Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Caputo Fractional-Order Compartmental Modelling of Cyberattacks on Financial Infrastructure

Nivedita Kumari[1], Bimal Kumar Mishra[2*]
[1]Department of Mathematics, Vinoba Bhave University, Hazaribag, Jharkhand, India.
[2*]Adarsh College, Rajdhanwar, Giridih, Jharkhand, India.
*Corresponding author;Bimal Kumar Mishra
*email: drbimalmishra@gmail.com

ARTICLE INFO

Received: 03 Nov 2024

Revised: 15 Dec 2024

Accepted: 25 Dec 2024

ABSTRACT

In an era where financial infrastructures are increasingly vulnerable to sophisticated cyberattacks, understanding the dynamics of threat propagation and the effectiveness of countermeasures is crucial. This study proposes a novel fractional-order SICS (Susceptible–Infectious–Countermeasures–Susceptible) epidemic model based on Caputo derivatives to analyze the transmission and containment of cyber threats in financial systems. The model incorporates memory-dependent behavior to more accurately represent real-world cyber phenomena, where the effects of an attack can persist and influence future vulnerabilities.

Using the Adams–Bashforth–Moulton predictor-corrector method, the system is numerically simulated under various parameter regimes. Comparative analyses between fractional ($\rho = 0.9$) and integer-order ($\rho = 1.0$) dynamics reveal that fractional models exhibit delayed peaks and prolonged persistence of infection, underscoring the importance of incorporating long-memory effects in cyberattack modeling. Sensitivity analysis demonstrates that increased transmission rates (β) amplify both peak and total infections, whereas enhancing isolation efficiency (α) and preventive countermeasures (γ) significantly mitigate the spread and duration of cyber threats.

While the model successfully captures key aspects of cyberattack dynamics, it assumes homogeneity and static parameters, limiting its representation of complex, adaptive adversarial behavior. The findings provide a rigorous mathematical foundation for strategizing effective cyber defense policies in critical financial sectors and highlight the potential of fractional calculus as a robust tool for modeling advanced cyber-physical systems.

Keywords: Fractional derivative; Caputo order; Reproduction number; Global stability; Lyapunov function; Sensitivity analysis; Adams–Bashforth–Moulton approach.

1. Introduction

In this digital age, cyberattacks on financial systems are becoming increasingly frequent and represent a serious risk to the stability and security of international economies. The financial industry is continuously under attack from malevolent cyber actors, from phishing scams targeting individual investors to ransomware operations targeting large financial institutions. The financial industry continues to grow rapidly to keep up with technology and shifting customer preferences. The way we handle and transmit money has completely changed, from digital wallets and cryptocurrencies to online banking and mobile payment apps. To understand how the financial system functions in the modern world, it is essential to know how these digital tools and platforms interact with conventional financial institutions. A financial system makes it easier for cash to move between lenders, investors, and borrowers who are involved in the financial market. Both national and international

financial systems operate [1]. Financial institutions are complex, interconnected markets, services, and organizations created to provide an effective and reliable relationship between borrowers and investors [2]. The financial system comprises four primary components:

a) Financial markets are the venues where buyers and sellers engage in the trading of bonds, shares, and other assets.

b) Financial instruments are the products exchanged in financial markets. The securities in the market vary according to the distinct criteria of loan seekers.

c) Financial institutions serve as intermediaries between investors and borrowers. They offer financial services to members and clients. They are also referred to as financial intermediates, as they serve as brokers between savers and borrowers. The investor's capital is activated either directly or indirectly through the financial markets. They provide services to organizations seeking to raise capital from markets and manage financial assets (deposits, securities, loans, etc.).

d) Financial services offerings supplied by asset management and liability management firms. They assist in acquiring the necessary cash and ensure their optimal investment. (for example, banking services, insurance services, and investment services).

The financial industry has been proved as a top target for cybercriminals. Financial institutions such as banks, insurance companies, and investment firms, manage extensive volumes of sensitive data and execute millions of transactions each day. Any interruption to these services might have profound effects, not only for individual but even for the entire economies. Malicious actors, including ransomware groups, state-sponsored hackers, and cybercriminal organizations, are acutely aware of this, persistently endeavoring to exploit weaknesses in financial networks. Recent high-profile events have illustrated how a single breach can impact global markets significantly. The Swift bank hacks and the Capital One data breach have compelled financial organizations to acknowledge that cyber resilience is vital.

Mathematical modeling is essential for comprehending the intricate dynamics of cyber attacks, offering insights into their patterns and associated risks. Researchers employ mathematical tools to simulate diverse attack scenarios and design effective prevention strategies to protect against cyber attacks. This method facilitates a more profound understanding of the fundamental principles of cyber attacks and improves the capacity to proactively manage risks in the digital realm. By developing and analyzing mathematical models, we can work towards enhancing cybersecurity measures and minimizing the risks associated with cyber threats in the financial sector. This research is essential for safeguarding the stability and security of financial systems in an increasingly digitized world. Also, by simulating different attack scenarios, researchers can identify vulnerabilities and develop strategies to strengthen cybersecurity defenses. These findings provide valuable insights for policymakers, financial institutions, and cybersecurity professionals in safeguarding against cyber threats in the digital age. Instead of using an ordinary derivative for the study of this paper, we use fractional derivative of Caputo order to get more accurate results. Fractional-time chaotic systems have been shown to exhibit richer dynamics and feature added degree of freedom, as in most cases the dynamics heavily depend on the fractional order [3]. Therefore, fractional concepts have been seen as a tool in the fields such as physics, chemistry, and engineering in terms of representing physical phenomena [4]. In contrast to the ordinary derivative, which functions as a local operator, the fractional order derivative possesses a principal characteristic known as the memory effect. Specifically, the subsequent state of the fractional derivative for any function f is contingent not only on its present state but also on all its prior states [5].

After analyzing the result, we focus on the security of the financial systems/ institutions. Here are some suggestive measures taken by them.

1.1. Robust Cybersecurity Frameworks and Strategies:

(a) Implement and comply with recognized frameworks such as the NIST Cybersecurity Framework, FFIEC Information Technology Examination Handbook, and the RBI Cybersecurity Framework in India. These establish a robust framework for mitigating cyber risks and fulfilling regulatory requirements [6-7].

(b) Risk-Based Supervision and Zero-Trust: Use a risk-based approach to supervision, adopting a "zero-trust" cybersecurity framework. This means no person or device is considered trusted by default, requiring authentication for every action in the system.

