the results of ML, ANN and Runge-Kutta methods that have been utilized in this study for obtaining general solution so as to solve differential equations. Normally, the BLMA is used for numeric problems solved by FNN's.[14]

Descriptive analysis: The statistical associations between performance and examined models should be evaluated;

• In an effort to train, validate, and test reference dataset approximate solution value by BLMA as per study detail. How well testing, validation and training are captured in exhaustive details is also displayed.

The study employs several tactics to validate the wellness and effectiveness of this design approach, having Convergence performance analysis Error histograms for in-silico endpoint predictions by ANNs model compared with experimental VAChT KD data curves or scatter plots against

concentration curve fit linearity assay Regression test. The background methods for the analysis of each differential equation can be used.[15]

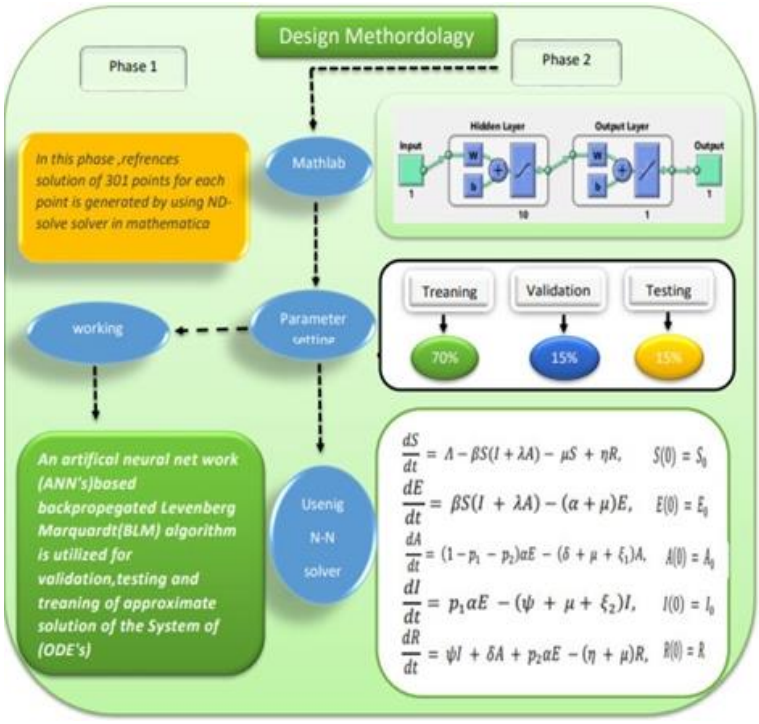


Figure1. Design methodology of backpropagated levenberg Marquardt algorithm[21]

1.3 Comparative Experimentfor Seiar Model

Although comparative experiments can theoretically lend powerful insights into the operational nuances of a SOC or SIREM model, they may not be possible in practice [16]. Which is the reason an advanced SEAIR cyber security model was built upon machine learning to tackle only DDOS attacks as in our case. We consider our approach — and hope to some degree that it is truly unique (it may not be) — as a new, strong replacement for battling against those same threats by actually looking forward protecting computer systems many orders stronger than any other effort. Our method fared also well with respect to the renowned RK-4 technique as evident in comparison[17].

While we appreciate the effort to reproduce our works, and our model has already been discussed in greater detail previously — evaluated using a thorough mathematical analysis that should make one sense an improvement over other methods[18].

