Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 44 (2023), No. 6, pp. 1043–1055
DOI : 10.47974/JIOS-1426

Computer virus propagation models: A mathematical review

Om Prakash *
Avadhesh Kumar †
School of Computing Science & Engineering
Galgotias University
Greater Noida
Uttar Pradesh
India

Sunil Kumar Bharti §
Department of Information Technology
Galgotias College of Engineering and Technology
Greater Noida
Uttar Pradesh
India

Abstract

The physical world has come together by the connection of devices on an extra ordinary level through internet of things. This forms a very complex and dynamic network system and number of heterogeneous device are connected with each other. Physical objects connected in a network, interchange data with other connected devices via communication networks. The data interchange is very helpful in a number of domains in day-to-day life of human beings. Security of connection and data is one of the major challenges for this connection and communication. A computer virus is a potential threat resulting into the damage of connected devices into a network and the data. Epidemic models, similar with biological virus spread models, are widely studied to investigate the behaviour of computer viruses. The primary objective of the article is to categorize a number of computer virus propagation model, so that their comparative studies becomes easier. This article contains a qualitative review and categorization of computer virus propagation models into three categories,

* *E-mail:* om.prakash@galgotiasuniversity.edu.in; palpal.prakash@gmail.com (Corresponding Author)
† *E-mail:* pvcdrak@galgotiasuniversity.edu.in
§ *E-mail:* sunil.kumarbharti@galgotiacollege.edu

namely, compartment model, network model and stochastic model. The study is helpful to further investigate the virus propagation mechanism and to control them optimally.

Subject Classification: *68M25 Computer security.*

Keywords: *Delay differential equation, Epidemic model, Network model, SIR model, SIS model, Stochastic model.*

1. Introduction

21st Century is the century of information &technology. All devices and objects are connected with each other to form a network. A program known as computer virus is very harmful for these networks due to the reason that they may infect the system without permission or prior knowledge. A virus has two important features as they may create own copy or may attach with same other system. A virus may spread into the system by network, services or by some other way such as phishing [1]. Viruses create a challenging security issue as they effect the production or may causes millions of Dollars loss. A traditional computer virus has properties such as function-ability, tendency to high information, accessibility without permission, infecting other systems and destroying to system and so on. With the advancement of technological development, computer viruses have been advancing in term of various ways like remote control feature, selected and targeted attack, transmission in various ways etc. [2, 16].

Computer viruses are computer programs written by persons for notorious activities. As soon as, a computer virus infects the system it captures CPU execution, it starts searching for the suitable program or storage to replicate its self and try to enter other connected computers. This mechanism is known as spreading of the computer virus. The computer which has the virus are termed as infected computers [5, 6, 7]. In order to work smoothly, computer networks are required to monitor against such computer virus spreading and a control mechanism is required to procure the infected computer system. Thus, computer virus detection and its control has become a challenging task in the connected world [13]. A number of researchers have been studied the computer virus propagation and proposed many mathematical models to describe the virus spreading mechanism and control dynamics. Dynamical study of computer virus spreading is very useful in prediction of its spreading so that suitable mechanism can be applied to reduce the damage optimally [29]. Zarin *et. al.* (2022) [23] applied fractional calculus to investigate the

computer virus dynamics and compared the findings with the classical models. This article contains a thorough review of existing computer virus propagation models. Computer virus propagation models exist in literature may be categorized into three groupsviz. compartmental model, network model and stochastic model [34-35].

The article is structured in 5 sections. Section 1 contains a brief introduction about computer virus and its propagation. Section 2 contains the detail description of compartment models. Section 3 includes the development of network model whereas as discussion of stochastic models are given in section 4. And at last,conclusion and future scopeis the part of section 5.

2. Compartmental Model

Compartmental models are given by various researchers such as Ross & Hudson, Kermeck & Mc-Kendrick in earlier decades of 20th Century. These models are deterministic in nature. Dynamic of these models are denoted by connected rectangular boxes. Each rectangular box is termed as a compartment and represents an infection status whereas the connection represents the transition flow [18, 19]. These are very general-purpose models widely used to investigate the infected population in epidemic. Later on, these models are applied to investigate the transmission and control of computer viruses in a system. These models are deterministic in nature. Few important compartmental models are discussed as below:

- SIS Model
- SIR Model
- SEIR Model

2.1 *SIS Model*

This model is known as "Susceptible to an infection of a Susceptible". This model has two compartments (states) Susceptible and infected. Figure 1 illustrates the block diagram for SIS model having two states.

