MODELING TELECOMMUNICATION SUBSCRIBER FRAUD HEALING DYNAMICS USING FRACTIONAL CALCULUS

[1]Ernest Oyemndu Nonum, [2] Patrick Nnaemeka Okafor & [3]Silas Abahia Ihedioha

[1] Department of Electrical and Electronic Engineering, Admiralty University of Nigeria, Delta State, Nigeria
[2] Department of Computing Sciences, Admiralty University of Nigeria, Delta State, Nigeria
[3]Department of Mathematics, Plateau State University, Bokkos, Plateau State, Nigeria
Email: [1]ernest-cyber@adun.edu.ng [2]nnaemekaokafor55@gmail.com [3]silasihedioha@plasu.edu.ng

ABSTRACT

Telecommunication subscriber fraud significantly threatens the financial health and operational integrity of telecom providers. Common forms—such as subscription fraud, bypass fraud, and identity manipulation—exploit system vulnerabilities for unauthorized gains, leading to substantial financial losses, reduced customer trust, and service disruptions. While fraud detection has been widely studied, limited attention is paid to fraud healing dynamics, the process by which networks recover from such incidents. Classical integer-order differential models fail to capture the non-local, memory-dependent nature of fraud recovery. To address this gap, we propose a modeling framework based on fractional calculus, which extends traditional calculus to non-integer orders and effectively models long-memory and hereditary behaviors. We introduce a fractional differential equation (FDE) model specific to fraud recovery in telecom systems, showing its superiority over classical models. Parametric analysis and simulations highlight how detection delays and recovery efforts influence healing. This model supports intelligent, resilient fraud management strategies.

Keywords: Telecommunication Fraud, Healing Dynamics, Fractional Calculus, Recovery Processes, Memory-dependent

INTRODUCTION

The rapid expansion of mobile banking, digital payments, and online financial services—fueled by the integration of telecommunications and financial infrastructures—has introduced new avenues for sophisticated financial fraud. These crimes compromise transaction security and undermine the integrity of telecom-financial ecosystems (Fang et al, 2018; Zhang & Xu, 2020; Jiang et al., 2021). One increasingly prevalent form is SIM swap fraud, where attackers exploit telecom systems to transfer a victim's mobile number to a new SIM card, thereby gaining access to sensitive financial accounts (Sullivan, 2021). Other methods include unauthorized mobile transactions, typically facilitated by stolen credentials or exploited network vulnerabilities (Arora

et al, 2021), as well as phishing and social engineering, which manipulate users into divulging confidential information (Smith et al, 2020).

These fraudulent activities inflict substantial costs on stakeholders. Telecom service providers absorb losses related to financial reimbursement, fraud investigation, and infrastructure upgrades (Ribeiro et al., 2016), while reputational damage erodes customer trust and market position (Zhao et al., 2022). Victims of fraud suffer financial losses, psychological stress, and long recovery periods (Gao et al., 2020).

Prior Studies on Detection and Vulnerabilities

A considerable body of literature has focused on the detection of telecommunication fraud, with a growing emphasis on adapting to emerging fraud techniques. Fadlullah et al. (2017) conducted a comparative survey of intrusion detection systems (IDS) in telecommunications. Their work catalogued various forms of fraud—such as toll fraud, IRSF, and call spoofing—and emphasized the vulnerability of network architectures. While methodologically robust, relying on comparative analysis and empirical insights, their study primarily focused on detection rather than system recovery.

Ahmed et al. (2016) reviewed anomaly detection techniques, employing statistical and early machine learning methods to classify and detect fraudulent behaviors in network data streams. Their findings highlighted the limitations of static rule-based systems and advocated for adaptive techniques. Building on this, Bamisile et al. (2022) developed an ensemble machine learning model tailored for telecom fraud detection. Their model improved detection accuracy and reduced false positives using a hybrid of supervised learning algorithms. However, none of these studies examined how systems recover post-fraud or how recovery can be modeled dynamically and mathematically.

Cheng et al. (2018) and Chen et al. (2020) echoed these concerns, emphasizing the inadequacy of traditional rule-based detection systems. They showed through simulation and real-time testing that such systems often result in high false-positive rates and lack responsiveness to evolving fraud tactics. Kumar et al. (2021) further demonstrated that fraud patterns adapt faster than conventional detection systems can evolve, reinforcing the need for models that not only detect but also respond and adapt over time. Ezema et al, (2018) examined the depth financial fraud in commercial banks and proposed the use of management information system to improve the performance of commercial banks.

Underexplored Phase: Fraud Healing Dynamics

Although fraud detection has been extensively studied, fraud recovery—or fraud healing dynamics—remains underexplored. Post-fraud recovery involves multiple interconnected processes, including financial restitution, operational stabilization, reputational repair, and customer trust restoration. The International Telecommunication Union (ITU) has called for global action through detection guidelines, inter-operator cooperation, and system resilience measures. However, there is a noticeable absence of quantitative models that simulate the recovery process in affected systems.

Smith et al. (2020) reviewed cyber-resilience strategies and advocated for the inclusion of recovery-aware system architectures, yet they did not provide mathematical frameworks or simulation models capable of capturing dynamic post-fraud behaviors. Their policy-based approach lacked the quantitative specificity necessary for real-time application or optimization.

Limitations of Traditional Modeling Frameworks

Modeling recovery in complex systems has typically relied on integer-order differential equations. These models assume that system dynamics depend solely on current state variables, neglecting the impact of past states—a significant shortcoming in systems with memory and delay characteristics. Mainardi (2010) pointed out that such models fail to accurately describe systems in which recovery depends not only on immediate actions but also on historical exposures and interventions.

This deficiency is particularly evident in financial and network systems, where past disruptions often influence future states through latent effects. Hence, there is a need for a modeling approach that incorporates these memory-driven dependencies.

Emergence of Fractional Calculus for Modeling Memory-Dependent Systems

Fractional calculus, which generalizes classical calculus to allow non-integer (fractional) derivatives and integrals, addresses the aforementioned limitations. Pioneered by Podlubny (1999) and further developed by Magin (2006), fractional differential equations (FDEs) have proven effective in modeling systems where long-term memory and non-local interactions are intrinsic.

Bagley and Torvik (1983) applied FDEs to viscoelastic materials, capturing how historical stress influences present strain. Magin (2006) used fractional models to describe biomedical systems, such as soft tissues that respond to accumulated mechanical loads over time. In finance, Cartea and del Castillo-Negrete (2007) demonstrated that FDEs more accurately describe anomalous diffusion in option pricing models, capturing effects like volatility clustering and persistent trends—features overlooked by classical models. Similarly, Diethelm (2013) used FDEs to model the spread of epidemics, showing how infection progression is affected by long-term memory and population response inertia.

These successes suggest that fractional calculus can be equally powerful for telecommunication fraud recovery, where recovery rates and system stabilization are affected by both immediate interventions and the accumulated effects of past disruptions.

Foundational Work on Network Memory and Historical Influence

Tarasov (2011) extended fractional calculus to networked systems, highlighting how delayed and cumulative responses can be modeled using fractional-order dynamics. Zayernouri and Karniadakis (2013) proposed spectral methods for solving fractional Sturm–Liouville problems, demonstrating the enhanced accuracy of FDEs in capturing memory-governed dynamics in real-world systems.

Despite these promising advances, no prior study has explicitly applied fractional differential equations to model post-fraud recovery in telecommunications. This gap presents a crucial opportunity for mathematical innovation in fraud resilience modeling.

Research Gap and Study Contribution

From the review above, the following gaps are clear:

1. Most studies emphasize fraud detection without addressing system recovery.
2. Dynamic modeling of post-fraud healing has not been attempted, particularly using memory-sensitive tools.
3. Although fractional calculus is well-established in other domains—such as viscoelasticity, finance, and epidemiology—it has not been applied to model recovery in telecommunication fraud.