(c) AI-Aware Defense Strategies: Use Artificial Intelligence (AI) and Machine Learning (ML) to enhance threat detection, anomaly identification, fraud prevention, and automated incident response. AI can analyze large datasets instantly, predict potential threats, and identify weaknesses more effectively. However, it's important to note that attackers are also using AI, which creates a competitive environment that requires ongoing adjustments.
(d) Multi-layered Defense: Relying solely on one security solution is not enough. Employ a tiered strategy that includes a variety of security measures and technologies, such as perimeter defenses (firewalls, antivirus) and internal protections (encryption, endpoint security, network segmentation).
(e) Holistic Cyber Risk Management: Formulate a proactive and all-encompassing plan that addresses cyber risks associated with personnel, processes, technology, and external entities, rather than concentrating exclusively on technology.

1.2. Essential Technical Measures:

(a) Robust Access Controls: Enforce multi-factor authentication (MFA) for all users and devices accessing critical systems and data [8]. Employ role-based access control (RBAC) to restrict information access according to an employee's job responsibilities. Perform systematic access evaluations and audits [9].
(b) Data Encryption: Implement effective encryption methods for data both at rest and in transit, including end-to-end encryption for communications.
(c) Develop a patch management strategy to quickly identify, obtain, test, and deploy software updates for all operating systems and applications. This protects against known vulnerabilities.
(d) Advanced Threat Detection and Response: Use intrusion detection systems to monitor network data for unusual behavior. Implement Security Information and Event Management (SIEM) systems to collect and analyze security data in real-time for quick issue identification and response [10].
(e) Vulnerability Management: Establish comprehensive vulnerability management protocols to proactively detect security deficiencies, vulnerabilities, and misconfigurations, and prioritize their remedy prior to potential exploitation by attackers.
(f) Network Segmentation: Partition the network into smaller, isolated portions to restrict the lateral movement of intruders in the event of a breach.

1.3. Addressing Emerging Threats:

(a) AI-Powered Cyberattacks: Be ready for more complicated assaults that use generative AI to create malware, phishing emails, deepfakes, password cracking, and voice cloning. Smart, AI-powered defenses are needed for this.
(b) Ransomware and Malware: To reduce the impact of ransomware attacks, put strong endpoint protection, safe offsite and unchangeable backups, and effective incident response policies into place. Employees should be trained to identify the social engineering techniques that frequently precede ransomware.
(c) Supply Chain Attacks: Verify and keep an eye on third-party service providers and vendors. Incorporate cybersecurity obligations and requirements into contracts, and evaluate their security posture and regulatory compliance on a regular basis.
(d) Social Engineering (Phishing): Employees should get frequent cybersecurity training to inform them of the most recent risks, including phishing and social engineering techniques. To assess and enhance their capacity to identify and react to such efforts, conduct phishing simulations.
(e) Mobile Automated Transfer Systems (ATS) Attacks: As mobile banking becomes more prevalent, be vigilant against malware designed to make fraudulent transactions via banking apps.

1.4. Organizational and Human Factors:

(a) Strong Cybersecurity Culture: Foster a cybersecurity culture throughout the organization, starting from the top. Ensure executive buy-in and emphasize that security is a shared responsibility, not just an IT prerogative. Encourage employees to report suspicious activities.
(b) Employee Awareness and Training: Provide continuous and regular training sessions to educate employees about evolving cyber threats and best practices.

(c) Incident Response Planning: Develop and regularly update comprehensive incident response plans. These plans should outline clear steps for responding quickly and effectively to security breaches, minimizing impact, and ensuring swift recovery.
(d) Regulatory Compliance: Ensure adherence to relevant financial cybersecurity regulations. Establish governance frameworks that include regular audits and compliance checks.
(e) Collaboration and Information Sharing: Engage in industry-wide collaboration and information sharing with other financial institutions, regulators, and cybersecurity agencies to stay informed about emerging threats and best practices.
(f) By implementing these strategies and continuously adapting to the evolving threat landscape, financial systems can significantly enhance their resilience against cyberattacks and protect sensitive data and critical operations.
Besides these attacks, politically driven cyberwarfare that is a large-scale attack on financial institutions, has become an important chapter for discussion now-a-days. We will not discuss these politically driven aspects in this paper, which have become an integral component of traditional combat. During these assaults, hackers target an adversarial state to incapacitate its essential computer systems. For example, a conflict between Ukraine and Russia has persisted for over years [11].
Financial institutions are fundamental to a nation's economy, and safeguarding them against cyberattacks is imperative. This necessity is driven by various factors that impact a nation's economic, national security, and public trust.
We here, therefore, establish a fractional order epidemic model, namely SICS (Susceptible- Infectious-Countermeasures- Susceptible) in which reproduction number, equilibrium points, stability, etc are discussed in this paper. Several paper mainly concerning fractional order model are given in the references. A mathematical model of SIR epidemic system for COVID-19 with the help of fractional order derivative is discussed in detail by Alqahtani [12]. Paul, Mahata, Mukherjee, and Roy [13] analysed the dynamics of COVID-19 with the help of the epidemic SIQR model. Additionally, in the analysis of COVID-19, Chatterjee and Ahmad [14] make another attempt to discuss the infection of epithelial cells using fractional order differential equations. An approach to solving the differential equation of fractional order for an epidemic model with a Mittag-Leffler fractional derivative is presented by Sene [15]. SEIR epidemic model of fractional order for COVID-19 with Caputo derivative has been analysed by Rezapour, Mohammadi, and Samei [16]. Also, in order to investigate the COVID-19 epidemic model, a way to non-singular fractional derivatives, a case study has been done by Batool, Khan, Li, Junaid, Zhang, Nawaz and Tian [17]. Qazza and Saadeh [18] do an analytical solution of fractional SIR model.

2. Mathematical formulation

2.1. Preliminaries:

2.1.1. Definition [19]: "*The Caputo's fractional derivative of order ρ can be defined as*

$${}_0^C D_t^\rho = \frac{1}{\Gamma(\rho-n)} \int_a^t \frac{f^{(n)}(\tau)d\tau}{(t-\tau)^{\rho+1-n}}, \quad (n-1) < \rho < n.$$

$$Here, \Gamma \text{ is the Gamma function.}$$

Under natural conditions on the function f(t), for $\rho \to n$ the Caputo derivative becomes a conventional n^{th} derivative of the function f(t)".