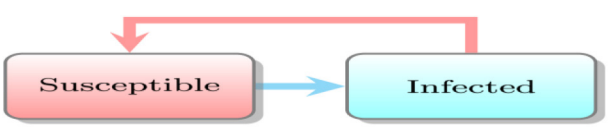

Figure 1

SIS model for computer virus propagation

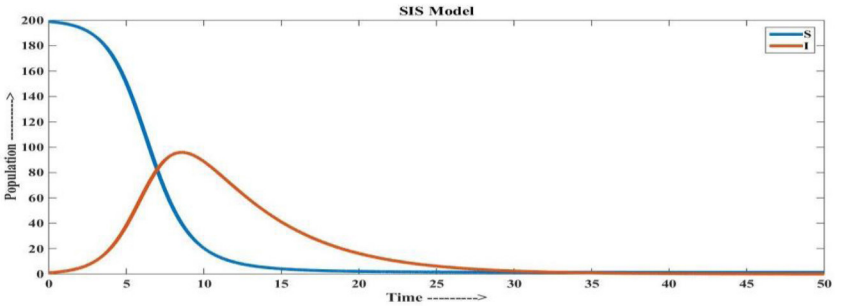

Figure 2

Evolution of population in SIS model for computer virus propagation

Here, both states are reversible i.e., a suspected node can become an infected node vice-versa.

Let a is the rate of transition of a suspected node to become an infected node and b is the rate of transition of infected node to become a susceptible node then SIS model may be defining as:

$$\frac{dS}{dt} = -\frac{aSI}{N} + bI$$
$$\frac{dI}{dt} = \frac{aSI}{N} - bI \qquad (1)$$

With Initial Conditions: $I(0) = I_0$ and $S(0) = N - I_0$

N is total number of computers in networks, S and I susceptible computers and infected computers respectively. Figure 2 illustrates the evolution of susceptible and infected population for $a = 1,\ b = 0.2$ and total population $N = 200$.

Wierman and Marchette (2004) [12] have investigated the SIS model with an additional parameter known as reintroduction parameter which is associated with the repeated virusrelease. This model is useful to investigate the quasi-stationary regime of the model. Korkiatsakul *et. al.* (2019) [28] have investigated the FSSIP model to examine how antivirus affects the way computer viruses spread.

2.2 *SIR Model*

This model has 3 compartments namely Susceptible (S), Infected (I) and Removed (R). S and I states have similar characteristics of SIS model whereas R node is also known as Immune State. This state has the antiviral ability to avoid virus. Figure 3 illustrates the block diagram for SIR model with three states.

Figure 3

SIR model for computer virus propagation

Let a be the transition rate for Susceptible node to become an infected node and b be the transaction rate for infected node to become a removed node, then the SIR model may be defining as below.

$$\begin{aligned}\frac{dS}{dt} &= -\frac{aSI}{N}\\ \frac{dI}{dt} &= \frac{aSI}{N} - bI\\ \frac{dR}{dt} &= dI\end{aligned} \tag{2}$$

With initial condition: $S(0) = N - I_0$, $I(0) = I_0$ and $R(0) = 0$. Total number of computers in the network are N.

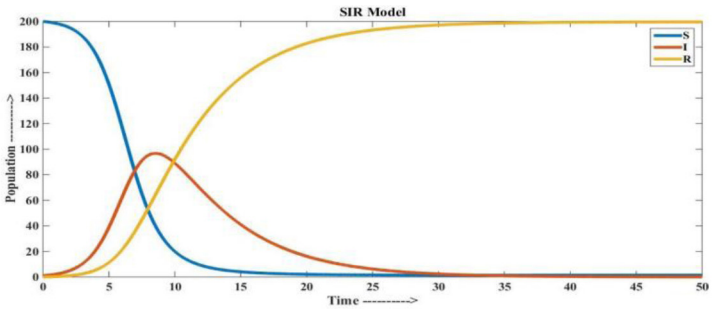

Figure 4

Evolution of population in SIS model for computer virus propagation

Figure 4 represents the evolution of SIS model for parameter values for a = 1, b = 0.2 and initial total population of 200 and infected population 1. Li *et. al.* (2014) have extended the SIR model by adding antidotal dimension and proposed SIRA model is highly efficient to explain the dynamical behavior of computer virus propagation. Shahrear *et. al.* (2018) [22] have proposed SAEIQRS model which is a variant of compartment model. Ren *et. al.* (2012) [14] have incorporated the delay parameter in the SIR model and investigated the global stability. Gan *et. al.* (2014) [7] have extended the SIRS model in term of vaccination probability and noticed that the internet holds the power law behavior.