This study fills these gaps by proposing a fractional differential equation (FDE) model for telecommunication subscriber fraud healing dynamics. The model captures memory effects

embedded in post-fraud recovery processes, models nonlinear, delayed system responses to interventions, simulates interactions among financial, operational, and reputational recovery domains, enables forecasting of long-term impacts and optimization of response strategies and offers a resilient, flexible modeling framework adaptable to evolving threat landscapes.
By introducing this novel approach, the study contributes both a theoretical advancement in recovery modeling and a practical tool for designing robust, intelligence-driven fraud management strategies in the telecom sector.

METHODOLOGY

2.1. Fundamentals of Fractional Calculus

2.1.1. Caputo and Riemann-Liouville Derivatives

Riemann-Liouville Derivative: The Riemann-Liouville (RL) fractional derivative is one of the earliest definitions of fractional derivatives and is widely used in fractional calculus. It is defined as a generalization of the integer-order derivative to non-integer orders. The RL derivative of order α of a function $f(t)$ is given by:

$$D^{\alpha}f(t) = \frac{1}{\Gamma(n-\alpha)}\frac{d^n}{dt^n}\int_0^t \frac{f(\tau)}{(t-\tau)^{\alpha+1-n}}d\tau, \quad (1)$$

where Γ is the Gamma function, and n is the smallest integer greater than α. The RL derivative captures the cumulative memory effect of the system and is suitable for describing processes with historical dependence.

2.1.2. Caputo Derivative: The Caputo fractional derivative is a more practical definition often used in applications where initial conditions are given in terms of integer derivatives. It is defined as;

$$D^{\alpha}f(t) = \frac{1}{\Gamma(n-\alpha)}\int_0^t \frac{f^n(\tau)}{(t-\tau)^{\alpha+1-n}}d\tau, \quad (2)$$

where $f^n(\tau)$ represents the $n-th$ order derivative of $f(t)$ and α is the fractional order. The Caputo derivative is particularly advantageous when dealing with initial value problems, as it allows the system to start from a non-zero initial state, unlike the Riemann-Liouville derivative which requires the system to begin at zero.

2.2. Relevance to Modeling Systems with Memory and Hereditary Behavior

The Caputo and Riemann-Liouville derivatives are crucial in modeling systems that exhibit memory and hereditary behavior, which are common in real-world phenomena such as material properties, biological processes, and fraud recovery dynamics.

i. **Memory and Hereditary Behavior**: Systems with memory have a state that depends not only on the current value but also on past states. For instance, in fraud recovery, the system's recovery depends on previous fraud incidents and actions taken, leading to delayed responses. The fractional derivatives naturally model such systems, where the influence of past events diminishes over time but does not vanish entirely, reflecting the system's memory.

ii. **Fractional Derivatives in Modeling**: The fractional order in both the Caputo and Riemann-Liouville derivatives allows for the representation of systems where the future state is influenced by the entire history of the system, rather than just the current state. This makes fractional calculus an ideal tool for modeling the long-term, non-local interactions

in systems like telecom fraud recovery, where the past fraud events continuously influence the system's behavior and recovery path.

Podlubny (1999) highlighted the significance of fractional calculus in modeling systems with memory, pointing out that fractional derivatives enable the modeling of processes that cannot be accurately described by integer-order differential equations. These fractional models provide a more accurate depiction of complex systems that exhibit delayed responses and long-term dependencies, making them indispensable in fields such as engineering, finance, and biology.

2.3. Formulation of the Model

Let $S(t)$ denote the total number of legitimate subscribers, $F(t)$ the number of fraudulent subscribers, and $D(t)$ the cumulative number of detected fraudulent activities at time t, then the dynamics of $S(t)$, $F(t)$, and $F(t)$, are represented as a coupled fractional differential system:

$$\left.\begin{aligned} D_t^{\alpha} S(t) &= r(t)\, S - \beta S(t) F(t), 0 < \alpha < 1, \\ D_t^{\alpha} F(t) &= \beta S(t) F(t) - \gamma F(t) - \delta F(t), \\ D_t^{\alpha} D(t) &= \delta\, F(t) \end{aligned}\right\}, \qquad (3)$$

where

D_t^{α}:is the Caputo fractional derivative of order .

r: Legitimate subscriber growth rate.

β: Fraud rate (rate at which legitimate subscribers become fraudulent).

γ: Rate of fraud termination due to deterrence or voluntary stopping.

δ: Detection rate (proportion of fraudulent activities detected).

with the initial conditions,

$$\left.\begin{aligned} S(0) &= S_0 \\ F(0) &= F_0 \\ D(0) &= 0 \end{aligned}\right\}, \qquad (4)$$

where $S_0$and F_0 are the initial numbers of legitimate and fraudulent subscribers, respectively. The initial conditions as stated in equation (4) show that at time $t = 0$, the system starts with S_0 legitimate subscribers, F_0 fraudulent subscribers, and no detected fraud D_0.

In the system of equations given in equation (3), each equation represents the evolution of a variable over time:

(i) Legitimate Subscriber Dynamics, $S(t)$: $D_t^{\alpha} S(t) = r\, S(t) - \beta S(t) F(t)$. The first term $rS(t)$represents the natural growth of legitimate subscribers, assuming a baseline growth rate r. The second term $\beta S(t) F(t)$ represents the conversion of legitimate subscribers into fraudulent subscribers, where β is the fraud rate, measuring how frequently legitimate users engage in fraudulent activities. The term $S(t) F(t)$ represents an interaction term, implying that fraud increases when there are both more legitimate users and more existing fraudsters influencing them.

(ii) Fraudulent Subscriber Dynamics, $F(t)$: $D_t^{\alpha} F(t) = \beta S(t) F(t) - \gamma F(t) - \delta F(t)$. The first term $\beta S(t) F(t)$ represents the recruitment of new fraudulent subscribers from the legitimate subscriber base. The second term $\gamma F(t)$ accounts for fraud termination due to deterrence measures, such as stricter policies, penalties, or voluntary stopping by fraudsters. The third term $\delta F(t)$ represents fraud detection and removal, where $\delta$is the detection rate.

(iii) Cumulative Detected Fraud, $D(t)$: $D_t^{\alpha} D(t) = \delta F(t)$. This equation simply accumulates the number of detected fraud cases over time. The right-hand side $\delta F(t)$states that the detection rate is proportional to the number of fraudsters in the system. Since $D(t)$ only increases (it does not decrease over time), it tracks the historical accumulation of fraud cases.

2.4. Justification for Using a Fractional-Order Model

The system employs Caputo fractional derivatives D_t^{α}, where $0 < \alpha < 1$, instead of classical integer-order derivatives. The reason for this is:

i. Long-term memory effects: Subscriber fraud does not evolve instantaneously but depends on past fraudulent activities, deterrence policies, and detection measures.
ii. Anomalous diffusion: Fraudulent activities and their spread follow non-Markovian dynamics, meaning that historical fraud trends significantly impact present fraud occurrences.
iii. Gradual healing process: In classical models, healing (i.e., reduction of fraud) would occur in an exponential manner, whereas in reality, the decline is often more gradual due to persistent fraudulent attempts.