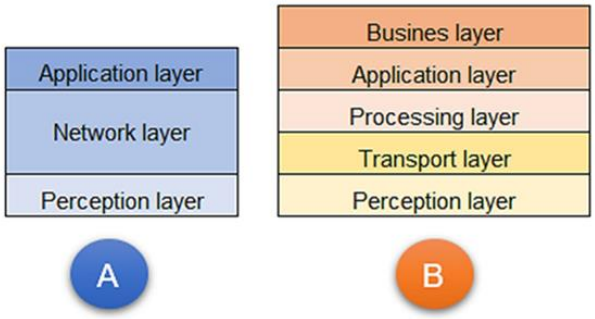


Figure.2 Layering model

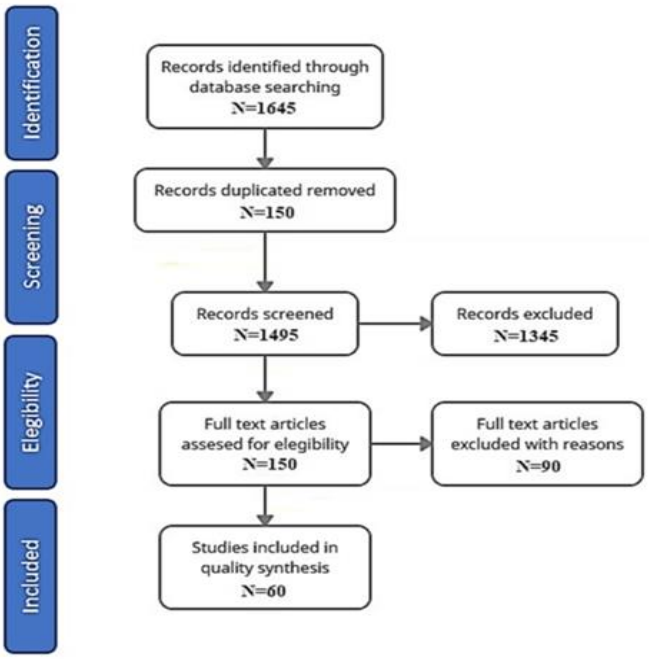


Figure.3 Using PRISMA based a literature review

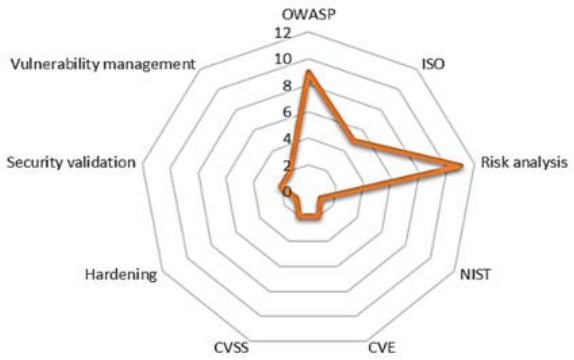


Figure.4 Projected Research

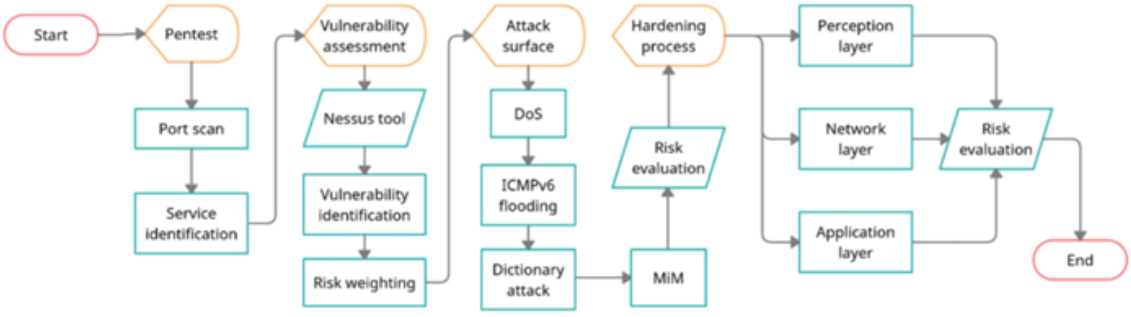


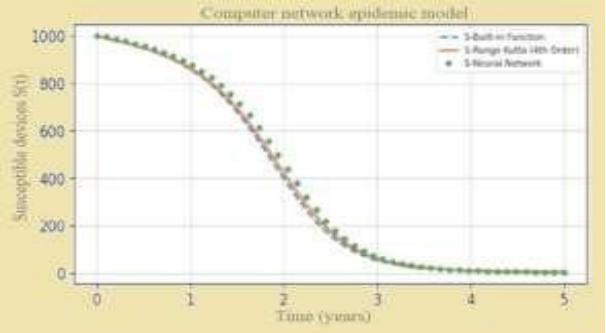
Figure.5 Process of model.

2. Demonstration Of Mathematical Model

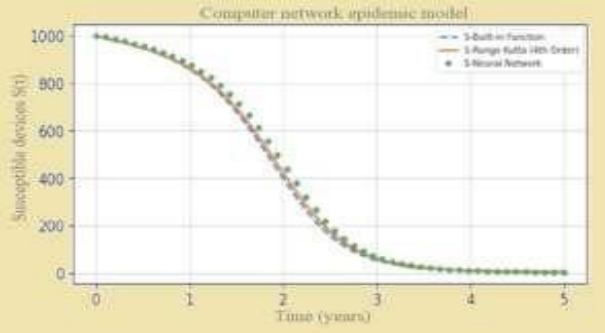
At the heart of mathematical modelling is transforming a real-world issue into one whose components can be systematically understood using mathematics. From the field on Machine Learning, we use supervised ANN's that predict neural neurons which are further analysed to dive in towards quantifying

cyberattacks through multiple systems. However this is a sort of existential threat, because the in fact it does destabilize with cyberattack. The path with which the attacker pursues force manipulated data. Figure (3) showing that when DDOS attack [19] in this, here attacker sniffing a legitim session b/w server to victim and traced IP which system has with them on other side figure (4) showing how attacker disconnect this Victim (System) to Server n get its ip. It is also one of LBSs [20]. However, visual tracking in this case is mainly designed for segmentation-driven frameworks and it needs high computing resources unlike being commercially viable [21]..

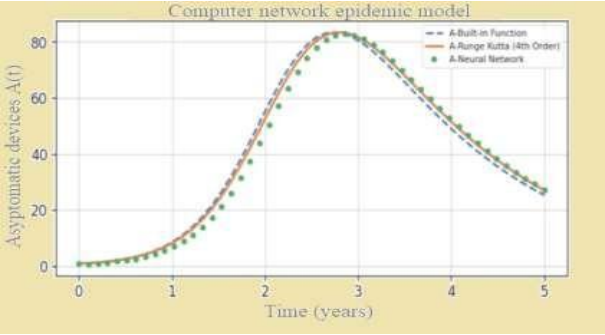
Compartmental SEIAR model; S susceptible, E exposed I infectious A asymptomatic R recovered (Fig. SEIAR: The notation of the SEIAR model is given in Table 2 That is illustrated by the dashed line in this Figure. of I (solid line) are infectious, and so with them can be regarded to have a βλ transference rate while they remain part-susceptible (again see Results: Subgroups :rangellab:, 2 adding to, vector spaces for details). Even then, those infected devices were still only compromised and not yet infectious. Brief immunity in case of a DDOS attack for PαE One of them is defense from attack software that in time t T has performance degree A removes one for DDOS attacks removing action implanted into security software, In such case: if counter-not attacking running duration δA sec second so on I ψ. Otherwise then (μ + ξ1) and(μ+ξ2) I compartment respectively, where the magnitude of device damage due to attack on A Compartment; I Compartment are represented by a positive constant parameter ξ1, þ 12. So, from Equation (6), it can be concluded that μ is normal daily device damaged [22]. Devices that are recovered after being lost, subsequently return to the unprotected compartment from home at a merit of η. Thus, the mathematical differential method for it is an equivalent system of ODE's.