2.3 *SEIR Model*

This model has 4 compartments, namely, Susceptible(S), Exposed (E), Infectious (I) and Recovered (R). This model is shown in following Figure (5).

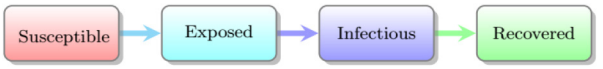

Figure 5

SEIR model for computer virus propagation

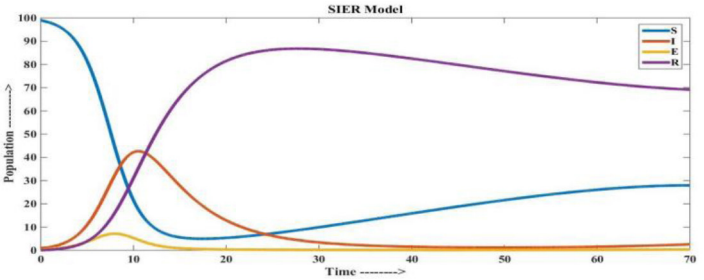

Figure 6

Evolution of population SIER model for computer virus propagation

Let a be the transition rate from susceptible node to exposed node, b be the transition rate from suspected node to be recovered node, c be the transition rate from exposed node to be a infected node and d be the transition rate from infected node to be a recovered node, then the SEIR model may be given as below.

$$\begin{aligned}
\frac{dS}{dt} &= bN - bS - \frac{aIS}{N} \\
\frac{dE}{dt} &= \frac{aIS}{N} - (b+c)E \\
\frac{dI}{dt} &= cE - (b+d)I \\
\frac{dR}{dt} &= dI - bR
\end{aligned} \tag{3}$$

w.r.t. initial conditions: $I(0) = I_0$, $E(0) = 0$, $R(0) = 0$ and $S(0) = N - I_0$. Total number of computers in the network are N.

Figure 6 shows the development of population of various types of nodes in SIER model with the parameter values a = 1, b = 0.2, c = 2, d = 0.2 and initial total population 100 and infected population 1. Liu and Zhong (2017) [30] have extended the SIR model and suggested that the spread of

virus infection can be control with choice of suitable parameters. M S S Khan (2014) [20] has extended the SIR model in term of probabilistic SEIR model and investigated the epidemic behavior of computer virus over scale free networks. Srivastava *et. al.* (2018) [21] have applied the SEIQR model to investigate the virus propagation dynamics over wireless sensor networks [2]and computed a reproduction number which plays a vital role in stability of the model. Yang and Yang (2014) [17] have assumed that the accessibility of a computer by others are equally likely and have applied the concept of asymptotically autonomous systems to propose a new epidemic model for computer virus propagation. There are many other variants of compartmental models exists in literature. These models are widely used to investigate the evolution dynamics of viruses and stability status for control purpose.

3. Network Model

Computer viruses spread into a network in various ways a single model is not sufficient to describe all characteristics of such viruses in a network. Interconnection of systems into a network are logical and dynamic mean, while cure rate of viruses are dynamics which causes the factors for computer viruses to differ from epidemic viruses [36-37]. Thus, a new computer virus spread model is suggested which is based on the computer network. This model is basically focuses on network connection and virus cure rate. In order to investigate the effect of network topology and storage media on computer virus spreading, Gan *et. al.* (2020) [33] have applied the concept of SIR model and proposed an updated network model. Their finding suggests that the virus can be eliminated from the network which depends on the outbreak threshold [38-39].

Late N, c, α, b and I are number of nodes in a network, network connection rate within the region, transmission probability of viruses, cure rate of infected node and total number of active infected nodes t, respectively than the network model may be defined as below.

$$\frac{dI}{dt} = (n\alpha c - b)I - \alpha c I^2 \tag{4}$$

Figure 7 depicts the evolution of computer virus population with parameter values b = 0.01, c = 0.5, a = 0.05 and initial population 150. Zhou *et. al.* (2011) [15] have projected a new computer virus model which capable to mimic the statistics of virus spreading over the network environment. Chu *et. al.* (2019) [31] have proposed the SVEIR model with delay.