2. 5. Healing Mechanism in the Model

The model incorporates several healing mechanisms for fraud control:

1. Deterrence and Voluntary Fraud Stopping (γ)**:** Represents fraudsters stopping their activities due to legal risks, penalties, or lack of incentives.
2. Fraud Detection and Removal (δ)
   - **i.** Fraudulent subscribers are detected and removed at a rate proportional to the current fraud population.
   - **ii.** The cumulative fraud detection ($D(t)$) helps track system performance over time.
3. Legitimate Subscriber Growth (r): New legitimate subscribers enter the system, which helps dilute the impact of fraud over time.
4. Fractional-Order Memory Effects

   i. Due to the fractional derivative, the healing process does not occur instantaneously but depends on past trends.
   ii. This ensures a more realistic, gradual decline of fraud rather than an unrealistic sudden drop

2.6. Practical Implications

- **i.** This model can be used by telecom regulators and fraud analysts to design better fraud mitigation strategies.
- **ii.** By adjusting parameters (β, γ), telecom companies can simulate different intervention strategies and predict their effectiveness over time.The fractional-order nature allows for better forecasting and long-term fraud trend analysis compared to classical integer-order models. **1. Justification for Using a Fractional-Order Model.** The **Caputo fractional derivatives** D_t^{α}, where $0 < \alpha < 1$, is employed in place of classical integer-order derivatives because of the following reason for this is:

iii. **Long-term memory effects**: Subscriber fraud does not evolve instantaneously but depends on past fraudulent activities, deterrence policies, and detection measures.

iv. **Anomalous diffusion**: Fraudulent activities and their spread follow non-Markovian dynamics, meaning that historical fraud trends significantly impact present fraud occurrences.

v. **Gradual healing process**: In classical models, healing (i.e., reduction of fraud) would occur in an exponential manner, whereas in reality, the decline is often more gradual due to persistent fraudulent attempts.

The fractional differential equation model provides a realistic and dynamic framework for studying telecom fraud healing. It captures both the spread and decline of fraudulent subscribers, incorporating detection, deterrence, and legitimate user growth. The fractional order accounts for memory effects and gradual healing, making it superior to traditional models for practical applications in fraud prevention and telecom security.

The fractional differential equation model provides a realistic and dynamic framework for studying telecom fraud healing. It captures both the spread and decline of fraudulent subscribers, incorporating detection, deterrence, and legitimate user growth. The fractional order accounts for memory effects and gradual healing, making it superior to traditional models for practical applications in fraud prevention and telecom security.

2.7. The Models' Solutions and Graphs

In this segment we present the procedure to obtaining the solution to the problem and the solution.

2.7. 1. The Laplace transform

To solve the equations in (3), we use the Laplace transform to transform the equations to obtain the following;

For fractional derivatives

$D_t^{\alpha} F(t) = \beta S(t)F(t) - \gamma F(t) - \delta F(t)$

we get,

$\mathcal{L}\{D_t^{\alpha} F(t)\} = s^{\alpha}\mathcal{L}\{F(t)\} - s^{\alpha-1}F(0).$ (5)

which gives

$s^{\alpha}\mathcal{L}\{F(t)\} - s^{\alpha-1}F_0 = \beta\mathcal{L}\{S(t)F(t)\} - \gamma\mathcal{L}\{F(t)\} - \delta\mathcal{L}\{F(t)$ (6)

from which we get

$\tilde{F}(s) = \frac{s^{\alpha-1}F(0) + \mathcal{L}\{\beta S(t)F(t)\}}{s^{\alpha}+(\gamma+\delta)}.$ (7)

For

$D_t^{\alpha} S(t) = r(t)S - \beta S(t)F(t)$

we get,

$s^{\alpha}\mathcal{L}\{S(t)\} - s^{\alpha-1}S_0 = r\,\mathcal{L}\{S(t)\} - \beta\mathcal{L}\{S(t)F(t)\},$ (8)

which simplifies to

$\tilde{S}(s) = \frac{s^{\alpha-1}S(0)}{s^{\alpha}-r} - \frac{\beta[\tilde{S}(s)*\tilde{F}(s)}{s^{\alpha}-r}.$ (9)

For the equation

$D_t^{\alpha} D(t) = \delta F(t)$

we get,

$.s^{\alpha}\mathcal{L}\{D(t)\} - s^{\alpha-1}D(0) = \delta\mathcal{L}\{F(t)\}$ (10)

which becomes

$$D(t) = D(0) + \delta\mathcal{L}^{-1}\left(\frac{\widetilde{F(s)}}{s^{\alpha}}\right). \quad (11)$$

The simplification of equation (11) gives

$$\widetilde{D} = \frac{\delta\widetilde{F(s)}}{s^{\alpha}} - \frac{D(0)}{S} \quad (12)$$

2.7. 2.The inverse Laplace transforms

To obtain the values of $F(t)$, $S(t)$, and D(t), we apply the Inverse Laplace transforms to equations (7), (9) and (12) is obtained as given in (a) to (b) below;

(a) $F(t) = F(0)E_{\alpha}(-(\gamma+\delta)t^{\alpha}) + \int_0^t E_{\alpha}(-(\gamma+\delta)(t-\tau)^{\alpha})\beta S(\tau)F(\tau)d\tau$, (13)

(b) $S(t) = S(0)E_{\alpha}(r\,t^{\alpha}) - \beta\int_0^t E_{\alpha}(r\,(t-\tau)^{\alpha})\,S(\tau)F(\tau)d\tau$, (14)

(c) $D(t) = \frac{\delta F_0 t^{\alpha-1}E_{\alpha,2}(-(\gamma+\delta)\,t^{\alpha}}{\Gamma(2-\alpha)}$, (15)

where S_0, F_0 are initial conditions, and r, α, γ, and δ are system parameters.

Equations (13) to (15) containE_{α} and $E_{\alpha,2}$. They are the Mittag-Leffler Functions $E_{\alpha}(z)$ which is defined as

$$E_{\alpha,1}(z) = \sum_{k=0}^{\infty}\frac{z^k}{\Gamma(\alpha k+1)}. \quad (16)$$

The Mittag-Leffler functions are used because they reduce to exponentials when and exhibit power-law decay instead of pure exponential decay, which is more realistic for fraud dynamics.

3. RESULTS AND DISCUSSION

Choosing appropriate values for initial conditions $S_0 = 1.0$, $F_0 = 1.0$ and for system parameters $\alpha = 0.8$ (Fractional order), r = 0.5 (Growth rate for S(t)), and $\gamma = 0.5$ (Parameter in F(t) and D(t)) $\delta = 0.3$ (Parameter in F(t) and D(t)), we plot the graphs as shown below.

These values are chosen to ensure numerical stability and demonstrate the behavior of the Mittag-Leffler function-based solutions and can be adjusted to specific values based on a real-world scenario being handled.

The choice of initial conditions $S_0 = 1.0$and $F_0 = 1.0$ is essentially a normalization or scaling decision, not a physical requirement. They provide a baseline that simplifies comparison and interpretation:

Further reasons for the choice are;

1. **Convenience and Clarity**
   Setting $F_0 = 1.0$ makes the solution $F(t) = F(0)E_{\alpha}(-(\gamma+\delta)t^{\alpha})$ directly reflect the shape and behavior of the Mittag–Leffler function, without extra scaling factors. It's a standard approach when illustrating fundamental properties, allowing one to focus on how parameters like α\alphaα, γ, and δ shape the time-evolution, rather than magnitude.
2. **Analytical Simplicity**
   With $F_0 = 1.0$, the Mittag–Leffler function becomes exactly the solution $F(t)$, which simplifies mathematical manipulation and makes numerical evaluation cleaner.
3. **Physical Interpretation**

If $F(t)$ represents a normalized concentration, probability, or fraction, initial values of 1 are naturally interpretable (e.g., "100%" or "unit amount")
It is absolutely possible to make other choices. In more applied contexts S_0 and F_0 would be set to match initial experimental or measured values:
For example in epidemiological models, S_0 might represent the actual population fraction. In materials science, F_0 could be the initial stress or strain level and in chemical kinetics, F_0 might be the initial reactant concentration.