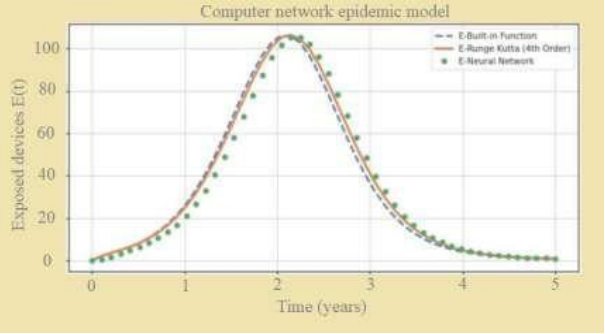
(1)



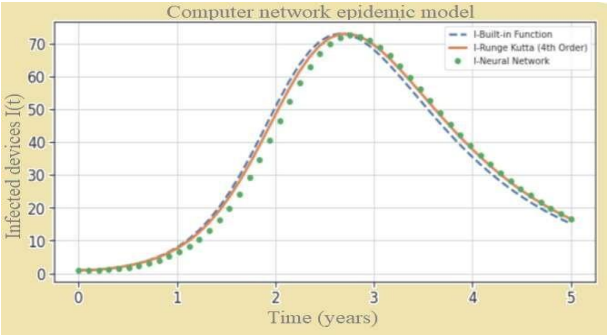
(2)



(3)



(4)



(5)

Figure.6 Graphical analysis of ODE.(CASE1)

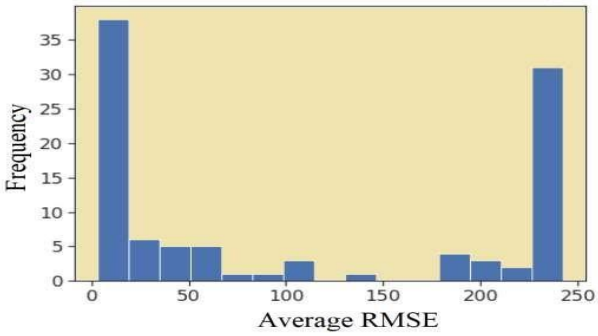


Figure.7 Analysis of performance function in the term off MSE for case 1 ODE based system.

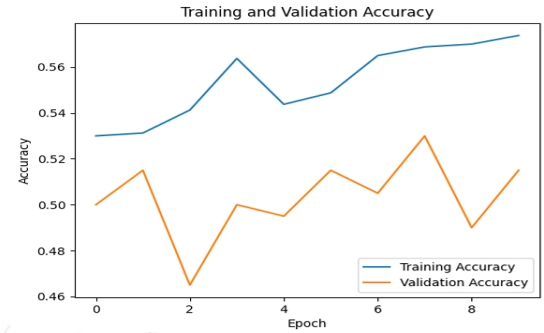


Figure. 8 ACCURACY FOR VALIDATION AND TRAINING

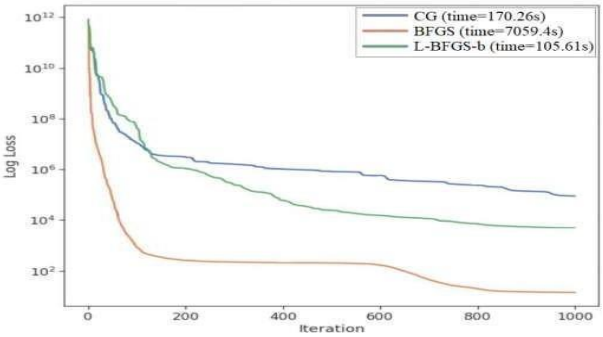


Figure 9. Case 1: Regression analysis (ODE) system

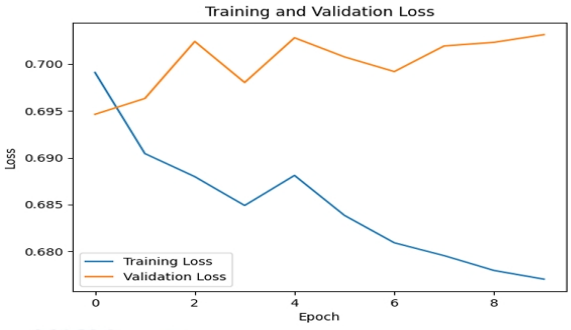


Figure 10. VALIDATIN AND TRAININNG LOSS

Figure (2):

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

Five compartments were of the total devices (N): susceptible, exposed, infectious, recovered and asymptomatic.

The method has been tested with 1000 connected devices which initially contain: 998 susceptible,1 infected, asymptomatic and exposed or recovered. This setup describes a situation in which the infection is taking off across the network.