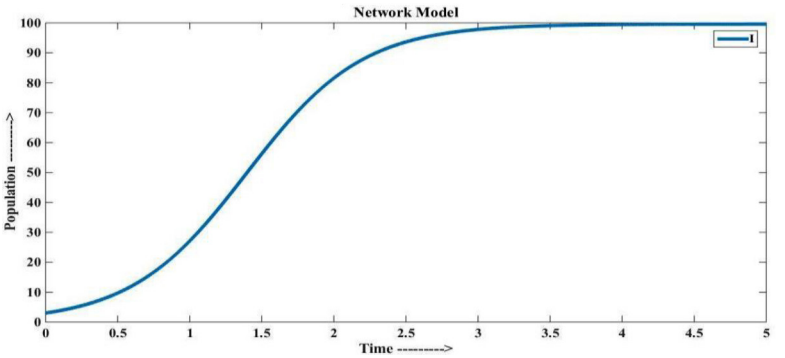

Figure 7

Evolution of population in network model for computer virus propagation

Investigation of distribution of characteristic values suggested for the Hopf bifurcation existence for this model. Amador and Artalejo (2013) [11] applied stochastic SIRS model to study the computer virus spreading dynamics and noticed the quasi-stationary behavior in the network.

4. Stochastic Model

Computer viruses are highly unpredictable and their dynamics is uncertain. Deterministic models as discussed in a compartmental model are not sufficient to capture their uncertain dynamics. In order to capture the uncertain behavior stochastic differential equations (SDE) are suggested in literature, specially, Ito SDEs are very helpful to investigate computer propagation's model [24, 25, 26]. Parametric and non-parametric, both type of perturbation is used to investigate stability analysis of the model, virus spread dynamic and control mechanism. A deterministic model can be transformed into a stochastic model by applying two techniques [24, 27]. A parameter of concern in deterministic model may be transform into random variable or a Brownian motion may be incorporated in differential equations. Raza *et. al.* (2019) have investigated the stochastic computer virus propagation model in term of numerical simulation schemes and suggested that such types of models are more efficient as compared with the deterministic models. The stochastic model driven by non-parametric perturbation is given as below [3].

$$dS = ((1-p)N - aSI - bSE + (p+c)S + \xi_1(t)S)dt$$
$$dE = (aSI + bSE - \alpha E - (k+c)E + \xi_2(t)E)dt$$
$$dI = (\eta E - (\nu + c)I + \xi_3(t)I)dt \quad (5)$$

Here $\xi_1(t)$, $\xi_2(t)$ and $\xi_3(t)$ are Gaussian White noise.

Zhang *et. al.* (2012) a stochastic computer virus that has been hypothesized and studied propagation model. This model is further analyzed by applying Ito calculus and Lyapunov functions. Raza *et. al.* (2019) [3]investigated the stochastic computer virus propagation model and compared the findings with the deterministic models. Their finding suggests that the stochastic models are more reliable as compared with the deterministic models in term of numerical treatments. In order to study the spreading effect of infected node over internet. Zhang *et. al.* (2019) [32] have applied the time delay in classical computer virus propagation models and proposed the SBLS model to study the control parameters for the epidemic spread.

5. Conclusion and Future Scope

The rapid growth in internet and technology have brought convenient life for people in many folds. A number of challenges associated with technology have also came in to existence due to technological growth. Computer and network security is one of the challenging issues in technological world now a days. It is important to study the virus spreading so that suitable mechanism can be applied for its control. The concept of epidemic modeling is widely used to study and investigate the virus propagation. In the number studies, this is found that malware spreads across IoT devices in a manner similar to how viruses spread through populations. This paper lists and categorizes significant viral propagation models to enable the selection of an appropriate mathematical model for future research.

Conflicts of Interest

The authors claim to have no conflicts of interest.

References

[1] A. Lohachab & B. Karambir, "Critical Analysis of DDoS; An Emerging Security Threat Over IoT Networks", *J. Commun. Inf. Netw.* vol. 3, pp. 57-78, (2018).

[2] A. Singh, A. K. Awasthi, K. Singh & P. K. Srivastava, "Modeling and Analysis of Worm Propagation in Wireless Sensor Networks", *Wireless Pers Commun,*, vol. 98, pp. 2535-2551, (2018).

[3] A. Raza, M. S. Arif, M. Rafiq, M. Bibi, M. Naveed, M. U. Iqbal, Z. Butt, H. A. Naseem and J. N. Abbasi, "Numerical Treatment for Stochastic Computer Virus Model", *Computer Modeling in Engineering & Sciences,* vol. 120, no. 2, pp. 445-465, (2019).