2.1.2.Generalized mean value theorem [20]: *Suppose that $f(x) \in C[a,b]$ and $D_a^\rho f(x) \in C[a,b]$, for $0 < \rho \leq 1$, then we have,*

$$f(x) = f(a) + \frac{1}{\Gamma(\rho)}\left(D_a^\rho f\right)(\xi).(x-a)^\rho$$

With $a \leq \xi \leq x, \forall x \in (a,b]$.

2.1.3. Lemma 1[21] : *Consider the following fractional-order system,*

${}^C D_t^\rho\left(Y(t)\right) = \phi(Y), Y_{t_0} = (y_{t_0}^1, y_{t_0}^2, \dots\dots\dots\dots\dots\dots, y_{t_0}^n),\ y_{t_0}^j, j=1,2,3,\dots\dots\dots,n$

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

with $0 < \rho < 1, Y(t) = \left(y^1(t), y^2(t), \ldots\ldots\ldots\ldots, y^n(t)\right)$ *and* $\phi(Y): [t_0, \infty) \to \mathbb{R}^{n\times n}$. *For* $\phi(Y) = 0$, *we get all the equilibrium points are locally asymptotically stable iff each eigenvalue* λ_j *of the jacobian matrix* $J(Y) = \frac{\partial(\phi_1, \phi_2, \ldots\ldots\ldots, \phi_n)}{\partial(y^1, y^2, \ldots\ldots\ldots y^n)}$ *calculated at the equilibrium points satisfies* $|arg\ (\lambda_j)| > \frac{\rho\pi}{2}$.

2.1.4. Lemma 2[22] : *Let* $h(t) \in \mathbb{R}^+$ *be a differential function. Then, for any* $t > 0$,

${}^{C}D_t^{\rho}\left[h(t) - h^* - h^* ln\frac{h(t)}{h^*}\right] \leq \left(1 - \frac{h^*}{h(t)}\right){}^{C}D_t^{\rho}\left(h(t)\right), \quad h^* \in \mathbb{R}^+, \forall \rho \in (0,1).$

We, here, discuss the useful framework of SICS (Susceptible- Infectious- Countermeasures- Susceptible) to understand the dynamics of cyberattacks and the effectiveness of security measures within a system of interconnected entities, such as financial institutions. The main components of the model are described here-

- S (Susceptible): These are financial institutions or their systems that are now robust yet susceptible to a cyberattack. They remain uncompromised; nonetheless, they exhibit vulnerabilities that a threat could exploit.
- I (Infectious): These refer to financial institutions or their systems that have been effectively breached by a cyberattack. They are now undergoing the attack and may be facilitating its propagation.
- C (Countermeasures): This is a critical state distinctive to the SICS model in this situation. Institutions in this state are those that have enacted or are currently enacting specific countermeasures against cyberattacks. This may entail rectifying vulnerabilities, implementing new security software, isolating affected systems, or initiating incident response protocols. The crucial aspect is their proactive mitigation of the threat.
- S (Susceptible): This facet underscores the cyclic characteristics of cyber threats. Despite the implementation of safeguards, institutions may ultimately regress to a vulnerable condition. This may occur as a result of: Emerging vulnerabilities: Zero-day exploits and software updates that introduce new defects; Advancing assault techniques: Perpetrators continually discover novel tactics to circumvent established protections; Human error: Employees committing errors that re-expose systems; Degradation of countermeasures: Security software is becoming obsolete, and policies are not being implemented.

Now, the model is described by Figure 1 below:

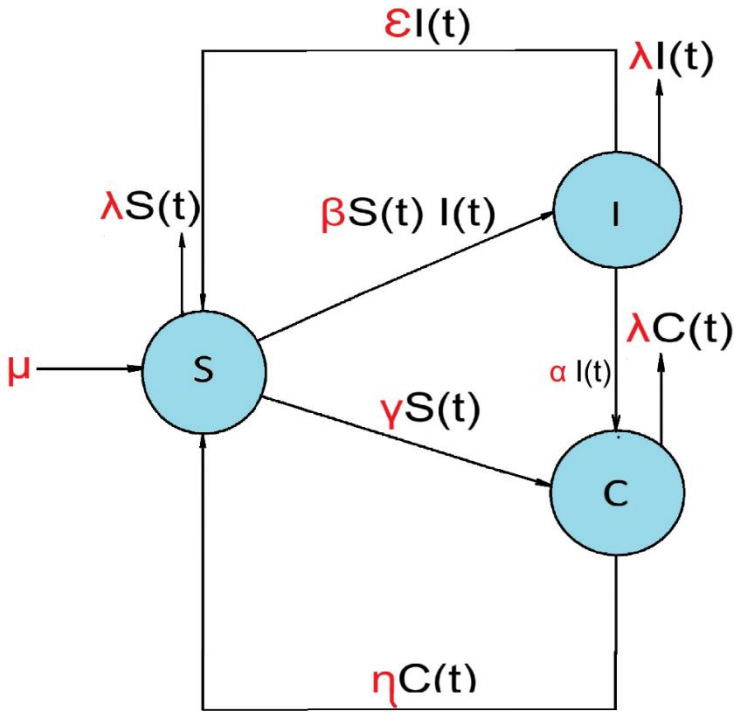

Figure 1: Propagation of malware due to ***cyberattack*** *in* ***financial systems.***

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

The system of linear fractional differential equations of **Caputo order** is given below in accordance with the above figure 1,

$$\left.\begin{aligned} {}_0^C D_t^\rho S(t) &= \mu - \beta S(t)I(t) - (\lambda+\gamma)S(t) + \eta C(t) + \varepsilon I(t) \\ {}_0^C D_t^\rho I(t) &= \beta S(t)I(t) - (\lambda+\alpha+\varepsilon)I(t) \\ {}_0^C D_t^\rho C(t) &= \alpha I(t) + \gamma S(t) - (\lambda+\eta)C(t) \end{aligned}\right\} \quad (1)$$

With initial conditions $S(0) = S_0 > 0, I(0) = I_0 \geq 0, C(0) = C_0 \geq 0$. ${}_0^C D_t^\rho$ is the Caputo fractional operator of order $0 < \rho \leq 1$.

