

Applied Nonlinearity in Modeling Secure Internet Service Dynamics for Academic Library and Research Data Systems

G S Murugapandian

Assistant Professor, Department of Mathematics, Nandha Engineering College Erode 52, T.N, India

KEYWORDS:

Nonlinear Dynamics;
Academic Libraries;
Research Data Systems;
Cybersecurity;
Service Trust;
Adaptive Security Response

Author's Email:

drskresearch@gmail.com

Received : 04.04.2026

Revised : 06.05.2026

Accepted : 08.06.2026

ABSTRACT

Academic library and research-data applications rely more and more on secure, responsive, and reliable information infrastructures, and their performance is dependent upon the nonlinear interactions that happen among the users' demand, the intensity of cyber-threat, the service delay, the trust that the user has, and the adaptive response to threat. The five key state variables of this study are the normalized service load $L(t)$, the intensity of cyber-threats $A(t)$, the level of service trust $T(t)$, the normalized delay $D(t)$ and the security-response level $R(t)$. The model is tested via computational simulation, equilibrium testing, and local stability analysis for five operating conditions, from normal service to the most severe of the security disturbance and adaptive recovery. The criteria for assessing performance is based on the average service load, peak threat intensity, average delay, minimum trust level, recovery time and a Secure Service Performance Index. In the results, severe attack conditions are found to delay and decrease the level of trust, while adaptive response is found to suppress the growth of threat, to gain recovery speed and to enhance secure-service performance, which leads to a resilient academic information-service management.

How to cite this article: Murugapandian GS, Applied Nonlinearity in Modeling Secure Internet Service Dynamics for Academic Library and Research Data Systems, Applied Nonlinearity in Science and Technology, Vol. 2, No. 2, 2026, 1-8

1. INTRODUCTION

Internet based scholar communication academic libraries and research-data repositories are the center point of today's scholarly communication, offering by means of digital collections, institutional publications, datasets, metadata and co-operative research tools, continuous and unimpeded access to these fields. Cloud-based platforms, distributed databases, remote authentication, APIs and web-based informational services are facilitating more accessibility and scalability. But this greater reliance on inter-dependent digital infrastructure makes academic systems vulnerable to hackers, insufficient credentials, denial of service attacks, malicious traffic, violation of data integrity and disruption of services.

The amount of service demand is dynamic, and so is the level of cybersecurity exposure. More concurrent

users can generate more computational and network loads, and increase the target area for attack if there are more repository transactions and remote access sessions. Security disturbances can cause delays in processing, decreased response, service unavailability, and user distrust. Malicious activity can be slowed down or suppressed by adaptive security mechanisms, but it also can add processing overhead. Hence, the service load, threat strength of cyber, latency, trust, and defensive attack should be viewed as a set of the system characteristics.

Many traditional security models employ static indicators, fixed thresholds or linear relationships. They may not reflect saturation, feedback, congestion growth, threat escalation and recovery after attacks adequately and can be useful for simplified analysis. Such interactions can be accommodated by a nonlinear dynamic modelling approach, which can be represented by continuously changing and interdependent system variables. To

date, however, the few studies that have both explored the service performance effects of cybersecurity conditions and tested for nonlinear relationships have done so separately.

This study proposes a coupled nonlinear dynamic framework to analyze secure Internet-service behaviour in academic information systems. The major contributions are: (1) nonlinear modeling of Internet-service dynamics; (2) combination of service-load, cyber-threat-intensity, service-trust, delay, and adaptive-security-response factors in one 5-state model; (3) equilibrium and stability analyses are used to identify key parameters and operating conditions; (4) scenario-based computational evaluations are conducted for normal, high-load, moderate-threat, severe-threat, and adaptive-recovery conditions. The framework enables systematic analysis of resilience, recovery and secure-service performance, but is not a particular deployed institution.

2. LITERATURE REVIEW

The importance of information infrastructures, such as a digital library for the Internet and academic research-data repositories, was identified, because of their role in storing, managing, discovering, and sharing scholarly information [3], [5]. The modern systems are increasingly using distributed storage, web services, remote access and cloud computing to support large collections and users located globally [4, 12]. While these two architectures yield better scalability, accessibility and resource utilization, they also add dependency between the servers, networks, authentication services, storage platforms and the external interfaces [8, 13]. Therefore, the security and usability of academic information services are tightly linked with the security and reliability of the digital infrastructure that provides them [14].

Cybersecurity has then become one of the immensely important issues in academic information environments [1] [2]. Common threats are unauthorized access, credential theft, malware, data leakage, integrity violations, denial of service attacks and service disruption [6]. Solutions about access control policies, authentication protocols, encryption, identity management, intrusion detection, and authorization systems have been explored to ensure security of library and research-data services [9]. But the high-security mechanisms can lead to the decrease of the service latency and computational overhead [10]. High volume, denial of service (DoS)

and malicious traffic can also cause a decrease in service availability, lengthen response time, and restrict access to academic resources [11], [15].