[4] B. K. Mishra and G. M. Ansri, "Differential Epidemic Model of Virus and Worms in Computer Network", *International Journal of Network Security,* vol. 14, no. 3, pp. 149-155, (2012).

[5] B. Zhu, S. Deng, Y. Xu, X. Yuan & Z. Zhang, "Information Security Risk Propagation Model Based on the SEIR Infectious Disease Model for Smart Grid", information, vol. 10, pp. 1-17, (2019).

[6] C. Gan, X. Yang, W. Liu & Q. Zhu, "A Propagation Model of Computer Virus with Nonlinear Vaccination Probability", "*Communications in Nonlinear Science and Numerical Simulation*", vol. 19, pp. 92-100, (2014).

[7] C. Gan, X. Yang, W. Liu & Q. Zhu, "Propagation of Computer Virus both Across the Internet and External Computers: A Complex-Network Approach", "*Communications in Nonlinear Science and Numerical Simulation*", vol. 19, pp. 2785-2792, (2014).

[8] C. Li, W. Hu and T. Huang, "Stability and Bifurcation Analysis of a Modified Epidemic Model for Computer Viruses", *Mathematical Problems in Engineering,* vol. 2014, ID. 784684, pp. 1-14, (2014).

[9] C. Zhang, Y. Zhao, Y. Wu and S. Deng, "A Stochastic Dynamic Model of Computer Viruses", *Discrete Dynamics in Nature and Society*, vol. 2012, article ID. 264874, pp. 1-16, (2012).

[10] H. Chen and Y. Huang, "Study of Computer Virus Propagation Models in Networks based on the Stability and Control", *Bio-Technology: An Indian Journal,* vol. 10, issue: 13, pp. 7417-7421, (2014).

[11] J. Amador and J. R. Artalejo, "Stochastic Modeling of Computer Virus Spreading with Warning Signals", *Journal of the Franklin Institute,* vol. 350, pp. 1112-1138, vol. (2013).

[12] J. C. Wierman and D. Marchette, "Modeling Computer Virus Prevalence with a Susceptible-Infected-Susceptible Model with Reintroduction", *Computational Statistics & Data Analysis*, vol. 45, pp. 3-23, (2004).

[13] J. N. C. Goncalves, H. S. Rodrigues, M T. T. Monterio, "Optimal Control Measures for a Susceptible-Carrier-Infectious-Recovered-Susceptible Malware Propagation Model", *Optimal Control Applications and Methods,* vol. 40, no. 4, pp. 691-702,(2019).

[14] J. Ren, X.Yang, Q. Zhu, L.X. Yang and C. Zhang, "A Novel Computer Virus and Its Dynamics", *Nonlinear Analysis:: Real World Applications,* vol. 13, pp. 376-384, (2012).

[15] J. Zhou, X. Hua & Chen, "Analysis and Simulation of Computer Virus Propagation Models in the Network Environment", *Advanced Materials Research,* vol. 204, pp. 433-436, (2011).

[16] K. Sha, W. T. Wei, A. Yang, Z. Wang & W. Shi, "On Security Challenges and Open Issues in Internet of Thing", *Future Generation Computer Systems,* vol. 83, pp. 326-337, (2018).

[17] L. X. Yang & X. Yang, "A New Epidemic Model of Computer Viruses", "*Communications in Nonlinear Science and Numerical Simulation*", vol. 19.pp. 1935-1944, (2014).

[18] L. X. Yang, X. Yang, L. Wen and J. Liu, "A Novel Computer Virus Propagation Model and Its Dynamics", *International Journal of Computer Mathematics,* vol. 89, no. 17, pp. 2307-2314, (2013).

[19] M. Peng, X. He, J. Huang and T. Dong, "Modeling Computer Virus and its Dynamics", *Mathematical Problems in Engineering*, vol. 2013, ID. 842614, pp. 1-5, (2013).

[20] M. S. S. Khan, "A Computer Virus Propagation Model Using Delay Differential Equations with Probabilistic Contagion and Immunity", *International Journal of Computer Networks & Communications*, vol. 6, no. 5, pp. 111-128, (2014).

[21] P. K. Srivastava, R. P. Ojha, K. Sharma, S. Awasthi and G. Sanyal, "Effect of Quarantine and Recovery on Infectious Nodes in Wireless Sensor Network", *International Journal of Sensors, Wireless Communications and Control*, vol. 2018, no. 8, pp. 26-36, (2018).