Parameters of the model:

- μ =*Constant rate of recruitment rate of susceptibles*
- β =*Coefficient of transmission between susceptible S(t) and infectious class I(t)*
- λ =*Natural mortality rate*
- ε =*Rate at which Infectious population goes to the susceptible class.*
- α = *Rate at which Infectious population goes to the countermeasure class*
- γ =*Rate at which susceptible class goes to the countermeasure class*
- η =*Rate at which countermeasure class of population goes to the susceptible class*

Total population is given by

$$N(t) = S(t) + I(t) + C(t) \quad (2)$$

Then, $${}_0^C D_t^\rho N(t) = \mu - \lambda N(t)$$

$$or, \quad {}_0^C D_t^\rho N(t) = \mu - \lambda N(t) \quad (3)$$

Which implies $N(t) \to \frac{\mu}{\lambda}$ *as* $t \to \infty$.

We study the dynamics of the fractional order SICS model in the biologically feasible set

$$\Omega = \left\{(S,I,C) \in \mathbb{R}^3 \middle| N(t) \leq \frac{\mu}{\lambda}\right\}. \quad (4)$$

Considering (3) as Initial Value Problem(IVP) with initial condition $N(t)|_{t=0}$ =N(0). Applying Laplace transform[19] to (3), we get,

$$L\ [{}_0^C D_t^\rho N(t)] = L[\mu - \lambda N(t)]$$

$$or, \quad s^\rho L[N(t)] - s^{\rho-1}N(0) = \frac{\mu}{s} - \lambda L[N(t)]$$

$$or, \quad L[N(t)] = \frac{s^{\rho-1}}{s^\rho + \lambda}N(0) + \frac{\mu s^{-1}}{s^\rho + \lambda}$$

Applying inverse Laplace transform[19] to the above equation, we get,

$$N(t) = N(0).E_{\rho,1}(-\lambda t^\rho) + \mu t^\rho E_{\rho,\rho+1}(-\lambda t^\rho) \quad (5)$$

According to the properties of Mittag-Leffler function,

$$E_{\rho,\alpha}(z) = z.E_{\rho,\rho+\alpha}(z) + \frac{1}{\Gamma(\alpha)}$$

We get from (4),

$$N(t) = \left(N(0) - \frac{\mu}{\lambda}\right)E_{\rho,1}(-\lambda t^\rho) + \frac{\mu}{\lambda}$$

Thus, $$\lim_{t\to\infty} Sup\ N(t) \leq \frac{\mu}{\lambda}$$

Hence, the model is bounded above and $S(t), I(t), C(t)$ are all non-negative and the model is non-negative invariant.

3. Reproduction Number

The threshold parameter for the system (1) is obtained by using second generation matrix and given by

$$R_0 = \frac{\beta S_0}{(\lambda+\alpha+\varepsilon)} \quad (6)$$

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

4. Equilibrium

4.1. Disease-free equilibrium: The disease-free equilibrium(DFE) is found by equating all equations of system (1) to zero and $S(0) = S_0, \quad I(0) = 0, \quad C(0) = 0$, We get,

DFE: $(S_0, 0, 0) = \left(\frac{\mu}{\lambda}, 0, 0\right)$

Showing no infection in the environment, nodes are susceptibles only.

4.2. Endemic equilibrium: Endemic equilibrium (EE) is given by equating all equations of system (1) to zero and

S(t)=S*, I(t)=I*, C(t)=C*, where S*, I*, C*∈ $\mathbb{R}^+$.

EE: $S^*=\frac{(\lambda+\alpha+\varepsilon)}{\beta}$;

$I^* = \frac{((\lambda+\gamma)S^*-\mu)(\lambda+\eta)-\gamma\eta S^*}{\eta\alpha-(\beta S^*-\varepsilon)(\lambda+\eta)}$;

$C^* = \frac{((\lambda+\gamma)\alpha-\gamma\beta S^*+\gamma\varepsilon)S^*-\mu\alpha}{\eta\alpha-(\beta S^*-\varepsilon)(\lambda+\eta)}$;

4.3. Theorem: The disease free equilibrium (DFE) is locally asymptotically stable if R_0<1, otherwise not stable.

Proof: For the disease free equilibrium(DFE), $\left(\frac{\mu}{\lambda}, 0, 0\right)$, the Jacobian matrix for the system (1) is given as-

$$J_{DFE} = \begin{pmatrix} -\lambda-\gamma & -\beta S_0+\varepsilon & \eta \\ 0 & \beta S_0-(\lambda+\alpha+\varepsilon) & 0 \\ \gamma & \alpha & -(\lambda+\eta) \end{pmatrix}$$

Since, $R_0 < 1, hence, \beta S_0 - (\lambda+\alpha+\varepsilon) < 1$, using (6).

The eigenvalues are here: $q_1 = -(\lambda+\gamma);\ q_2 = -(\lambda+\eta); and\ q_3 = \beta S_0 - (\lambda+\alpha+\varepsilon)$, are all negative. Hence, by Fractional Routh-Hurwitz criteria [22], all the roots follow-

$$|\arg(q_i)| > \frac{\rho\pi}{2}; i = 1,2,3 \quad and \quad 0 < \rho < 1.$$

4.4. Theorem: If $R_0 > 1$, then the endemic equilibrium is locally asymptotically stable.

Proof: For the endemic equilibrium, the Jacobian for the system (1) is given as

$$J_{EE} = \begin{pmatrix} -\beta I^*-(\lambda+\gamma) & -\beta S^*+\varepsilon & \eta \\ \beta I^* & \beta S^*-(\lambda+\alpha+\varepsilon) & 0 \\ \gamma & \alpha & -(\lambda+\eta) \end{pmatrix}$$

Which gives rise to the characteristic equation as

$x^3 + A_1x^2 + A_2x + A_3 = 0$

Where,

$A_1 = 3\lambda+\alpha+\varepsilon-\beta S^*+\beta I^*+\gamma+\eta;$

$A_2 = (\lambda+\alpha+\varepsilon-\beta S^*)(\lambda+\beta I^*+\gamma)+(2\lambda+\beta I^*+\gamma+\alpha+\varepsilon-\beta S^*)(\lambda+\eta)+\beta^2 S^* I^*-\gamma\eta;$

$A_3 = (\lambda+\alpha+\varepsilon-\beta S^*)(\lambda+\beta I^*+\gamma)(\lambda+\eta)+\beta\eta^2 I^*-\beta\varepsilon I^*(\lambda+\eta)-\eta\gamma(\lambda+\alpha+\varepsilon-\beta S^*);$

Let us denote its discriminant

$$\Delta = 18A_1A_2A_3 + (A_1A_2)^2 - 4{A_2}^3 - 4{A_1}^3A_3 - 27{A_3}^2$$

The following lemma will complete our proof of the theorem.