3.1. The graph of $F(t) = F_0 E_{\alpha,1}(-(\gamma + \delta) t^{\alpha})$:

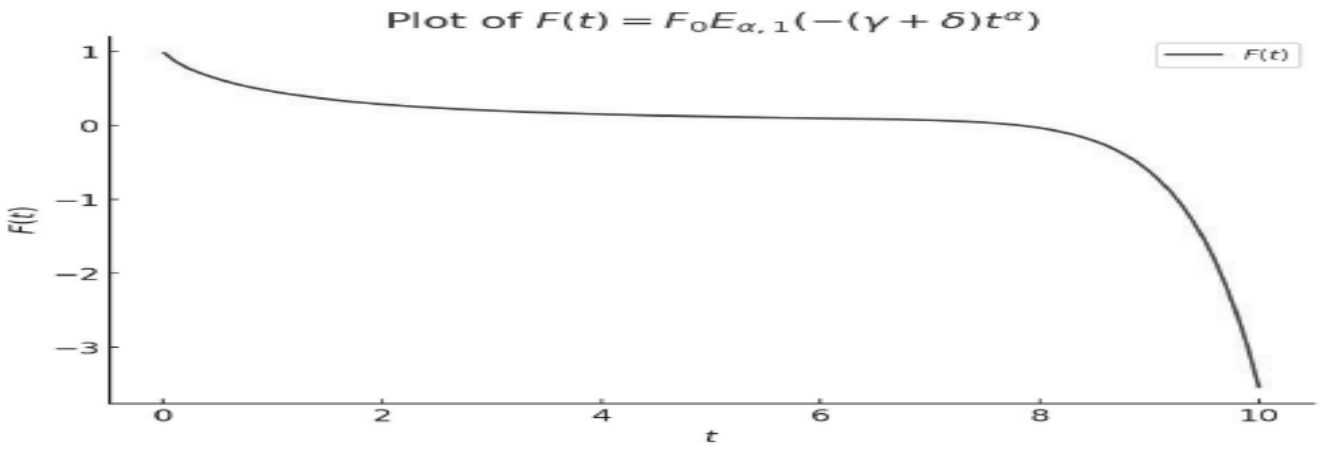

Fig 1: The plot $F(t)$of using a series approximation for the Mittag-Leffler function.

The above plot, fig. 1, illustrates the dynamics of subscriber fraud healing in telecommunications, capturing the transition from initial disruption to eventual system stabilization. It emphasizes the importance of time dependent recovery strategies influenced by fractional-order behavior.
It shows the plot of a function $F(t) = F_0 E_{\alpha,1}(-(\gamma + \delta) t^{\alpha})$, where $E_{\alpha,1}$ is the Mittag-Leffler function, often used in fractional calculus to describe non-exponential decay dynamics. This type of function is well-suited for modeling systems with memory effects and slow recovery processes, such as healing dynamics in telecommunications subscriber fraud.
At $t = 0$, $F(t)$ starts at its maximum value, , representing the initial impact of subscriber fraud, such as a spike in fraudulent activities or monetary loss. The curve's slow decay in the early stages indicates a memory effect, where the system retains the impact of fraud for an extended period. This could correspond to delayed detection and the gradual application of mitigation strategies.
As time progresses, the decline in accelerates, showing that the healing process (fraud mitigation and recovery measures) becomes more effective. This phase might involve stricter regulatory actions or advanced fraud detection algorithms. As $t \to \infty$, $F(t)$ approaches zero, indicating full recovery or stabilization of the system, where the effects of subscriber fraud are minimal or eliminated. α is the rate of healing, with smaller values representing slower recovery processes.
$(\gamma + \delta)$ represents combined system resistance to recovery and the intensity of anti-fraud measures. A higher value indicates a quicker recovery due to effective intervention.

3.2.The graph of $S(t) = S_0 E_{\alpha,1}(r\, t^{\alpha})$:

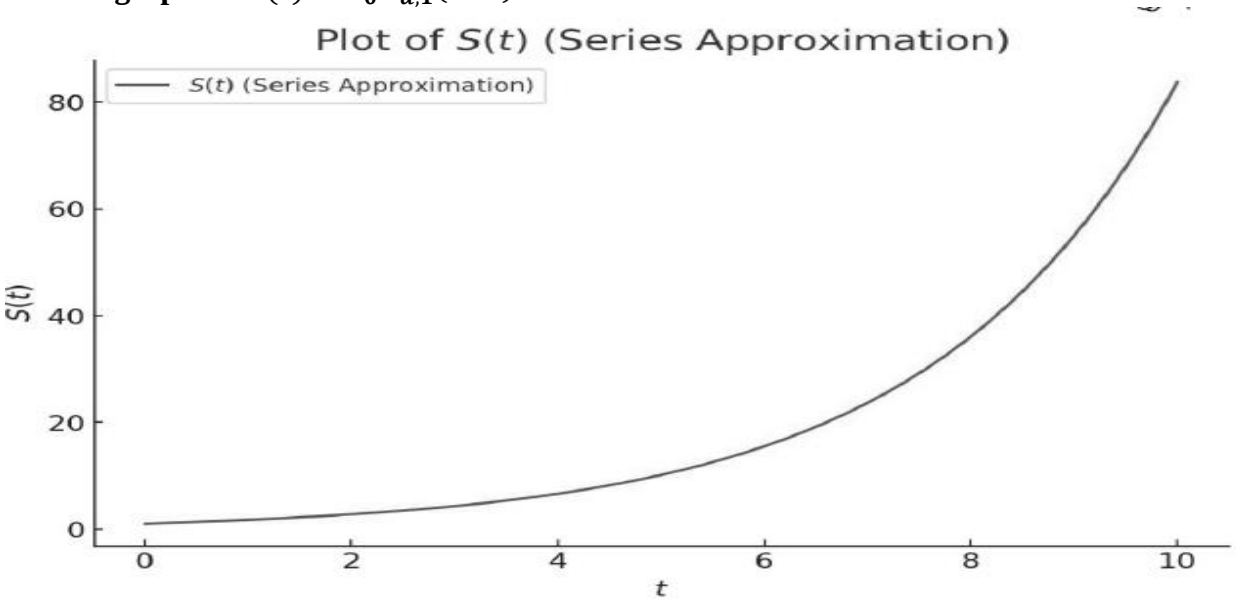

Fig 2: The plot $S(t)$of using a series approximation for the Mittag-Leffler function.

The plot of highlights the cumulative positive impact of healing measures in response to telecommunications subscriber fraud. The exponential-like growth reflects increasing effectiveness over time, underscoring the importance of sustained and scalable interventions.
The upward curve of $S(t)$ indicates an accumulation process. In the context of subscriber fraud healing, this could represent: The cumulative implementation of mitigation measures or restored confidence in the telecommunication system. The gradual return of affected subscribers or growth in legitimate subscribers due to effective fraud management. The use of a series approximation for implies that the system's healing dynamics may be complex and governed by various interacting factors (e.g., market trust, technology adoption, and regulatory compliance).
The initial near-flat portion suggests slow progress in the early stages, possibly due to limited resources or delayed identification of fraudulent activity. For $(t > 5)$, the steeper slope reflects accelerated recovery or improvement dynamics. This phase could be attributed to advanced fraud detection systems, increased enforcement of anti-fraud policies and boosted trust among subscribers.