[22] P. Shahrear, A. K. Chakraborty, M. A. Islam and U. Habiba, "Analysis of Computer Virus Propagation Based on Compartmental Model",

Applied and Computational Mathematics, vol. 12, no. 1-2, pp. 12-21, (2018).

[23] R. Zarin, H. Khaliq, A. Khan, D. Khan, A. Agkul and U. W. Humphries, "Deterministic and Fractional Modeling of a Computer Virus Propagation ", *Results in Physics*, vol.33, ID. 105130, pp. 1-13, (2022).

[24] S. K. Choudhary, "Emergence of Power Law Behavior in Threshold based Neuron Model with Stochastic Membrane Constant", *International Journal of Applied Mathematics and Informatics,* vol. 12, pp. 21-28, (2018).

[25] S. K. Choudhary, K. Singh and V. K. Solanki, "Spiking Activity of a LIF Neuron in Distributed Delay Framework", *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 3, no. 7, pp. 70-76, (2016).

[26] S. K. Choudhary and K. Singh, "Temporal Information Processing and Stability Analysis of the MSHN Neuron Model in DDF", *International Journal of Interactive Multimedia and Artificial Intelligence,* vol. 4, no. 2, pp. 39-45, (2016).

[27] S. K. Choudhary and V. K. Solanki, "LIF Neuron with Hypo-exponential Distributed Delay: Emergence of Unimodal, Bimodal, Multimodal ISI Distribution with Long Tail", Recent Patent on Engineering, vol. 12, pp. 21-28, (2020).

[28] T. Korkiatsakul, S. Koonprasert and N. Neamprem, "Analytical Solutions of Computer Virus Propagation Model with Anti-virus Software and Time Dependent Connecting Network in Caputo Fractional Derivative Sense", *International Journal of Engineering Research and Technology,* vol. 12, no. 12, pp. 3006-3017, (2019).

[29] W. C. Yen, E. Lin and C. L. Huang, "Predicting Spread Probability of Learning-Effect Computer Virus", *Coevolving Spreading Dynamics of Complex Networks,* vol. 2021, ID. 6672630, pp. 1-17, (2021).

[30] W. Liu & S. Zhong, "Web Malware Spread Modelling and Optimal Control Strategies", *Sci Rep*, vol. 7, no. 42308, pp. 1-19, (2017).

[31] Y. Chu, W. Xia and Z. Wang, "A Delay Computer Virus Model with Nonlinear Incidence Rate", *Systems Science & Control Engineering*, vol. 7, no. 1, pp. 389-406, (2019).

[32] Z. Zhang, S. Kumari and R. K. Upadhyay, "A delayed e-Epidemic SLBS Model for Computer Virus", *Adv Differ Equ,* vol. 2019, ID. 414, pp. 1-24, (2019).

[33] C. Gan, Q. Feng, Q. Zhu, Z. Zhang, Y. Zhang and Y. Xiang, "Analysis of Computer Virus Propagation Behaviors over Complex Networks: A Case Study of Oregon Routing Network,," *Nonlinear Dyn*, vol. 100, pp. 1725-1740, (2020).

[34] Kar, A. K., & Aswani, R. (2021). How to differentiate propagators of information and misinformation–Insights from social media analytics based on bio-inspired computing. *Journal of Information and Optimization Sciences,* 42(6), 1307-1335.

[35] Kumar, A., Singh, K., & Khan, T. (2021). L-RTAM: Logarithm based reliable trust assessment model for WBSNs. *Journal of Discrete Mathematical Sciences and Cryptography,* 24(6), 1701-1716.

[36] Kumar, A., Singh, K., Khan, T., Ahmadian, A., Saad, M. H. M., & Manjul, M. (2021). ETAS: An efficient trust assessment scheme for BANs. IEEE Access, 9, 83214-83233.

[37] Shariq, M., Singh, K., Lal, C., Conti, M., & Khan, T. (2022). ESRAS: An efficient and secure ultra-lightweight RFID authentication scheme for low-cost tags. *Computer Networks,* 217, 109360.

[38] Khan, T., & Singh, K. (2019). Resource management based secure trust model for WSN. *Journal of Discrete Mathematical Sciences and Cryptography*, 22(8), 1453-1462.

[39] Singh, A., & Bist, A. S. (2020). OSX malware detection: Challenges and solutions. *Journal of Information and Optimization Sciences,* 41(2), 379-385.