Digital information-service systems involve enterprises that must be highly trusted and reliable, as users demand secure, accurate and continual delivery of services [13]. Research on networked and cyber-physical systems has demonstrated that dynamic and nonlinear models can be used to model interactions between traffic load, system resources, disturbances, feedback controls and recovery mechanisms [7]. Nonlinear modeling is of special value in the study of saturation, threshold effects, fast changes of state as well as coupled feedback effects not sufficiently captured by (static/linear) models. Analysis of system stability for example using equilibrium and eigenvalue analysis has also been utilized to find out if complex systems revert to safe operating conditions following disturbance [7].

Even with these advances, there are still some drawbacks. The academic information services, cyber security mechanisms, network performance, trust or system reliability are individual research areas that are explored in many studies [1, 3]. Likewise, nonlinear and stability models can be used to model communication networks and cyber-physical systems more frequently than digital-service environments in academia [6] [7]. Limited work is the interaction of service load and cyber threat intensity, service delay, the trust, and adaptive security response as temporal variables. This gap drives the development of a coupled nonlinear model of the secure Internet-service dynamics of academic library and research-data systems [5], [12].

3. METHODOLOGY

3.1 Secure Academic Internet Service System Model

The modeled secure academic Internet service environment features academic library users, research-data users, authentication services, Internet service gateway, academic information services, repository and database resource services, and an integrated secure-monitoring and adaptive-response layer. User requests go through authentication and through the Internet service gateway to digital library or research-data services and storage resources as seen in Figure 1. The security layer streams the service usage data and supplies feedback for threat detection and adaptation response.

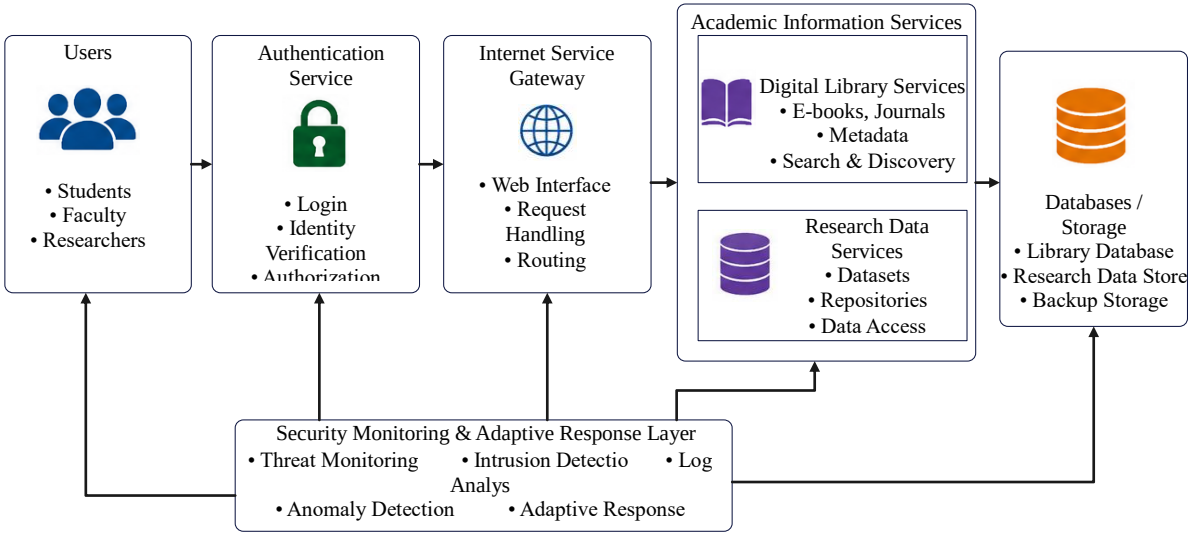


Fig. 1. Proposed Secure Academic Internet Service Architecture

The five state variables of the architecture are normalized: service load $L(t)$, cyber-threat intensity $A(t)$, service trust $T(t)$, service delay $D(t)$ and adaptive security response $R(t)$. These are the

primary service-performance and security conditions that are included in the nonlinear model. The important variables and a few of the model parameters are listed in Table 1.

Table 1. State Variables and Model Parameters

Symbol	Variable / Parameter	Meaning	Range / Value
$L(t)$	Service load	Normalized service demand	0-1
$A(t)$	Threat intensity	Level of cyber-threat activity	0-1
$T(t)$	Service trust	Reliability and user confidence	0-1
$D(t)$	Service delay	Normalized response delay	0-1
$R(t)$	Security response	Adaptive defensive response	0-1
λ	Load growth rate	Service-demand growth	0.40
μ	Threat growth rate	Cyber-threat growth	0.30
δ	Threat suppression	Security-response effectiveness	0.45
η	Trust recovery	Rate of trust restoration	0.35
ρ	Delay coefficient	Nonlinear congestion effect	0.40

3.2 Nonlinear Service-Load and Threat Dynamics

The secure academic web service is developed based on coupled nonlinear equations of the service load and cyber-threats intensity. The normalized service load $L(t)$ wraps around logistic growth as a result of the system capacity limit and the security response and the service delay:

$$\frac{dL}{dt} = \lambda L \left(1 - \frac{L}{K} \right) - \alpha RL - \beta DL \quad , \quad (1)$$

where λ is the load growth rate, K is the normalized service capacity, α the effect of security response and β the effect of delay. The logistic term represents a nonlinear growth in the load and saturation as demand nears system capacity.