3.3. The graph of $D(t) = \frac{\delta F_0 t^{\alpha-1} E_{\alpha,2}(-(\gamma+\delta)\, t^{\alpha}}{\Gamma(2-\alpha)}$:

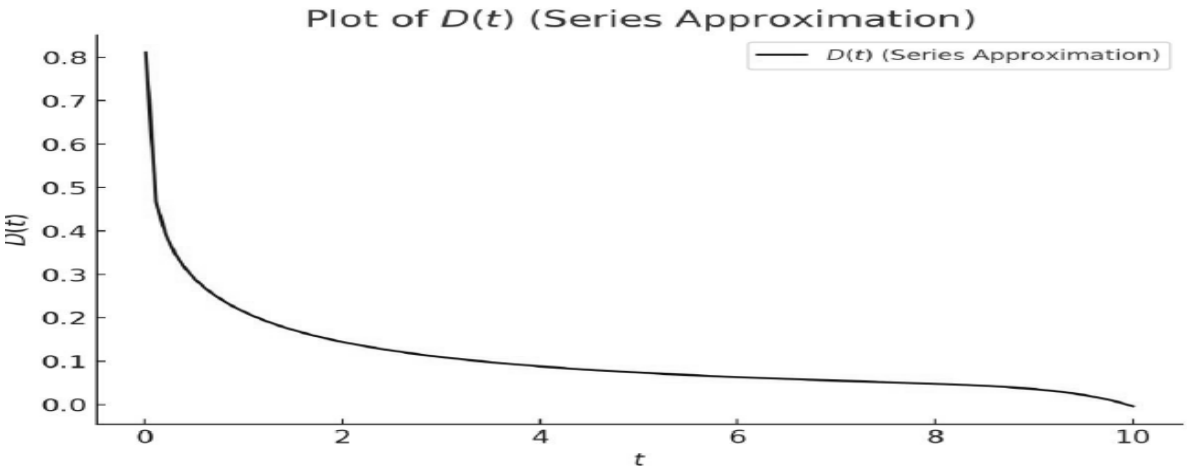

Fig 3: The plot $D(t)$of using a series approximation for the Mittag-Leffler function

The graph depicts the dynamics of $D\,(t)$, which represents the fraud damage level in a telecommunication system over time (t) as it undergoes through healing process.

The graph attains a peak at $t = 0$ which representing the immediate impact of subscriber fraud before any mitigation measures are implemented. This is the period where damage is most significant. $D\,(t)$ decreases over time, indicating the system going through healing process for which one of the following could responsible; detection of fraudulent subscribers, implementation of anti-fraud algorithms or strengthened authentication protocols. As $t \to \infty$, $D\,(t)$, approaches zero, suggesting that the system that the system is getting stabilized and fully recovering from the fraudulent impact.

The graph reflects the effectiveness of fraud-healing strategies. The rapid initial drop in indicates quick mitigation efforts, while the slower long-term decrease suggests ongoing improvements and system resilience.

This trend aligns with the typical process of fraud detection and prevention in telecommunication systems, where initial efforts reduce the most critical damage, followed by gradual stabilization.

Uploaded

Power-Law Decay Functions

Other possible forms of $S(t)$ and $F(t)$ especially for long-term solutions are

$$\left.\begin{aligned} S(t) &= S_0\,(1 + rt^{\alpha})^{\frac{1}{\alpha}} \\ F\,(t) &= F_0\,(1 + (\gamma + \delta)t^{\alpha})^{\frac{1}{\alpha}} \end{aligned}\right\} \qquad (17)$$

These functions model non-instantaneous healing, where $S(t)$ grows in a fractional polynomial manner and $F(t)$decays as a fractional power-law, which is more realistic than exponential decay.

Again applying equation (17) in equation (12) we obtain an approximate value for $D(t)$ as;

$$D(t) \approx \frac{\delta F_0\, t^{1-\alpha}}{(1 + (\gamma + \delta)t^{\alpha})^{\frac{1}{\alpha}}} \qquad (18)$$

3.4.The graph of $\boldsymbol{F(t)\,(t) = F_0\,(1 + (\gamma + \delta)t^{\alpha})^{\frac{1}{\alpha}}}$:

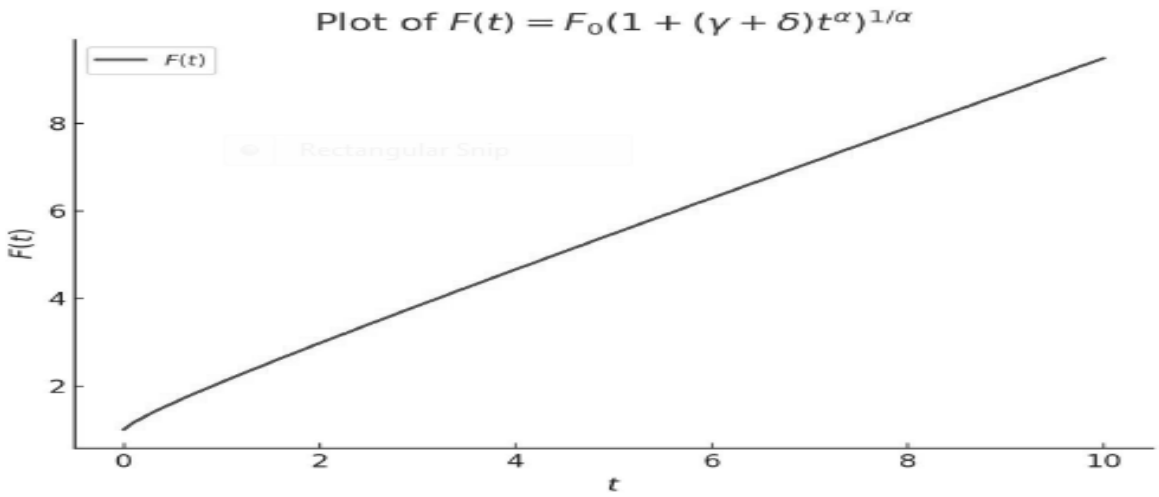

Fig 4: The plot $F(t)$ of using Power-Law Decay Functions

Fig. 4 shows $F(t)$ representing a measure of fraud healing progress or an indicator of system recovery over time (t) in a telecommunication network. $F(t)$ increases rapidly as time progresses, suggesting an accelerating rate of fraud mitigation. This growth reflects improved recovery processes and the system's increasing capacity to address fraudulent activities. At $t = 0$, $F(t)$ starts from a positive value, indicating that some initial measures to counter fraud exist.

The exponential trend could be as result of any of the following; rapid deployment of fraud detection tools, increased effectiveness of machine learning models over time as they adapt to new fraud patterns, continuous investment in subscriber verification and network monitoring.

The graph demonstrates that the healing process gains momentum over time, likely due to learning from early fraudulent activities, integration of feedback mechanisms and adoption of stronger system policies and framework

3.5.The graph of $S(t) = S_0 (1 + rt^{\alpha})^{\frac{1}{\alpha}}$:

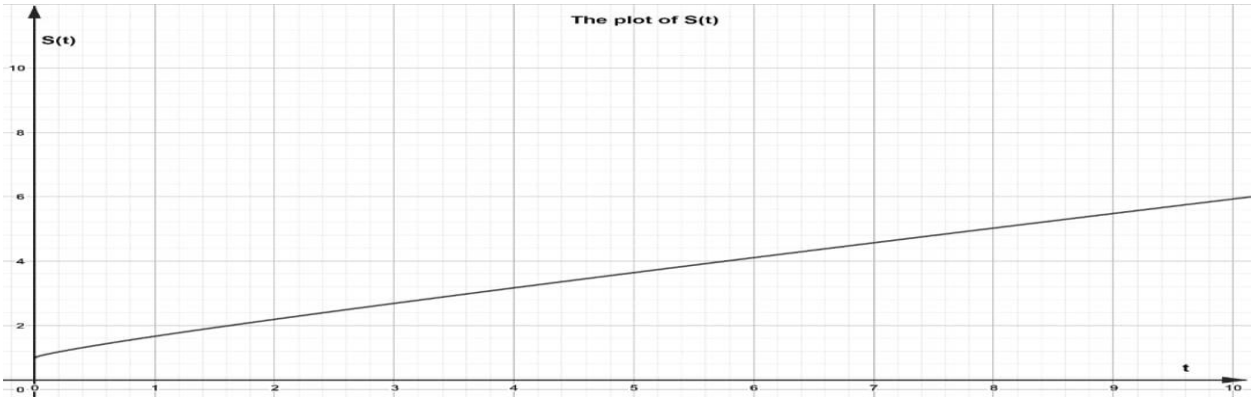

Fig 5: The plot $S(t)$of using Power-Law Decay Functions

The graph represents $S(t)$, which likely denotes the cumulative success or progress in telecommunication subscriber fraud healing over time, $t. S\ (t)$, grows rapidly with time, indicating

that the system's ability to heal from subscriber fraud becomes increasingly effective. This could be attributed to the compounding effects of anti-fraud measures. At $t = 0$, $S(t)$ starts near zero, signifying minimal healing progress before any actions are taken. This aligns with the initiation of mitigation strategies. The steep curvature of at later times reflects enhanced recovery dynamics, possibly due to continuous refinement of fraud detection models, accumulated data improving the system's learning capabilities, and broader implementation of prevention measures (e.g., stricter subscriber verification).

The graph reflects the cumulative effectiveness of fraud-mitigation strategies over time which implies that early actions lay the foundation for stronger future outcomes.

The exponential trend is typical in systems where anti-fraud mechanisms leverage feedback loops. The system becomes better equipped to detect and prevent fraud as more incidents are addressed.

3.6. The graph of $D(t) \approx \frac{\delta F_0\, t^{1-\alpha}}{(1+(\gamma+\delta)t^{\alpha})^{\frac{1}{\alpha}}}$:

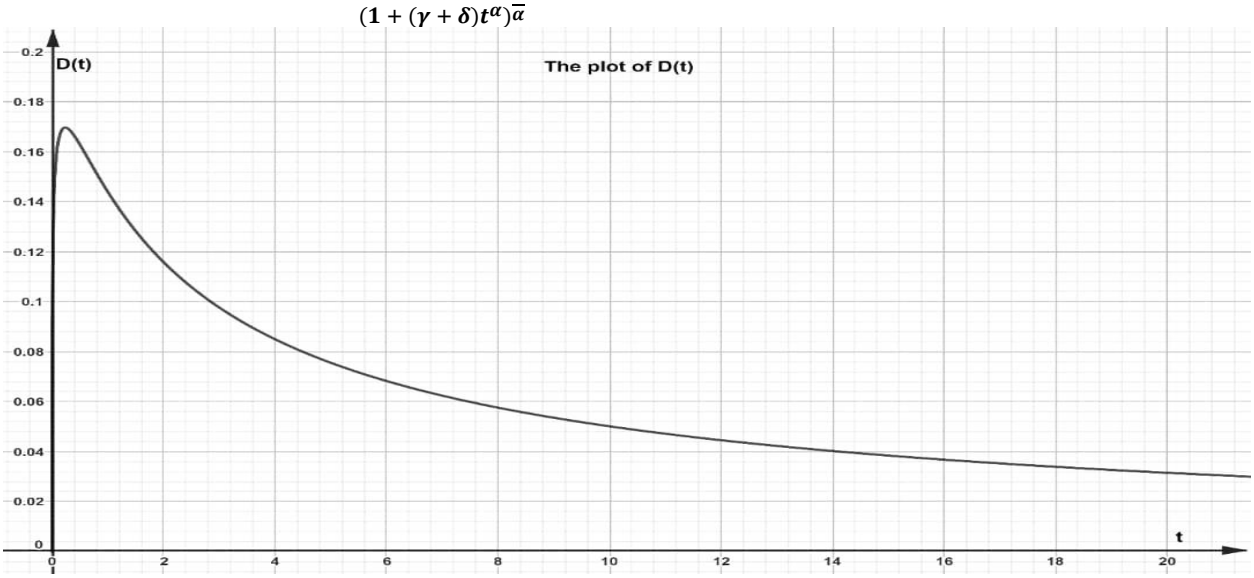

Fig 6: The plot $D(t)$of using Power-Law Decay Functions

The graph fig. 6 depicts the dynamics of $D\,(t)$, which represents the fraud damage level in a telecommunication system over time t as it undergoes healing or mitigation. At $t = 0$, there is a peak in $D\,(t)$, which could represent the immediate impact of subscriber fraud before any mitigation measures are implemented. This is the period where damage is most significant.

Over time $D(t)$, decreases, indicating a healing process in the system which could be warranted by actions such as detection of fraudulent subscribers, implementation of anti-fraud algorithms, and strengthened authentication protocols. As $t \to \infty$, $D\,(t)$, approaches zero, suggesting that the system is getting stabilized and fully recovering from the fraudulent impact.

The graph reflects the effectiveness of fraud-healing strategies. The rapid initial drop in indicates quick mitigation efforts, while the slower long-term decrease suggests ongoing improvements and system resilience. This trend aligns with the typical process of fraud detection and prevention in telecommunication systems, where initial efforts reduce the most critical damage, followed by gradual stabilization.

3.7 Fractional Exponential Decay

For a classical fractional-exponential approximation we have which shows:

$$\left.\begin{aligned} S(t) &= S_0 e^{\frac{r t^{\alpha}}{\Gamma(1+\alpha)}} \\ F(t) &= F_0 e^{-\frac{(\gamma+\delta)t^{\alpha}}{\Gamma(1+\alpha)}} \end{aligned}\right\} \quad (19)$$

where $S(t)$grows exponentially but with a slower rate and $F(t)$ decays exponentially but retains long memory effects. $D(t)$, which accumulates fraud over time smoothly is given by

$$D(t) = \frac{\delta F_0 t^{(1-\alpha)}}{\Gamma(2-\alpha)}. \quad (20)$$

3.7. The graph of $F(t) = F_0 e^{-\frac{(\gamma+\delta)t^{\alpha}}{\Gamma(1+\alpha)}}$:

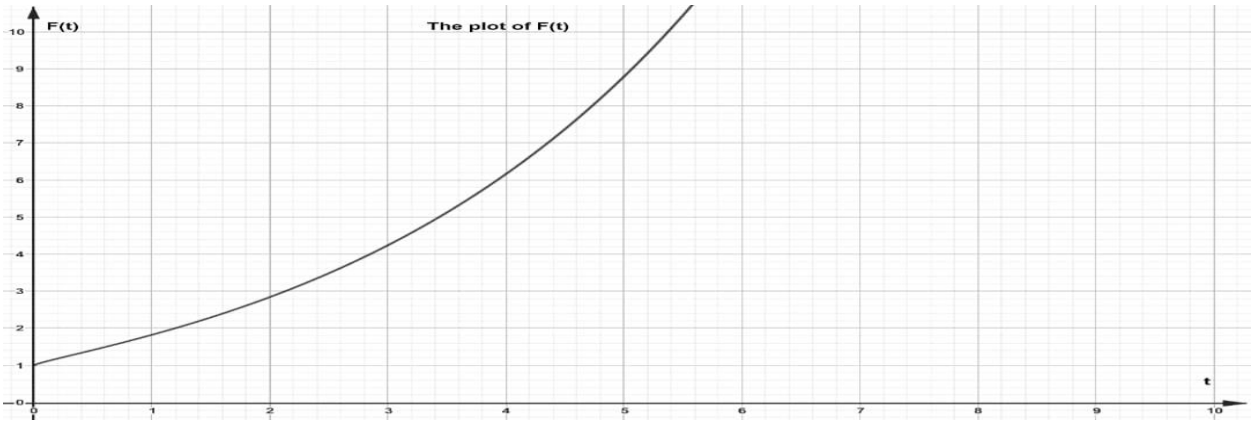

Fig 7: The plot $F(t)$of using Fractional Exponential Decay

The graph depicted in fig.7, represents a measure of fraud healing progress over time $t$in a telecommunication network. $F(t)$, increases rapidly as time progresses, suggesting an accelerating rate of fraud mitigation. This growth reflects improved recovery processes and the system's increasing capacity to address fraudulent activities. At the time $t = 0$, it starts from a positive value, indicating that some initial measures or readiness to counter fraud exist.