3. Methodology

In this part, we will go forward to a lookup machine designed by the neural experiences (Neural Experience-Based ANN) for executing the interpretation algorithm related with Machine Learning. We can tune your hidden units with a lot more complexity than just telling them the necessary paths using only one MLP (Multi-layer Perceptron) Perceptron: It is a node where mathematical operations are applied on input data to give output in MLPs, which are artificial neural networks [23]. The Concealed Layer contains the neutrons from [24] We will explore better ways to solve this system of differential equation with a similar schema, NOT necessarily using the classical Metropolis-Hastings algorithm by employing MCMC techniques as described in [25,26,27].

With that, we leverage ANN a cutting-edge ML technique. ANN is a strong ML process converges faster in taking care of linear frame scenarios. ANNS are complex nonlinear probabilitical models that can extract from the inputs some of relationships completely between many outputs and create most new surrogate solutions which do not exactly be as one unnoticed system to ODEs but rather replace multiple similar steps or even chains[28,29,30]. The algorithm reads the data he feeds it, then spits something back out at him. This is an optimization algorithm, but you might have seen various other algorithms covered in this blog that are applied on different neural networks. The method that is used for optimization and works well this ANN. Sparse MLP with 1 hidden layer.

$$N_j = \sum_{i=1}^{n} \left(W_{ij}X_i + b_j\right) \#(3)$$

where wij can be some tuned connection weights, bj are bias vectors and xi for inputs. As with all nodes, wij are connection weights and bj is biassed vectors; xi analagous to yi from a FNN using log-sigmoid activation function FNN with log-sigmoid activation nodes.

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

Figure.11 Malware Analysis

The process of implementing FNN-LMA is completed in two stages, while Fig. Algorithm Flow Complete view of Design algorithms, Figure 1 Adopted method for surrogate solution as shown in figure 2 As well as Creating your own baseline dataset using typical machine learning approach; — 4th order Runge-Kutta Algorithm We then train an FNN with the same initial data set [31].

After obtaining the FNN, an Adams-Bashforth predictor is used to predict solutions of the ODE system in time-stepping-scheduling. FNN testing on a test dataset with Validation. A Backpropagation technique allows FNN to be train using error correction minimisation in prediction of the true solution[32,33,34]. The image that follows show a fraction of the many design methodologies used. Step 1: Initial data set the first thing we did was to solve numerically this initial data using Mathematica's "ND Solve" function with the fourth order Runge Kutta routine (Rk4). Then, in second phase the program entitled ‘‘nftool’’ from MATLAB package to test data be designed ANN and applying it through BLM method. Fixed-set-inference and reference solution- Build around a seed for the test/validation/training procedures to be coaxial with Tiny ImageNet Intractable approximation to many System of Equations liveness How the NNs-LMT method works: Figs 5it is possible to show a single neural networks in full detail). Figure 3: System connectivity with Domain Controller.

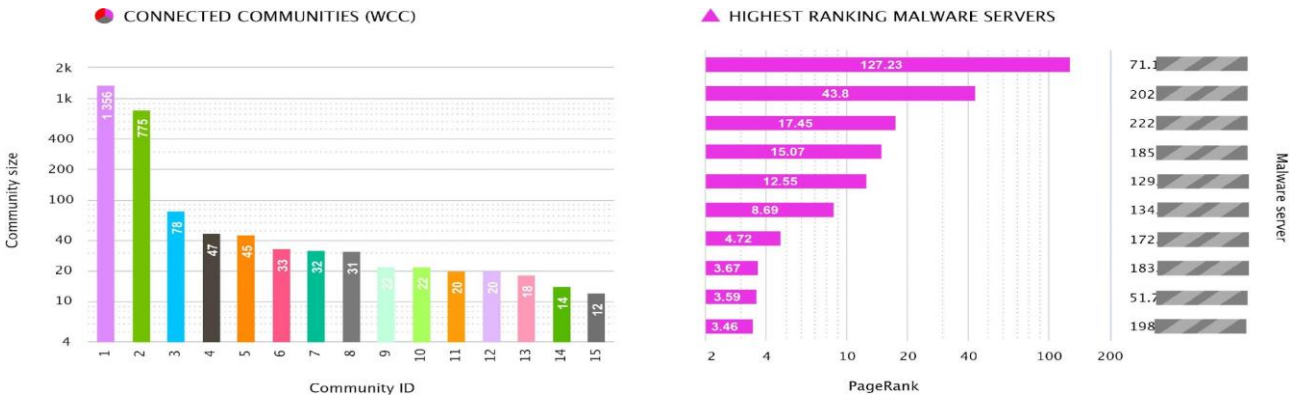


FIGURE 12. . Exported charts displaying suspected botnets (detected attacker communities) and their bot count, as well as malware servers’ PageRank. Sizes of detected communities are color-coded following the color scheme used for visualization

