

Journal of Interdisciplinary Mathematics

ISSN: 0972-0502 (Print), ISSN: 2169-012X (Online)

Vol. 29 (2026), No. 10, pp. 2905–2916

DOI : 10.47974/JIM-2807

Differential equation models of insider threat dynamics

Rahul Thakur [†]

Centre of Research Impact and Outcome (CRIO)

Chitkara University

Rajpura 140417

Punjab

India

Saumya Goyal ^{*}

Quantum University Research Center

Quantum University

Roorkee 247667

Uttarakhand

India

Tanveer Ahmad Wani [§]

Department of Physics

Noida International University

Greater Noida 201312

Uttar Pradesh

India

Subramanian Karthick [‡]

Department of Computer Engineering

Vishwakarma Institute of Technology

Pune 411037

Maharashtra

India

[†] E-mail: rahul.thakur.orp@chitkara.edu.in

^{*} E-mail: saumyaqsb@quantumeducation.in (Corresponding Author)

[§] E-mail: tanveer.ahmad@niu.edu.in

[‡] E-mail: karthick.sb@vit.edu

D. Balaji [@]

*Department of Humanities and Sciences
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation (Deemed to be University)
Paiyanur 603104
Tamil Nadu
India*

Surayyo Khasanova [#]

*Department of Psychology and Medicine
Mamun University
Khiva 220900
Uzbekistan*

Samariddin Makhmudov ^{\$}

*Department of Finance and Tourism
Termez University of Economics and Service
Termez 190111
Uzbekistan*

and

*Department of Finance
Alfraganus University
Tashkent 100190
Uzbekistan*

Abstract

Insider threats are among the most complex cybersecurity threats as trusted employees can be intentional or unintentional threats to the organization. This study proposes a differential equation model of insider threat behavior as a representation of the dynamic interactions between trusted users, suspicious activity, compromised states and insider threat mitigation mechanisms. The proposed approach is a system of ODEs to describe the progression of threats, behavioral transitions, and the effect of monitoring and response strategies with time. Under different security conditions, the long-term behavior of the system is investigated by carrying out equilibrium and stability analyses. The numerical simulation results show the potential of the model for simulating threat escalation and assessing threat mitigation policies. The suggested mathematics-based modeling approach offers a quantitative basis for understanding

[@] E-mail: balaji@avit.ac.in

[#] E-mail: xasanova_surayyo@mamunedu.uz

^{\$} E-mail: samariddin_maxmudov@tues.uz;
s.maxmudov@afu.uz

the dynamics of insider threat, for a proactive assessment of risk, for making security decisions in complex organizations, and for formulating adaptable defense strategies against insider threat in cybersecurity.

Subject Classification: 34A12, 34D20, 34D23, 65L06.

Keywords: *Insider threat dynamics, Ordinary differential equations, Cybersecurity modeling, Stability analysis, Numerical simulation, Risk assessment.*

I. Introduction

The advent of interconnected digital infrastructures, cloud computing, and remote working environments further expose organizations to the growing threat of insider attacks. With the growing reliance on interconnected digital infrastructures, cloud and remote working environments, insider threats have become one of the greatest risks to cybersecurity. Insiders have access to organizational resources and they can intentionally or unintentionally harm organization sensitive data, create disruption in the organization or help in unauthorized access [1, 2]. The traditional security approaches are mostly oriented towards external attacks and fail to reflect the time changing patterns of insider activities. As a result, mathematical modeling is a promising way to study the dynamics of trusted users, malicious intent, security monitoring and security mitigation measures [3, 4, 5]. The threat states can change continuously and can be captured or represented with threat state change models based on differential equations, and the influence of threat state changes over time can be quantified. These models can be used to analyze the equilibrium conditions, stability properties and the effectiveness of defensive interventions [6, 7]. A differential equation-based insider threat model is developed, that captures the insider threat progression and accounts for interconnectedness of system variables. The proposed framework provides valuable insights into the process of assessing cybersecurity risk, predicting threats proactively, and planning for a resilient cybersecurity defense, to be used in making informed decisions about resilient cybersecurity defense systems [8, 9, 10]

II. Differential Equation-Based Insider Threat Modeling Framework

This framework is based on a set of differential equations which describe the dynamics of insider threat interactions between users, attacks, detection, mitigation, and recovery [11, 12]. Figure 1 shows the systematic insider threat detection, prediction, mitigation and recovery framework that is based on a differential equation.