4.4.1. Lemma 3: Assume that $R_0 > 1$ and one of the following conditions are satisfied

(i). $\Delta > 0, A_1 > 0, A_2 > 0, and\ A_1A_2 - A_3 > 0.$

(ii). $\Delta < 0, \rho \in \left(0, \frac{2}{3}\right], A_1 \geq 0, A_2 \geq 0, and\ A_3 > 0.$

Then, endemic equilibrium of the fractional order model with Caputo derivative is locally asymptotically stable.

Proof: The detailed proof of this lemma is similar to that of [22].

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

4.5. Global stability of endemic equilibrium

Let us construct a Lyapunov function as

$$L(t) = I(t) - I^* - I^* \ln \frac{I(t)}{I^*} \quad (7)$$

Taking derivative both sides of equation (7), and using lemma (2), we get,

$${}_0^cD_t^\rho L(t) \leq \left(1 - \frac{I^*}{I(t)}\right) {}_0^cD_t^\rho I(t),$$

Using endemic conditions in above equation, we have

$$or, \quad {}_0^cD_t^\rho L(t) \leq \frac{I(t) - I^*}{I(t)} [\beta(S(t)I(t) - S^*I^*) - (\lambda + \alpha + \varepsilon)(I(t) - I^*)]$$

$$or, \ {}_0^cD_t^\rho L(t) \leq -\frac{(I(t)-I^*)^2}{I(t)} \left[(\lambda + \alpha + \varepsilon) - \frac{\beta}{(I(t)-I^*)}(S(t)I(t) - S^*I^*)\right] \quad (8)$$

$If\ R_0 > 1, then,\ {}_0^cD_t^\rho L(t) < 0, from\ (8)$. Therefore, EE$(S^*, I^*, C^*)$ is globally asymptotically stable, according to LaSalle's invariance principle[23-26].

5. Sensitivity Analysis and Discussion

Sensitivity analysis is a way to determine the importance of each parameter for the disease transmission. The sensitivity index of R_0 with respect to x is defined as

$$\Gamma_x^{R_0} = \frac{\partial R_0}{\partial x} \frac{x}{R_0}$$

The sign of each index makes it possible to know whether the parameter increases (positive sign) or decreases (negative sign) the value of R_0 [3]. The parameters here for this model are-

$\beta, \mu, \lambda, \varepsilon, \alpha, \gamma, \eta$. We have,

$\Gamma_\beta^{R_0} = 1;$

$\Gamma_\mu^{R_0} = 1;$

$\Gamma_\lambda^{R_0} = \frac{1}{\alpha+\varepsilon}\left[\frac{\lambda^2}{\lambda+\alpha+\varepsilon} - (\lambda + \alpha + \varepsilon)\right];$

$\Gamma_\varepsilon^{R_0} = -\frac{\varepsilon}{\lambda+\alpha+\varepsilon};$

$\Gamma_\alpha^{R_0} = -\frac{\alpha}{(\lambda+\alpha+\varepsilon)};$

$\Gamma_\gamma^{R_0} = 0;$

$\Gamma_\eta^{R_0} = 0;$

Note that R_0 does not depend upon η, γ, so,

$\Gamma_\eta^{R_0} = 0$, $\Gamma_\gamma^{R_0} = 0$. We have found here that , $\Gamma_\alpha^{R_0}, \Gamma_\lambda^{R_0}, \Gamma_\varepsilon^{R_0} < 0$, which means that an increment in $\alpha, \lambda, \varepsilon$, will cause R_0 to decrease. Also, $\Gamma_\mu^{R_0}, \Gamma_\beta^{R_0} > 0$, cause R_0 to increases

Example 1: The fractional-order simulation of the epidemic model using the Adams–Bashforth–Moulton method for the Caputo derivative with order ρ=0.9 is performed.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

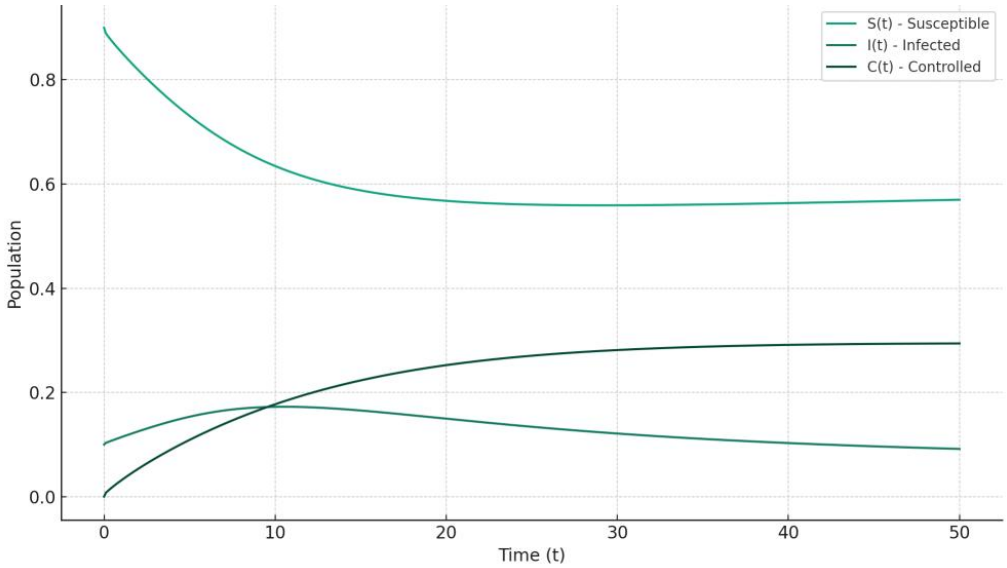

Figure 2: ***Fractional-order*** *using the* ***Adams–Bashforth–Moulton method*** *for the Caputo derivative with order ρ=0.9*

From figure 2, susceptible S (t) declines gradually over time due to infection and transition into control; infected I (t) initially rises due to the transmission, peaks, and then decreases as more individuals move to the controlled class or die; controlled C(t) increases steadily, representing individuals either isolated from the susceptible class or recovered and moved to control.