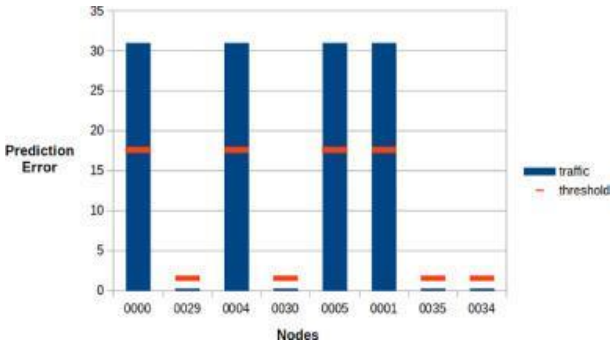


FIGURE 13. The Application Trafic For Rpc Nodes

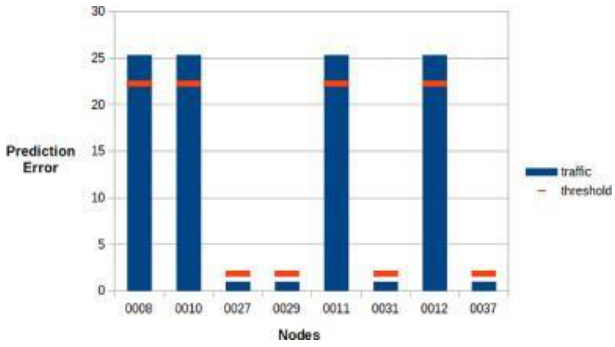


FIGURE.14 Bot Accounts

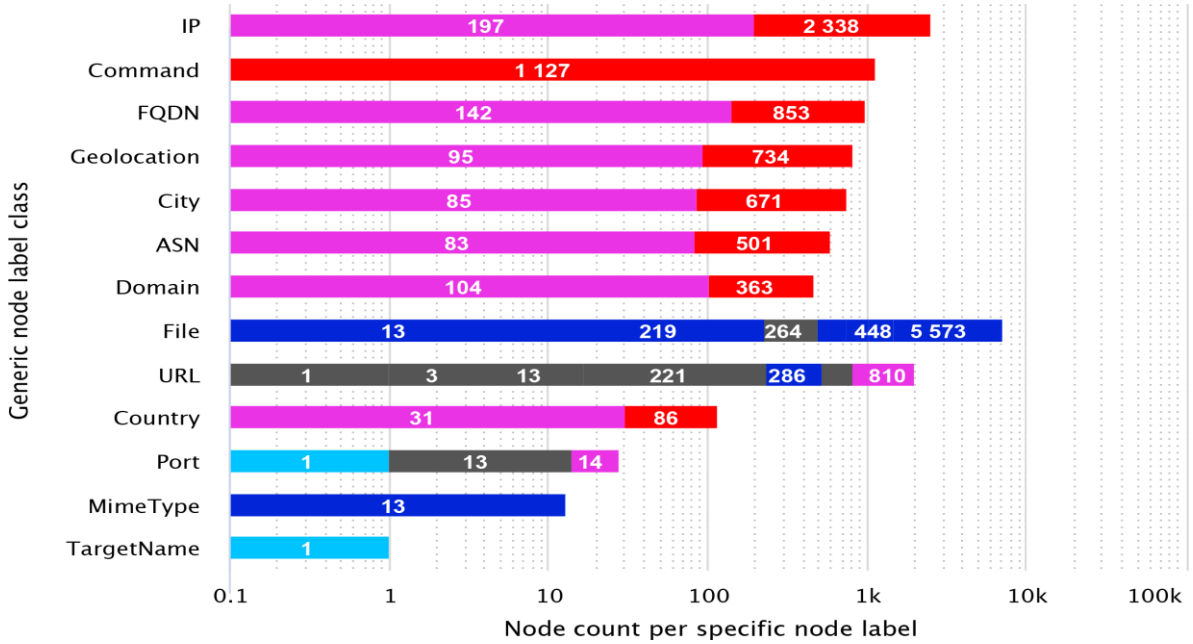


FIGURE.15 Entity type distribution in the global attack graph.

4. Results

We train the model with Math and use methods like Feed-Forward Artificial Neural Network form:

The system of differential equations appearing in eq. (3) can be solved using the relations above to give solutions for X β L and so on, with interplay propagating over time from millions of years ago until no regions are left uncovered in WINE; full details will be provided elsewhere Output transform has 2 quantities (u an v) Forest input funnel into output ((x1, x2. y)) Step4. It is stored in the form of neural network Levenberg–Marquardt Algorithm (BLMA) [32,33,34]. In addition to that, we take into account a corresponding neural network for this system of ODEs as illustrated in Fig. 5,