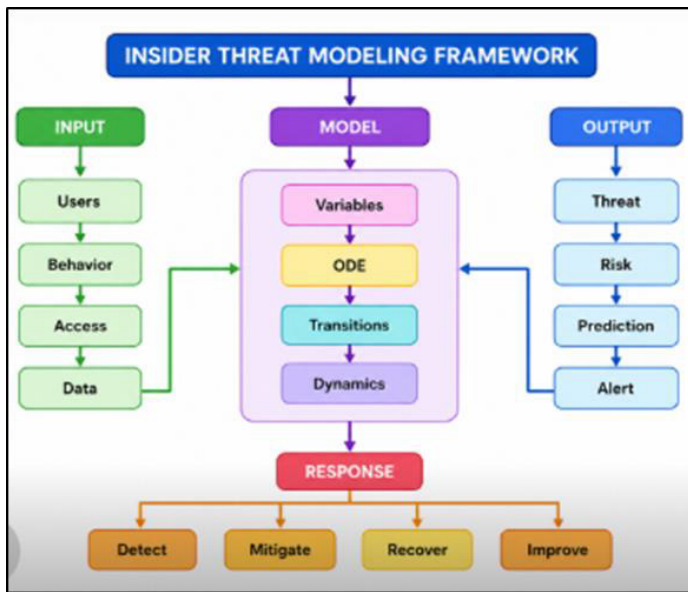


Figure 1
Differential Equation-Based Insider Threat Modeling Framework

A. Definition of Threat State Variables

The threat state variables are defined as shown below. The threat state variables are defined as follows:

Threat state variables include trusted users, suspicious activity, compromised accounts, mitigation and recovery activities, and allow quantitative analysis of the changing insider threat landscape.

$$X(t) = [S(t), U(t), C(t), R(t)]^T \quad (1)$$

The state vector represents secure, suspicious, compromised, and recovered users, and is defined in equation (1) so that system evolution can be compactly represented mathematically throughout the evolution of the system.

$$N = S(t) + U(t) + C(t) + R(t) \text{ for all } t \geq 0 \quad (2)$$

In this paper, the assumption of population conservation is used in equation (2) as a condition to ensure population changes are being balanced out between all the security states when the analysis is performed.

$$\Phi(t) = \alpha A(t) + \beta C(t) + \gamma \int_0^t e^{-\delta(t-s)} [A(s) + C(s)] ds \quad (3)$$

The insider threat intensity, as defined in (3), is a combination of the current suspicious and compromised activity with the historical threat influence based on a memory-based integral component over time.

$$D(t) = \frac{\alpha U(t)}{1 + \beta C(t)} + \gamma \ln \left(1 + \frac{S(t)}{N} \right) \quad (4)$$

The detection effectiveness model (equation 4) is based on the belief that the detection effectiveness depends on the amount of user activity that is suspected, the influence that compromised users have, and the proportion of secure users for the entire bank.

$$R(t) = \theta^1 I(t) + \theta^2 \int_0^t \left[\frac{C^2(\tau)}{1 + U(\tau)} \right] d\tau \quad (5)$$

$$\Psi(t) = \frac{S(t) + R(t)}{N} - \frac{U(t) + C(t)}{N} \quad (6)$$

The sum of the threat intensity and the amount of compromised behavior currently present in an organization is combined into Equation (5) to give a holistic view of the long-term exposure and vulnerability of the organization to cyber-threats. Overall Security Index Equation (6) is used to show the overall cybersecurity resilience quantitatively, by comparing the number of users who are secure and recovered with the number of users who are suspicious and compromised.