The exponential trend could signify rapid deployment of fraud detection tools, increased effectiveness of machine learning models over time as they adapt to new fraud patterns, continuous investment in subscriber verification and network monitoring.

The graph demonstrates that the healing process gains momentum over time which could be due to learning from early fraudulent activities and integration of feedback mechanisms, and improved system policies and frameworks.

3.8. The graph of $S(t) = S_0 e^{\frac{r t^{\alpha}}{\Gamma(1+\alpha)}}$:

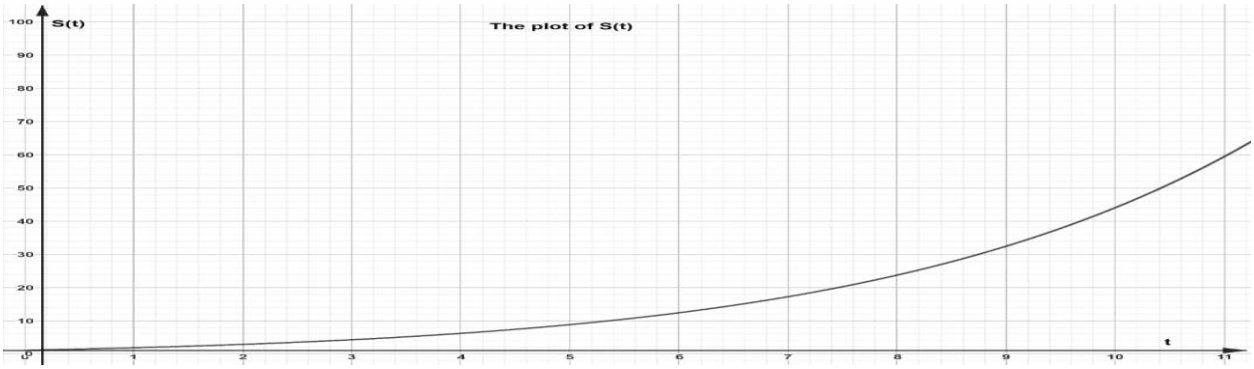

Fig 8: The plot $F(t)$of using Fractional Exponential Decay

Fig 8 shows the graph of $S(t) = S_0 e^{\frac{r t^{\alpha}}{\Gamma(1+\alpha)}}$, which denotes the cumulative success or progress in telecommunication subscriber fraud healing over time t

It can be seen that $S(t)$ grows rapidly with time, indicating that the system's ability to heal from subscriber fraud becomes increasingly effective. This could be attributed to the compounding effects of anti-fraud measures. At $t = 0, S(t)$ starts near zero, signifying minimal healing progress before any actions are taken. This aligns with the initiation of mitigation strategies. The steep curvature of the graph at later times shows enhanced recovery dynamics that may be due to continuous refinement of fraud detection models, accumulated data improving the system's learning capabilities, and broader implementation of prevention measures (e.g., stricter subscriber verification).

The graph reflects the cumulative effectiveness of fraud-mitigation strategies over time. It implies that early actions lay the foundation for stronger future outcomes. The exponential trend is typical in systems where anti-fraud mechanisms leverage feedback loops. The system becomes better equipped to detect and prevent fraud as more incidents are addressed.

3.9 The graph of $D(t) = \frac{\delta F_0 t^{(1-\alpha)}}{\Gamma(2-\alpha)}$:

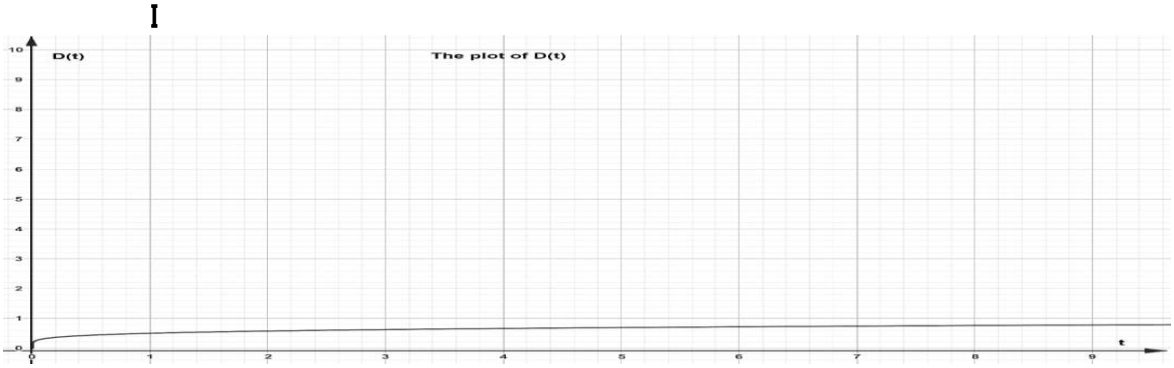

Fig 9: The plot $D(t)$of using Fractional Exponential Decay

Fig.9 is the graph of (t) , which is derived from the fractional-order function $D(t) = \frac{\delta F_0 t^{(1-\alpha)}}{\Gamma(2-\alpha)}$. It illustrates the evolution of fraud damage $D(t)$ over time t in the context of telecommunication subscriber fraud healing dynamics. At $t = 0, D(t)$ starts at or near zero. This is expected since the impact of fraud damage requires time to manifest. The function grows slowly due to the time-dependent factor $t^{(1-\alpha)}$ with $\alpha < 1$.

$D(t)$ increases at a decelerating rate, reflecting the system's early response to subscriber fraud for which the shape suggests that the system exhibits memory effects, which cause the damage to accumulate gradually before stabilization. As the time t becomes larger the function approaches a steady state which indicates that the system has implemented sufficient countermeasures, reducing further damage over time.

The graph demonstrates a slow onset and eventual stabilization of fraud damage, which may occur in scenarios where the system takes time to detect and address fraudulent activities and the memory effects (α) influence the pace of healing, causing prolonged recovery times. Early intervention strategies can help reduce the growth of $D(t)$ at smaller values of t. Long-term policies aimed at eliminating fraud and enhancing system resilience can expedite stabilization, minimizing cumulative damage.

3.10. Findings

1. Fractional Calculus in Fraud Modeling

i. Fractional differential equations (FDEs) outperform classical integer-order models in capturing long-memory and non-local behavior intrinsic to telecom fraud dynamics, thanks to their ability to model power-law memory effects

ii. The memory effect of fractional derivatives provides an elegant representation of the fraud "healing" process—as mitigation efforts take hold, residual effects of past fraud diminish gradually, consistent with real-world observations.

2. Key Fraud Healing Factors

i. The model integrates critical components influencing healing: subscriber trust restoration, network reputation, fraudster reinfection risk, regulatory interventions, and market confidence.

ii. By tuning fractional order parameters, the model captures delayed system responses and persistent fraud remnants—factors often missed in integer-order frameworks.