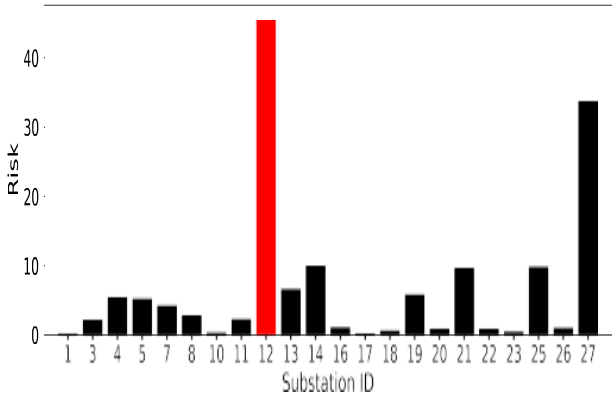
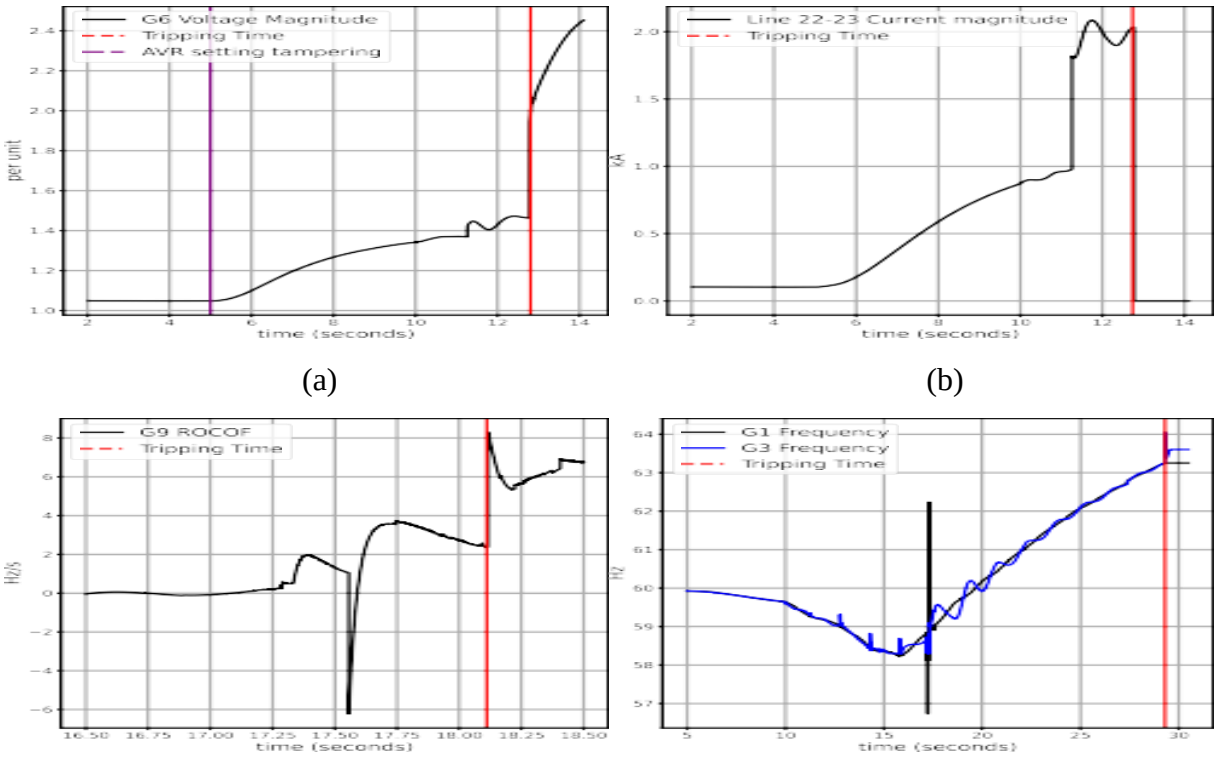


Figure 14. SUSSTATION ID,S AT RISK

A similar test as was used in LSM, for the ANN-Approach it would not be possible because to long training times Result Fig. (17) 34 runs 15 Top). Only ~34% of the fitting results good enough with (1.23 *10^-07 average error). Hopefully this will lower error as we keep more data points. Rump , Ass, BLMA in [35,36]. ANN-Approach has been shown to be applicable for solving ODEs here. Many authors have introduced ANN based techniques such as Lagares throughout [37,38,39] to enclose the boundy and initial value problem. The effect changes of connected devices damaging rate Figure(2)

with Design algorithm BLMA. This unique technique is a model free neural network based approach which can be represented in form of almost solution (this approximator) to the system ODE using universal approximation theory [Hornik et al. Hypothesis: A moderately tiny concealed layer FNN is universal approximators for continuous function.



(a) (b)

(b) (d)

Figure 15. Case 3 of ODE for training analysis

The ODE's should be written as the following system in order to achieve this:

$$\{S'(q) = F_1(S(q), E(q), I(q), A(q), R(q), q), S(q_0) = S_0\ E'(q) = F_2(S(q), E(q), I(q), A(q), R(q), q), E(q_0) = E_0\ I'(q) = F_3(S(q), E(q), I(q), A(q), R(q), q), I(q_0) = I_0\ A'(q) = F_4(S(q), E(q), I(q), A(q), R(q), q), A(q_0) = A_0\ R'(q) = F_5(S(q), E(q), I(q), A(q), R(q), q), R(q_0) = R_0\ \#(5)$$

These results can be written in terms of the solution to a differential equations,

$$y'(q) = F(y(q), y(q)) = y_0 \#(6)$$

Here in this solution y^'(t) indicates LHS, F(y(q),(q)) 100 times stands for the RHS and y(q_0)=q_0 provided by system's beginning condition. Here y(t) is relevant not just to time t but rather some current and past times, thus serving as another more global internal state: Another way of arriving at the same solution applies an ANN with 10 hidden layers for fitting a function instead of approximating matrix multiplication in the form:

$$N(q, w) = W_{k2} u(W_{k1} + b_1) + b_2 \#(7)$$

In this, W is weights and t for input (in stat). here again the linear activation function wit Sigmoid & Tanh as 2 case of u with bias term b1,b2 where wk1 to wkn are weight matrices [40,41,42]. All the parameters are denoted here W [Wk1,b1,Wk2,b2] This answer is further rewrite as follows;-

$$y(q,w) = y_0 + q - q_0 N(q,w) \#(8)$$

Where,$N(q_0,w) \neq y_0 \#(9)$

Such that y(q0,w) y0 and caused his [43] Given the loss function (w), we can then obtain an ideal parameter.