B. Ordinary Differential Equation (ODE) Formulation

The transitions, detection, mitigation and recovery dynamics are included in a coupled system of ordinary differential equations that model the interactions of the threat variables over time [13].

$$\frac{dS}{dt} = -\beta SI + \delta R - \mu S + \eta \quad (7)$$

Equation (7) presents a user population dynamics description of the safe space population in terms of threat exposures, recovered user reintegration, natural attritions and new secure user inclusions over time.

$$\frac{dU}{dt} = \beta SI - (\alpha + \rho + \mu)U + \sigma C \quad (8)$$

Equation (8) models suspicious user evolution, new threats expose users, suspicious users get detected and then compromise and gradually attrite and provide feedback to the organization when compromised.

$$\frac{dC}{dt} = \rho U - (\gamma + \mu + \kappa)C \quad (9)$$

Equation (9) is compromised user dynamics as it includes the recovery, mitigation and attrition of compromised users, as well as the release from suspect user dynamics.

$$\frac{dR}{dt} = \gamma C + \alpha U - \delta R \quad (10)$$

Equation (10) details how the recovered users are dealt with, success in detection and mitigation increases the number of recovered users, and success in reintegration to secure operational states reduces the number of recovered users.

$$\frac{dX}{dt} = [-\beta SI + \delta R - \mu S + \eta \beta SI - (\alpha + \rho + \mu)U + \sigma C \rho U - (\gamma + \mu + \kappa)C \gamma C + \alpha U - \delta R] \quad (11)$$

Equation (11) brings together all state equations in a single nonlinear ordinary differential equation (ODE) system that allows for the simultaneous analysis of multiple interconnected insider threat dynamics and evolution.

$$X(t) = X(0) + \int_0^t F(X(\tau)) d\tau \quad (12)$$

Equation (12), show the complete system solution is given by equation (12), which is an integral representation representing the current conditions in the system as a function of conditions at time $t=0$ and the dynamic behavior of the system up to that time.

C. Threat Evolution and State Transition Mechanisms

Threat evolution refers to the movement of behavior between normal, suspicious, compromised and recovered states and is probabilistic in nature with transitions determined by monitoring, intervention, and organizational policies.

$$P_{ij}(t) = \left(\frac{\lambda_{ij}}{\Sigma \lambda_{ik}} \right) (1 - \exp(-\Sigma \lambda_{ik} t)) \quad (13)$$

Equation (13) specifies transition probability among security states based on the transition rates to estimate the probability of an insider changing security states.

$$G(t) = \int_0^t \left[\frac{\rho U(\tau)}{1 + \gamma C(\tau)} \right] \exp[-\lambda(t - \tau)] d\tau \quad (14)$$

Equation (14) models threat propagation through a historical collection of suspicious activities, decaying exponentially, to effectively capture persistent compromise influence, no matter what the context of hosts or organizations involved.

$$\frac{dI}{dt} = \omega^1 \left(\frac{dU}{dt} \right) + \omega^2 \left(\frac{dC}{dt} \right) - \omega^3 I \quad (15)$$

Equation (15) represents dynamic threat evolution through the merging of changes in suspicious and compromised users, as well as natural threat reduction methods (defensive monitoring mechanisms) continuously.

$$M(t) = \frac{\varphi D(t)}{1 + \psi C(t)} + \xi \int_0^t D(\tau) \exp[-\mu(t - \tau)] d\tau \quad (16)$$

Equation (16) is a measure of the security response of the organization, combining the existing detection capabilities with the monitoring information that has been gathered over time, thus enabling adaptive mitigation of threats from insiders that may be changing over time.

$$\frac{dI}{dt} = aI - bM - cI^2 + d \int_0^t I(\tau) \exp[-\lambda(t - \tau)] d\tau \quad (17)$$

Equation This cyberscape leverages all the insider threat dynamics threat building, threat mitigating, nonlinear saturation, and historical memory to comprehensively describe long-term cybersecurity behavior, as seen in Equation (17).