Example 2: Comparison the fractional-order model ρ=0.9 with the integer-order model ρ=1.0

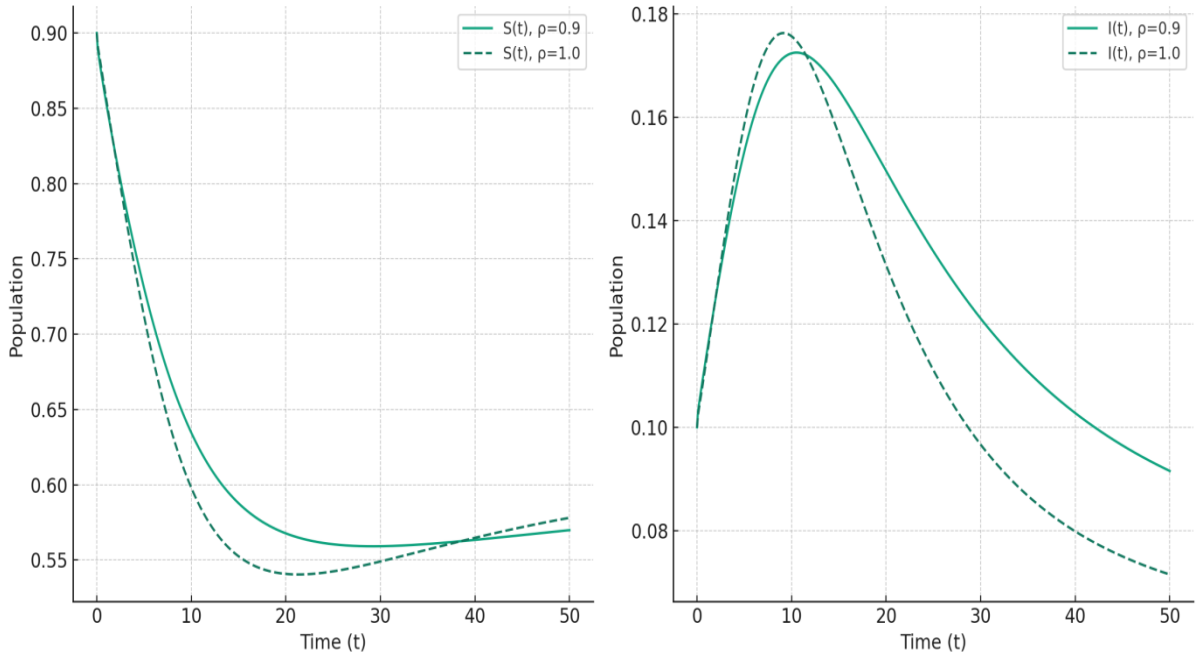

Figure 3: Comparison the fractional-order model ρ=0.9 with the integer-order model ρ=1.0 for S(t) and I(t) compartment

From figure 3, it is evident that the fractional model shows slower decay in infection and more persistent memory effects in the population dynamics, whereas, the integer model responds faster, reaching equilibrium more quickly.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Example 3: Sensitivity of the infected population I(t) with respect to variations in the transmission rate β, under fractional-order dynamics ρ = 0.9
From figure 4, it is evident that higher β values (0.5, 0.6) cause a faster and more intense rise in infections, lower β values (0.2, 0.3) slow down the outbreak and reduce the peak infection.

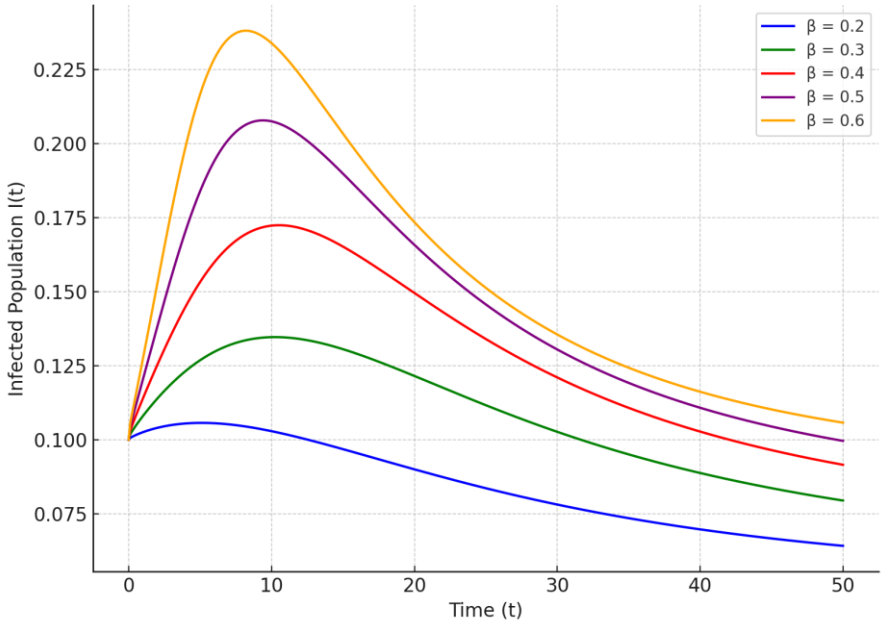

Figure 4: *Sensitivity of the infected population I(t) with respect to variations in the transmission rate β, under fractional-order dynamics ρ=0.9*

Example 4: When peak infected population I(t) varies with different values of the transmission rate β
From figure 5 it is evident that as β increases, the peak infection level increases sharply. This confirms that even small increases in the transmission rate can significantly intensify the epidemic's severity. Fractional-order systems capture these dynamics with more realism due to memory effects.