In order to check the design algorithms for effectiveness and efficiency, Table 3. and Table 4. Figure 12(a) and (b) compare results of Runge–Kutta method [44], least square method [45] versus machine leaning algorithm FNN-BLM recursive learning process equivalent to effective response for various value set in Tables III - IV. The numeric results show that the FNN-BLM method is very accurate and numerically approximates these types of solutions by an error less than 10−5 to fewer then 10−8 absolute values.

5. Discussion

The research identifies cybercrime within Jordanian adapting COVID-19 issues through the timeline mapping Table 52: Timeline Mapping of Major Events and Malicious Attacks Event/Cyber Attack centered Impact on Org Statement Made before an attack by a group or individual Porcos malevolos | Ciberataques, Crime corporative in addition to evaluating its cybersecurity Fig. This study will try to include cyber crime in Jordan criminal justice system and challenges, it covers some of the Jordanian legislation on combating cybercrime or any different type of crimal activities committed using an electronic device [46,47]. Cybercrime affects billions of people, resulting in the stealth of personal details. Events in the past year only have affected million's of people belonging to U.S. (i.e., 54 m), Turkey, S Korea and Germany each having an impact on between 16–20 million individuals. [48] In 2007, the National Social Crime Records Bureau registered a total of 217 incidents under IT Act in comparison to merely142 what was recorded in the year preceding it which is getting close to more than half '52.8%' rise! Maharashtra accounted for the maximum share (21.56%), followed by Kharghar, Tamil Nadu and states/UTs .Greatest number or 99 of the overall casualties which were listed under IT Act 2000 were in rebald publishing or transference etc. RTVF commonly known as cyber pornography. [49,50]

I/P	O/P	Desired value	AE
0	998.6985	999	2.45E-04
0.5	969.7854	973.2886	5.67E-03
1	951.1200	925.6871	6.99E-04
1.5	926.7823	901.363	3.89E-05
2	901.2540	879.2326	4.81E-03
2.5	889.3298	859.23	1.34E-03
3	857.3698	862.1548	8.33E-04
3.5	827.4930	812.1254	3.78E-03
4	815.3210	795.3579	2.34E-04

4.5	795.0035	812.1245	2.76E-04
5	774.2589	774.2159	2.18E-05

Table 1. Case for Asymptomatic device and comparing ML derived outcomes with RK-4

All cases (46.5%) [51] A natural system to apply the new control scheme is the Keller-Segel equations [52], which model a group of organisms with fascination and revulsion, whose tracking can be in charge under stability conditions. It aims to discover control mechanisms that, when present in the system stabilize globally Is undertaken to build a workable and accurate mathematical model which describes the propagation behaviour of an infinite number potential Threats originated from outside.

I/P	**O/P**	**Desired value**	**AE**
0	1	1	2.98E-07
0.5	0.952444	1.5626	4.32E-07
1	0.907898	1.9233	9.43E-08
1.5	0.866174	2.3659	2.34E-08
2	0.827094	2.9823	4.45E-08
2.5	0.790492	3.2658	1.32E-07
3	0.785424	3.7896	3.45E-08
3.5	0.745265	4.2202	3.34E-08
4	0.631555	4.8963	2.53E-07
4.5	0.663256	5.1635	1.34E-07
5	0.614847	5.6856	2.13E-07

Table 2. Case for Recovered device

The earliest step is to create a list of solution from the system of ordinary by obtaining results through numerical approaches The system of differential equations employs the TheRK-4 method helps to access a bunch effective resolutions as an collection of sequence, usually in form time series number. Having created the data-set, it can now use to train an ANN[53,54,55]. These RK-4 results are used as target data in training the ANN. Training an ANN is about creating a model to predict based on the input data, which has not been seen in training and this process starts from feeding the weights(bias) initial values of These are simply tensors that represent how different factors affect each attribute. After this forecasted result is collated to the desired result and we get an error as a difference between these two. We simply takeback the fallicies through the network using basic algebra (backpropagation), and we then adjust our weights & biases to minimize that error. The weight update method is performed again for many values , where an value means passing one example through the network whereas a pass over all training examples in this manner goes by name epoch. The aim is to minimalize the fallacy in forecasted output vs desired output for every input by changing the weights and bias till the prediction has a low amount of error. When the dataset is tested, validated and trained then it’s performed value are predicted using BLMA. For each data set, a convergence analysis was performed in combination with error histograms to highlight the effectiveness and precision of the design strategy[56,57].

I/P	O/P	Desired value	AE
0	0	0	1.98E-07
0.5	0.078	0.456	6.32E-02
1	0.124	1.243	1.43E-02
1.5	0.212	1.659	2.34E-01
2	0.275	2.233	2.45E-01
2.5	0.353	2.849	2.32E-01
3	0.424	3.7896	3.45E-01
3.5	0.444	4.2202	4.34E-01
4	0.459	4.8963	4.53E-02
4.5	0.534	5.1635	4.34E-01
5	0.563	5.6856	5.13E-07

Table 3. Case for Susceptible devices

I/P	O/P	Desired value	AE
0	1	1	4.56E-07
0.5	0.925646	0.925646	6.34E-09
1	0.907898	0.907898	2.87E-06
1.5	0.866174	0.866174	1.07E-09
2	0.827094	0.827094	2.59E-08
2.5	0.730492	0.730492	1.32E-07
3	0.65424	0.65424	3.45E-08
3.5	0.645265	0.645265	2.62E-08
4	0.531555	0.531555	8.65E-07
4.5	0.463256	0.463256	6.65E-07
5	0.414847	0.414846	2.13E-07