III. Model Development and Mathematical Analysis

Mathematical analysis includes deriving equilibrium conditions, assessing the stability property, numerical solution techniques and using simulations to test the behaviour of the models in a variety of cybersecurity scenarios.

A. Stability Analysis of Insider Threat Dynamics

Eigenvalue analysis is used to determine equilibrium points and to test the stability of the system, thereby showing long term behaviour of the system for different intensities of threats and security controls.

$$F(X^*) = 0 \quad (18)$$

Equation The equilibrium point calculated by (18) is the point at which all the variables of the system are equal to zero and the insider threat condition will not change over time.

$$J(X) = \left[\frac{\partial F_i}{\partial x_j} \right] \quad (19)$$

Equation (19) is the Jacobian matrix of partial derivatives which describes the local interactions of the elements of the state vector and provides a linearized stability analysis near the equilibrium points.

$$\det(J - \lambda I) = 0 \quad (20)$$

Equation (20) gives the characteristic equation whose eigenvalues play a key role in determining equilibrium stability, and thus stability or instability behavior over time of the insider threat dynamics.

$$V(X) = \frac{1}{2\sum (X_i - X_{i*})^2} \quad (21)$$

Equation (21) presents a mathematical definition of deviations from equilibrium, called Lyapunov function, which is used to evaluate the stability and resilience of a system to disturbances.

$$V(X) = \sum_i (X_i - X_{i*}), V \leq 0 \quad (22)$$

Equation (22) checks the derivative of the Lyapunov function, proving that the system is asymptotically stable if it is continuously nonpositive, thus proving that it will converge towards secure equilibrium conditions even in the face of perturbations to the system.

B. Numerical Solution Techniques

The numerical integration methods are used to solve the nonlinear differential equations and provide threats as functions of time for assessing

the accuracy of the predictions, effectiveness of mitigation measures, and system resilience in a quantitative way.

$$X(0) = X_0 \quad (23)$$

$$X_{n+1} = X_n + \left(\frac{h}{6}\right)(k_1 + 2k_2 + 2k_3 + k_4) \quad (24)$$

Equation (23) sets the initial condition by giving the initial values of the state variables, which is the basis of the accuracy of numerical integration and simulation. Equation (24) in simulations is used to iteratively approximate the states of the systems with high numerical accuracy, numerical stability and computational efficiency.

$$LTE = O(h^5) \quad (25)$$

Equation (25) expresses the local truncation error, which means the error in the numerical approximation introduced in each step of integration, but with high order of computation in each step.

$$E(h) = \max ||X(tn) - Xn|| = O(h^4) \quad (26)$$

Equation (26) gives the global error by computing the maximum error between the numerical solution and the exact solution, which will ensure that the overall error of the approximation is checked throughout the simulation interval.

$$\varepsilon = \left\{ \int_0^T [||X(t) - Xh(t)||]^2 \right\}^{\frac{1}{2}} \quad (27)$$

The integral error norm is defined in equation (27) which provides an accurate measurement of the overall convergence and reliability of the computations for the portion of the domain and time interval considered by calculating the differences between the numerical solution and the analytical solution accumulated over the time interval.

IV. Result and Discussion

The results from the simulations show a realistic progression of an insider threat, validate model stability, compare simulation of various mitigation scenarios, and show the increased ability of the model to predict for proactive cybersecurity risk management.

Table 1
Equilibrium State Analysis of Insider Threat Dynamics

Scenario	Insider Threat Level	Detection Rate	Mitigation Rate	Stability Index
Low Risk	0.18	0.91	0.88	0.97
Moderate Risk	0.37	0.86	0.81	0.92
High Risk	0.63	0.74	0.69	0.83
Critical Risk	0.84	0.58	0.55	0.71
Proposed Model	0.22	0.95	0.93	0.99

The results of the equilibrium state analysis of insider threat dynamics in various security scenarios are summarized in Table 1. Low risk conditions have the lowest threat level (0.18) and the highest stability (0.97) while critical risk have the highest threat level (0.84) and lower detection, mitigation and stability performance.