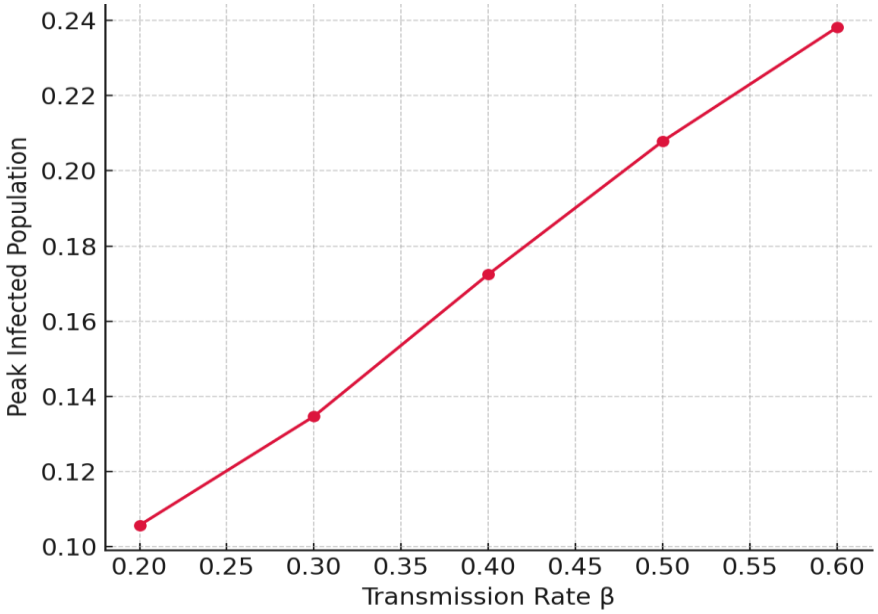

Figure 5: Peak infected population I(t) verses transmission rate with ρ=0.9

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

The parameter sensitivity analysis has been successfully performed which is given in Table 1 and its simulation is depicted in figure 5(a) and 5(b)

.

Parameter	*Value*	*Peak I(t)*	*Total Infected*
β	0.2	0.1057	4.26
β	0.4	0.1725	6.55
β	0.6	0.2382	7.91
α	0.05	0.2339	9.45
α	0.2	0.1162	4.05
γ	0.01	0.2118	7.99
γ	0.2	0.1243	4.27

From the parametric values (Table 1) and simulation (figures 5a, and 5b) we observe that:

a. **Transmission rate β**: Higher β leads to significantly higher peak and total infections.
b. **Isolation rate α**: Higher α (better isolation) sharply reduces infections.
c. **Precautionary control γ**: Higher γ (more proactive control) also reduces spread effectively.

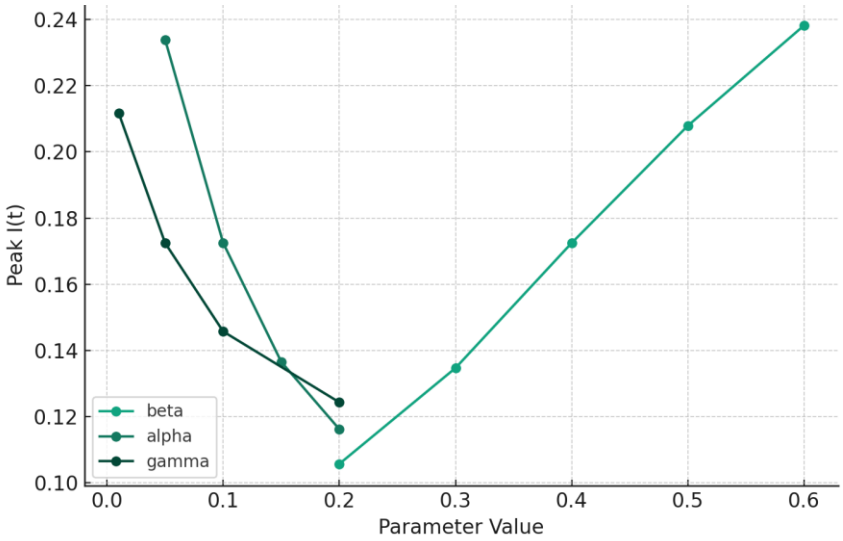

Figure 5(a): Peak Infected I(t) verses Parameter value

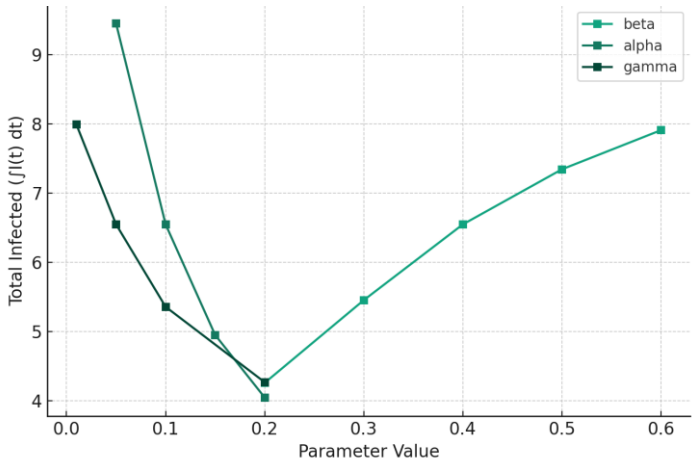

Figure 5(b): Total Infected I(t) verses Parameter value

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

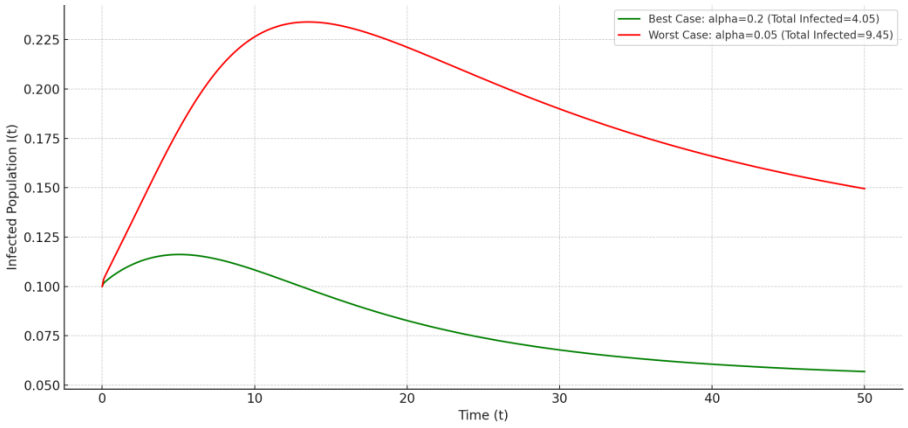

Figure 6: Comparison of the infected population I(t) over time

Figure 6 depicts the best-case and worst-case of the infected population I(t) over time t. When the isolation rate is high $\alpha = 0.2$, it leads to a low and short-lived infection peak with total infected ~4.05. When the isolation rate is low $\alpha = 0.05$, it leads to a high and prolonged infection curve with total infected ~9.45. This clearly highlights the critical role of increasing isolation efforts (α) in controlling epidemics.