Table 4. Case for Exposed devices

The Figure of the numerical solution has been constructed with Matlab software. We trained the network by using Backpropagation Levenberg- Marquardt method (BLMA). BLMA techniques are particularly well-suited for working through linear scenarios due to simple basic concept and easy interface[58,59]. This also compares well to other machine learning techniques, with the BLMA chain. We utilized training data, validation and testing as 70%(701 samples),15(150 samples)% & same for testing with the hidden neurons of fitting network having layer configuration shown in Fig (13) / each input. The worst value and arrows in histograms to compare the output data versus target, Figure compute the error. This week, Figure 14 focused on how to analyse the number of cyber attacks over the time using a histogram approach. This histogram shows you distributions of attacks in a specific time period for each attack as well as distribution data about some attack features like duration, type and strength. The histogram visualization helps Cybersecurity experts to recognize that how cyber assaults patterns generally look like and where extra security can be needed. The root of that fallacy / number of the samples is called as MSE. shown in Figure(14). And the image suitable shows accuracy Although when converge towards zero and are near to 0 here, mean output is most accurate (Figure 17). Figure (19) gives evidence, Figure 20: Gradient Exemplification (Behaviour)The training Figure

which explains the behaviour, depicts error in comparing RK-4 with target data for different parameters[60,61,62].

I/P	O/P	Desired value	AE
0	0	0	1.94E-07
0.5	0.01	0.56	8.64E-07
1	0.03	1.03	9.02E-06
1.5	0.04	1.55	5.36E-08
2	0.06	2.06	7.23E-08
2.5	0.07	2.57	1.02E-07
3	0.08	2.67	1.23E-06
3.5	0.09	3.67	2.65E-08
4	0.10	4.51	5.68E-07
4.5	0.11	4.92	4.36E-06
5	0.13	5.23	2.89E-07

Table 5. Case for Infected Devices

Case 1 — Random setups chosen by us Also employ a similar process in order to reach the surrogate answer. Also plotting the curve solution with Matlab In next case, it varies with birth percentage(B), recovery percentage Re: Regeneration Stage), infectious recovering stage (αRc From Infected Recovered/ Over device Crash :(M)), death ratio to crashed devices (μNatural or Natural Death) and existence device is not need anymore[64]. This is done at same time to hold infection rate, contact and the new vulnerability of device infected in this case devices leaving Unprotected are either already being compromised may be due to download instructions or they contacting neighbours. Then in the forwarding case, birth percentage recovery percentage infectious recovering stage device crash and exits inputted as constant[65]. Furthermore, it attributes other variables like: infection rates involving devices left exposed either to the infected one or an attacked device as demonstrated in Figure (4), contact rate and so forth. The error is calculated in the histogram Figure, by collating output data vs desired. As shown in Figure 8, the MSE is equal to square root of total errors by number sample points. Accuracy of this Figure fitting. Figure (6): Countermeasure to recognise the number of cyber threats with passage of time. Histogram visualizing amount of attacks in a time span per and distribution of attack attributes (duration/duration range, type too etc.). Cyber security analysts can gain insight to the nature of cyberattacks, possible regions where more secure precautions are needed by examining this histogram. This plot is shown in Figure (7) which represents when all points on the converged at zero, or very near to zero means it goes accurate result. The Figure (9) illustrates the gradient behaviour during training[66,67]. The gradient that the optimising algorithm is with respect to network weights and it tries to learn how they can be changed in order for better network performance. We also validate the curves to target solutions and hope for a regression of 1 with respect to all forecasted output like we have shown in Figure.

6. Conclusion

Artificial Intelligence based technique is Artificial Neural Networks through which we are developing the descriptive model to simulate Pony Stealer in Developed connection. The model is compartmental

in that it views both symptomless devices and Exposed, Susceptible, Infectious and Recovered as separate systems connected through a common server. There are, however, infections that may be transmitted when the carrier of a pathogen has no symptoms (e.g. Although not all of the devices listed here are generally used in cyber security models, it is important to have a complete classification- and infection-devices include those viruses that can be traced by means of infections facilities for they usually aim at enabling an unintended access shared and written from remote site (wherefrom collecting user data might be possible) [68]. In actual world these process are governed by a system of ODE. They can resolve the ODE method beneath epidemic model by employing machine learning methods based on deep neural training [69]. We will make a single layer per node and equation for one hidden layers of Matlab nodes arteries, then creating the RK-4 reference solution.

which is then used in the training testing. validation steps of Levenberg Marquardt algorithm. The outcome of these Graphical Analysis disclose that applied approach is true and efficient as this presents least absolute errors when compared with well-known methods in front of approximate solutions, analytical answers. Furthermore, the performance indicator values were approaching zero which is evidence of a superior outcome modelling.

References:

[1] O. David, S. Sarkar, N. Kammerer, C. Nantermoz, F. M. de Chamisso, B. Meden, J.-P. Friconneau, and J.-P. Martins, ‘‘Digital assistances in remote operations for ITER test blanket system replacement: An experimental validation,’’ Fusion Eng. Des., vol. 188, Mar. 2023, Art. no. 113425.

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

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

[4] R. Pinciroli and C. Trubiani, ‘‘Performance analysis of fault-tolerant 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 wire- less 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 classifi- cation 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.

.