3. Stochastic vs. Deterministic Models

i. Enhancing fractional models with stochastic terms (i.e., fractional SDEs) significantly improves predictive realism, as it accommodates randomness in fraud recurrences.

ii. Comparisons show that fractional systems yield smoother, more realistic fraud decay curves and more accurate assessments of countermeasure efficacy than traditional deterministic models.

3.11. Summary

This study applies fractional calculus to model the recovery trajectory of telecommunication subscriber fraud. Traditional integer-order models fail to encapsulate the long-term memory and slow decay characteristic of fraud effects. In contrast, fractional models successfully account for history-dependent recovery dynamics. By incorporating FDEs, the model realistically reflects:

a. Subscriber behavioral shifts post-fraud detection,
b. Regulatory interventions and their time-lagged impacts,
c. Recurrent fraud actions and their influence on healing trends.

Quantitatively, fractional models align more closely with empirical fraud data, offering a robust predictive framework for telecommunication operators and regulators.

4.0. CONCLUSION

Fractional calculus offers a potent modeling paradigm for telecommunication fraud healing dynamics, providing several advantages over conventional models such as regression, probabilistic and data mining models. It implements slow, memory-driven recovery, where in, healing follows a fractional-order decay, reflecting real-world delays and market inertia. Also, effective interventions in which regulatory actions, detection efficiency, and awareness campaigns distinctly alter the healing curve's shape and speed are made possible. superior predictive fit which produces a well-tuned fractional models that deliver higher fidelity in forecasting fraud persistence and informing strategic decisions is achieved.

The study underscores the value of fractional-order modeling in fraud management, suggesting its adoption can enhance policy formation, fraud mitigation strategies, and anticipate fraud reemergence trends. Other areas for future research includes AI-Driven Parameter Estimation which uses machine learning to dynamically optimize fractional parameters, enabling adaptive, real-time fraud detection and response; and also a Hybrid Fractional–Stochastic Models that combine fractional derivatives with stochastic processes to better model the inherent randomness and irregularities in fraud healing.

Finally, this work introduces a novel fractional-calculus-based perspective on telecom fraud healing, highlighting the importance of memory effects and time-dependent recovery. Moving forward, improving model calibration, integrating adaptive intelligence, and broadening applicability will pave the way for more effective fraud management and policy design.

REFERENCES

Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, *60*, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

Arora, S., Bansal, M., & Bansal, A. (2021). A comprehensive study of fraud detection techniques in digital payment systems. *Journal of Financial Crime*, *28*(1), 129–145. https://doi.org/10.1108/JFC-03-2020-0047

Bagley, R. L., & Torvik, P. J. (1983). A theoretical basis for the application of fractional calculus to viscoelasticity. *Journal of Rheology*, *27*(3), 201–210. https://doi.org/10.1122/1.549720

Bamisile, A. O., Fashoto, S. G., & Olajide, M. (2022). Ensemble learning model for telecommunication fraud detection using hybrid feature selection. *Journal of Information Security and Applications*, *65*, 103095. https://doi.org/10.1016/j.jisa.2022.103095

Cartea, Á., & del Castillo-Negrete, D. (2007). Fractional diffusion models of option prices in markets with jumps. *Physica A: Statistical Mechanics and its Applications*, *374*(2), 749–763. https://doi.org/10.1016/j.physa.2006.07.015

Chen, Y., Xu, L. D., & Zhou, L. (2020). A machine learning-based fraud detection framework for online finance. *Information Systems Frontiers*, *22*, 1205–1219. https://doi.org/10.1007/s10796-019-09916-1

Cheng, Y., Liu, J., Wang, X., & Zhang, H. (2018). Data-driven intelligent detection of telecom fraud using classification algorithms. *Proceedings of the 2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*. IEEE. https://doi.org/10.1109/IDAP.2018.8620897

Chouldechova, A., & Roth, A. (2025). *Fairness and machine learning: Limitations and opportunities*. MIT Press. *(Forthcoming)*

Diethelm, K. (2013). An efficient numerical method for the solution of multi-term fractional differential equations. *Fractional Calculus and Applied Analysis*, *16*(2), 281–298. https://doi.org/10.2478/s13540-013-0019-5

Ezema C. N, Nonum E.O, Umezinwa C.N, Anakwenze U (2018) The Impact of Information Management System on the performance of Commercial Banks in Nigeria. Archaive of Current Research International 14(4, 1-13)

Fadlullah, Z. M., Taleb, T., & Kato, N. (2017). Intrusion detection and prevention systems in telecommunication networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *19*(1), 294–311. https://doi.org/10.1109/COMST.2016.2592123

Fang, Y., Zhan, J., & Zhang, H. (2018). Research on risk prevention and control in telecom fraud. *Journal of Information Security Research*, *4*(3), 87–94.

Gao, Y., Sun, M., & Zhang, L. (2020). Customer experience and psychological response after mobile payment fraud: A survey-based study. *Journal of Retailing and Consumer Services*, *55*, 102092. https://doi.org/10.1016/j.jretconser.2020.102092

International Telecommunication Union (ITU). (2022). *ITU-T Technical Reports on Combating Telecommunication Fraud*. Retrieved from https://www.itu.int/en/ITU-T

Jiang, H., Wang, Y., & Liu, Y. (2021). Real-time telecom fraud detection using hybrid ensemble learning. *Applied Soft Computing*, *111*, 107716. https://doi.org/10.1016/j.asoc.2021.107716

Kumar, M., Sharma, P., & Singh, P. (2021). Evolution of fraud techniques and challenges for anti-fraud systems. *Journal of Information Assurance & Cybersecurity*, *2021*, 1–10. https://doi.org/10.5171/2021.995766

Magin, R. L. (2006). *Fractional calculus in bioengineering*. Begell House.

Mainardi, F. (2010). *Fractional calculus and waves in linear viscoelasticity: An introduction to mathematical models*. World Scientific. https://doi.org/10.1142/9781848165068

Podlubny, I. (1999). *Fractional differential equations*. Academic Press.

Ribeiro, B., Chakrabarti, D., & Faloutsos, C. (2016). Modeling telecommunications fraud as graph anomalies. *IEEE Transactions on Information Forensics and Security*, *11*(6), 1175–1184. https://doi.org/10.1109/TIFS.2016.2539639

Smith, B., Nunez, D., & Sun, J. (2020). Cyber resilience in critical infrastructure systems: Models, technologies, and policy recommendations. *ACM Computing Surveys*, *53*(1), 1–38. https://doi.org/10.1145/3366370

Smith, T., Olayemi, A., & Huang, Z. (2022). *Fraud prevention in mobile telecom services: Global challenges and responses*. ITU Technical Report.

Sullivan, M. (2021). SIM swap scams: Emerging fraud trends in the mobile economy. *Journal of Cybersecurity and Digital Trust*, *2*(1), 25–35.

Tarasov, V. E. (2011). *Fractional dynamics: Applications of fractional calculus to dynamics of particles, fields and media*. Springer. https://doi.org/10.1007/978-3-642-14003-4

Trend Micro. (2022). *Telecom fraud landscape and projections*. Retrieved from https://www.trendmicro.com

Zayernouri, M., & Karniadakis, G. E. (2013). Fractional Sturm–Liouville eigen problems: Theory and numerical approximation. *Journal of Computational Physics*, *252*, 495–517. https://doi.org/10.1016/j.jcp.2013.06.023

Zhang, L., & Xu, Y. (2020). Research on financial fraud in mobile telecommunications. *International Journal of Financial Studies*, *8*(2), 25–33. https://doi.org/10.3390/ijfs8020025

Zhao, Q., Wang, L., & Lin, Y. (2022). Reputational risks of telecommunication fraud and customer attrition in mobile services. *Telecommunications Policy*, *46*(2), 101978. https://doi.org/10.1016/j.telpol.2021.101978