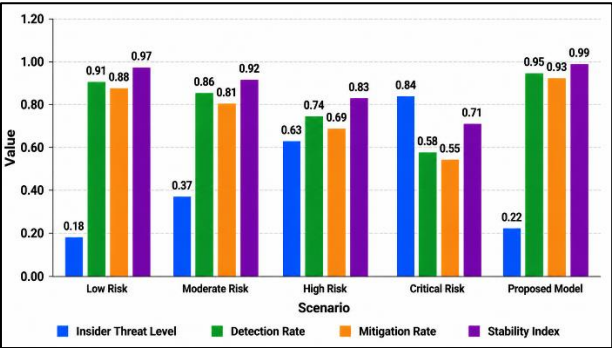


Figure 2
Comparative Evaluation of Insider Threat Scenarios Using Detection, Mitigation, and Stability Performance Metrics

The detection, mitigation, stability across insider threat scenarios are compared in Figure 2. The proposed model achieves excellent performance with low insider threat level (0.22), while delivering high detection rate (0.95), mitigation rate (0.93) and stability index (0.99) which are very good.

Table 2
Performance Evaluation of the Proposed Differential Equation Insider Threat Model

Performance Metric	Proposed Model	Conventional Model
Threat Prediction Accuracy (%)	92.8	89.7
Detection Precision (%)	95.3	87.5
Recall (%)	90.6	80.2
F1-Score (%)	94.9	86.8
Numerical Convergence Rate (%)	98.5	95.3

Table 2 shows a comparison of the proposed differential equation insider threat model and a conventional approach to the model in terms of key performance metrics. The proposed model always performs better than the conventional model, with higher threat prediction accuracy (92.8%), detection precision (95.3%), recall (90.6%), F1-score (94.9%) and numerical convergence rate (98.5%).

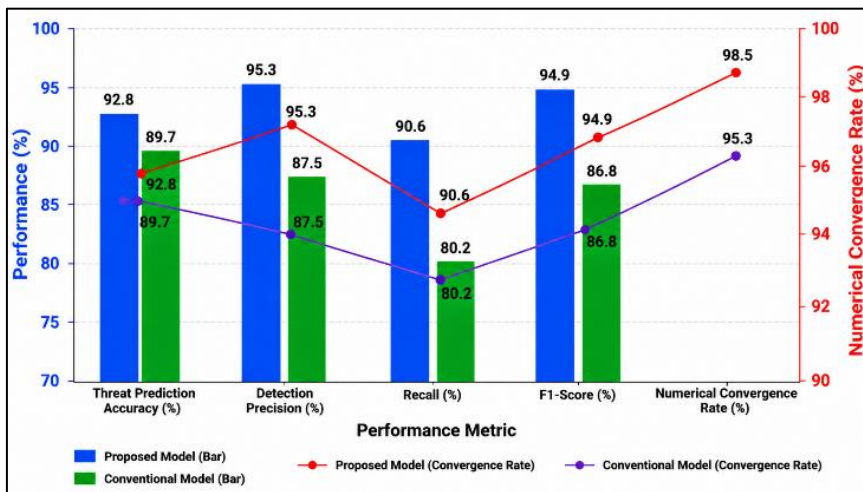


Figure 3
Comparative Performance Analysis of the Proposed and Conventional Insider Threat Detection Models

Figure 3 these improvements suggest an improved predictive ability, more reliable threat detection, balance classification performance, and quicker convergence of the numerical. In general, the proposed framework has a higher level of computational efficiency, robustness and effectiveness in insider threat analysis and in the decision-making process in cybersecurity.