6. Conclusion

This study presents a novel fractional-order SICS epidemic model to explore the dynamics of cyberattacks on financial systems, incorporating memory effects and long-range dependencies inherent in real-world cyber-physical networks. By employing Caputo fractional derivatives, the model captures the non-Markovian nature of cyber incidents, where the future system state depends not only on its current condition but also on its entire attack-response history.

Numerical simulations using the Adams–Bashforth–Moulton scheme reveal critical insights into the system's sensitivity to parameters such as the transmission rate of cyberattacks (β), the detection/isolation rate (α), and the implementation strength of countermeasures (γ). Comparative analysis between fractional ($\rho = 0.9$) and classical integer-order ($\rho = 1$) models demonstrates that the fractional model more accurately reflects the persistence and delayed response characteristics typical of cyber threats in financial systems.

Sensitivity analysis highlights that increasing α (early detection and containment) and γ (preventive countermeasures) significantly reduce both the peak infection load and the total system compromise. Conversely, higher β (rapid malware propagation or phishing vulnerability) leads to extensive breaches and delayed recovery, underscoring the need for proactive defense strategies.

The proposed fractional SICS model provides a powerful analytical framework for understanding the propagation, impact, and control of cyberattacks within financial ecosystems. The integration of fractional calculus not only enhances modeling accuracy but also enables strategic planning for cyber resilience. This work lays the foundation for future explorations that may include AI/ML-driven adaptive control, real-time anomaly detection, and blockchain-enhanced security protocols within the same modeling paradigm.

References

1. O'Sullivan, Arthur; Sheffrin, Steven M. (2003). Economics: Principles in Action. Upper Saddle River, New Jersey 07458: Pearson Prentice Hall. pp. 551. ISBN 0-13-063085-3.
2. Gurusamy, S. (2008). Financial Services and Systems 2nd edition, p. 3. Tata McGraw-Hill Education. ISBN 0-07-015335-3
3. Baleanu D., Balas V.E., and Agarwal P., "Fractional Order Systems and Applications in Engineering", Academic press, Elsevier, 2023, ISBN: 978-0-323-90953-2.

4. Baskonus H.M., Bulut H., "On the numerical solutions of some fractional ordinary differential equations by fractional Adams-Bashforth-Moulton method", DE GRUYTER, 2015; 13:547-556.
5. Mouaouine A., Boukhouima A., Hattaf K., and Yousfi N., "A fractional order SIR epidemic model with nonlinear incidence rate", Advances in Difference Equations (2018) 2018:160,https://doi.org/10.1186/s13662-018-1613-z.
6. https://www.nist.gov/cyberframework
7. https://ithandbook.ffiec.gov
8. https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661
9. https://www.ibm.com/think/topics/rbac
10. https://www.ibm.com/think/topics/siem
11. Gulyás, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. Procedia Computer Science, 219, 84–90. https://doi.org/10.1016/j.procs.2023.01.267
12. Alqahtani, R.T., Mathematical model of SIR epidemic system (COVID-19) with fractional derivative: stability and numerical analysis. Adv Differ Equ 2021, 2 (2021). https://doi.org/10.1186/s13662-020-03192-w
13. Paul S., Mahata A., Mukherjee S., Roy B., Dynamics of SIQR epidemic model with fractional order derivative. Partial Differential Equations in Applied Mathematics, Volume 5, 2022, 100216, ISSN 2666-8181, https://doi.org/10.1016/j.padiff.2021.100216.
14. Chatterjee A. N., Ahmad B., A fractional-order differential equation model of COVID-19 infection of epithelial cells. Chaos Solitons Fractals. 2021 Jun;147: 110952. Doi: 10.1016/j.chaos.2021.110952. Epub 2021 Apr 30. PMID: 33967407; PMCID: PMC8086832.
15. Sene N., SIR epidemic model with Mittag–Leffler fractional derivative. Chaos, Solitons & Fractals, Volume 137,2020,109833, ISSN 0960-0779, https://doi.org/10.1016/j.chaos.2020.109833.
16. Rezapour S., Mohammadi H. & Samei M.E., SEIR epidemic model for COVID-19 transmission by Caputo derivative of fractional order. Adv Differ Equ 2020, 490 (2020). https://doi.org/10.1186/s13662-020-02952-y
17. Batool H., Khan I., Li W., Junaid M., Zhang J., Nawaz A., Tian L., Fractional modeling and numerical investigations of COVID-19 epidemic model with non-singular fractional derivatives: a case study. Sci Rep. 2025 Apr 17;15(1):13256. doi: 10.1038/s41598-025-93095-1. PMID: 40246880; PMCID: PMC12006423.
18. Qazza A., Saadeh R., On analytical solution of fractional SIR epidemic model. Applied Computational Intelligence and Soft Computing, 2023. 6973734. Wiley Online Library. https://doi.org/10.1155/2023/6973734.
19. Podlubny I. (1999). Fractional Differential Equations. Volume 198, MATHEMATICS IN SCIENCE AND ENGINEERING, Academic press.
20. Odibat, Z. M., & Shawagfeh, N. T. (2007). Generalized Taylor's formula. Applied Mathematics and Computation, 186(1), 286–293. https://doi.org/10.1016/j.amc.2006.07.102
21. Mahata, A., Paul, S., Mukherjee, S., & Roy, B. (2022). Stability analysis and Hopf bifurcation in fractional order SEIRV epidemic model with a time delay in infected individuals. Partial Differential Equations in Applied Mathematics, 5, 100282. https://doi.org/10.1016/j.padiff.2022.100282
22. Ahmed E., El-Sayed, El-Saka Hala A.A., "On some Routh-Hurwitz conditions for fractional order differential equations and their applications in Lorenz, Rössler, Chua and Chen systems", Physics Letters A 358(1):1-4, October 2006.
23. Shuai Z., Van Den Driessche P., "GLOBAL STABILITY OF INFECTIOUS DISEASE MODELS USING LYAPUNOV FUNCTIONS", SIAM J. APPL. MATH, Vol. 73, No. 4, pp. 1513–1532, 2013.
24. La Salle J.P., "The stability of dynamical systems", Soc. Indust. Appl. Math. (1976).
25. Diekmann O., Heesterbeek J.A.P., Roberts M.G., "The construction of next-generation matrices for compartmental epidemic models", J R Soc Interface, 2010 Jun 6;7(47):873-85.
26. Van Den Driessche P., Watmough J., "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission", Math Biosci. 2002 Nov-Dec; 180:29-48.