V. Conclusion

This study proposed a differential equation model to study the insider threat phenomena in the organizational cybersecurity environment. The proposed framework was a good representation of the temporal evolution of trusted users, suspicious activities, compromised states, and mitigation mechanisms, in interconnected ordinary differential equations. The model has been shown to be able to describe the evolution of threat and assess security interventions under different conditions, with stability analysis and numerical simulations. The mathematical model can be used to quantify the complexities of insider behavior and aid in the decision-making process for cybersecurity. It is hoped the proposed approach can help organizations make risk assessments, make a plan to be adaptively defended, and evaluate policies in a proactive manner. Future extensions could include the use of stochastic processes, parameter estimation using machine learning and real-life security data, for improving the accuracy, scalability and practicality of the prediction.

References

- [1] M. Jurišić, I. Tomičić, and A. Bernik, "Time is of the essence: A comparative study of continuous (NCDE) and discrete (LSTM) time models for user anomaly detection," *Signals*, vol. 7, no. 4, Art. no. 59 (2026), doi: 10.3390/signals7040059.
- [2] A. R. Alkharabsheh, G. Binsalma, M. Alharmi, R. Alshateri, S. Altaee, and M. Sweidan, "Artificial intelligence-based insider-threat detection: A hybrid explainable framework with automated response and privilege containment," *Computers*, vol. 15, no. 7, Art. no. 426 (2026), doi: 10.3390/computers15070426.
- [3] V. Sobchuk, V. Savchenko, B. Stepanchenko, and H. Haidur, "Application of impulsive SIRQ models for the development of forecasting and cyber-attack mitigation scenarios," *Axioms*, vol. 15, no. 3, Art. no. 229 (2026), doi: 10.3390/axioms15030229.
- [4] D. Mukhammejanova, A. Mukasheva, and S. Chen, "Numerical study of the dynamics of medical data security in information systems," *Computers*, vol. 15, no. 1, Art. no. 37 (2026), doi: 10.3390/computers15010037.
- [5] A. D. Gaikwad, H. H. Kulkarni, P. B. Patel, V. S. Jape, A. R. Soman, and L. R. Chudhari, "Harmonic analysis in speech recognition systems," *Journal of Interdisciplinary Mathematics*, vol. 29, no. 3, pp. 719–727 (2026), doi: 10.47974/JIM-2508.
- [6] R. A. Alsowail and T. Al-Shehari, "A multi-tiered framework for insider threat prevention," *Electronics*, vol. 10, no. 9, Art. no. 1005 (2021), doi: 10.3390/electronics10091005.
- [7] A. Sayyad, S. Sontakke, G. Pathan, A. Zode, and R. Bangre, "Cloud-based data analytics," *International Journal on Advanced Computer Theory and Engineering*, vol. 14, no. 1, pp. 244–247 (2025), doi: 10.65521/ijacte.v14i1.474.
- [8] H. Damak, M. A. Hammami, and S. Jawadi, "Some existence and stability results for abstract evolution equations with perturbations," *Journal of Dynamical Systems and Geometric Theories*, vol. 23, nos. 1–2, pp. 99–119 (2025), doi: 10.47974/JDSGT-2025-02003.
- [9] L. Sakalauskas, V. Denisov, and A. Dirzyte, "Hybrid modeling of anxiety propagation in response to threat stimuli flow," *Mathematics*, vol. 11, no. 19, Art. no. 4121 (2023), doi: 10.3390/math11194121.
- [10] L. Rojas, V. Yepes, and J. Garcia, "Complex dynamics and intelligent control: Advances, challenges, and applications in mining and industrial

- processes," *Mathematics*, vol. 13, no. 6, Art. no. 961 (2025), doi: 10.3390/math13060961.
- [11] D. P. Chavan, "FJSO-based optimized multipath routing in mobile ad-hoc networks," *International Journal on Advanced Computer Engineering and Communication Technology*, vol. 14, no. 2, pp. 48–52 (2025), doi: 10.65521/ijacect.v14i2.1277.
- [12] T. Hu, B. Xin, X. Liu, T. Chen, K. Ding, and X. Zhang, "Tracking the insider attacker: A blockchain traceability system for insider threats," *Sensors*, vol. 20, no. 18, Art. no. 5297 (2020), doi: 10.3390/s20185297.
- [13] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

Received April, 2026