Cyber-threat intensity $A(t)$ is modeled as

$$\frac{dA}{dt} = \mu A(1 - A) + \gamma LA - \delta RA \quad , \quad (2)$$

where μ is the intrinsic threat-growth coefficient, γ represents the effect of service load on cyber exposure, and δ represents threat suppression through adaptive security response. The model therefore captures threat growth, load-related exposure, and defensive control within the same nonlinear framework.

3.3 Trust and Service-Delay Dynamics

The service trust $T(t)$ evolves with the effects of adaptable security response, cyber-threat intensity and service delay. The greater the attacks and the

worse the network performance, the less the user will trust the network; the more effective the defensiveness, the better the recovery of trust. The trust dynamics are expressed as

$$\frac{dT}{dt} = \eta R(1 - T) - \theta AT - \phi DT, \quad (3)$$

where η denotes the trust-recovery coefficient, θ represents the effect of cyber threats on trust, and ϕ represents the influence of service delay. The term $\eta R(1 - T)$ captures trust restoration through effective security response.

Service delay $D(t)$ is modeled as

$$\frac{dD}{dt} = \rho L^2 + \sigma A - \kappa D, \quad (4)$$

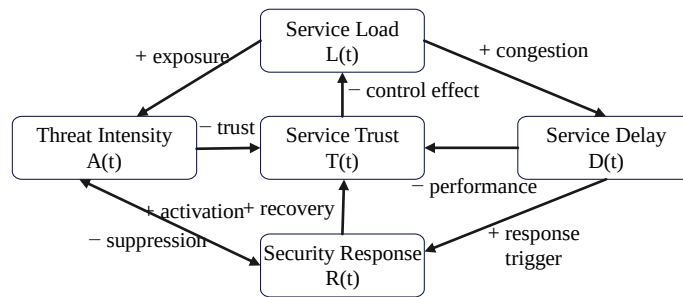


Fig. 2. Coupled Nonlinear State-Interaction Model

3.4 Adaptive Security Response and Secure Service Index

The adaptive security-response state $R(t)$ represents defensive activation when cyber-threat intensity or service degradation increases:

$$\frac{dR}{dt} = \xi A(1 - R) + \psi D(1 - R) - \omega R, \quad (5)$$

where ξ is the threat-response coefficient, ψ is the delay-response coefficient, and ω is the response-decay rate. The model thus enhances defence if there is increased threat or delay and decreases it once stabilised.

Overall service-security performance is measured using

$$S_p = w_1 T + w_2(1 - D) + w_3(1 - A) + w_4 R \quad (6)$$

subject to

$$w_1 + w_2 + w_3 + w_4 = 1$$

with $w_1 = 0.30$, $w_2 = 0.25$, $w_3 = 0.25$, and $w_4 = 0.20$. Higher S_p indicates a more secure and reliable operating condition.

where ρ is the nonlinear congestion coefficient, σ represents the impact of cyber threats on delay, and κ denotes the delay-recovery rate. The nonlinear L^2 term represents the rapid increase in service delay as network and application load becomes high.

Figure 2 illustrates that the five state variables are interdependent: higher service load leads to higher congestion levels and cyber exposure levels, higher threat activity and delay leads to lower trust levels, and adaptive security response enhances recovery, but lowers threat activity. This interaction scheme is the base of the proposed nonlinear model for service-security.

The simulation parameters and initial conditions necessary to test the nonlinear model are summarized in Table 2. The values are considered to be assumed values for computation and not experimentally determined parameters.

Table 2. Simulation Parameters and Values

Parameter	Symbol	Value
Simulation duration	T_s	100 time units
Time step	Δt	0.01
Initial service load	$L(0)$	0.30
Initial threat intensity	$A(0)$	0.10
Initial service trust	$T(0)$	0.90
Initial service delay	$D(0)$	0.15
Initial security response	$R(0)$	0.20
Service capacity	K	1.00
Load growth coefficient	λ	0.40
Threat growth coefficient	μ	0.30
Threat suppression coefficient	δ	0.45
Trust recovery coefficient	η	0.35
Nonlinear delay coefficient	ρ	0.40

3.5 Stability Analysis and Experimental Scenarios

The equilibrium condition is obtained by setting all state derivatives to zero:

$$\frac{dL}{dt} = \frac{dA}{dt} = \frac{dT}{dt} = \frac{dD}{dt} = \frac{dR}{dt} = 0 \quad , \quad (7)$$

The local stability is assessed by the eigenvalues and Jacobian matrix: if the real part (RP) of the eigenvalues is negative, then the equilibrium is

locally stable. Five scenarios are investigated: S1 - normal service, S2 - high service load, S3 - moderate cyber threat, S4 - severe security disturbance, and S5 - adaptive security response and recovery. The workflow (see Figure 3) features model definition, model parameter initialization, numerical simulation, performance evaluation, system-behavior analysis, scenario comparison, sensitivities, visualization and interpretation of the numerical results.

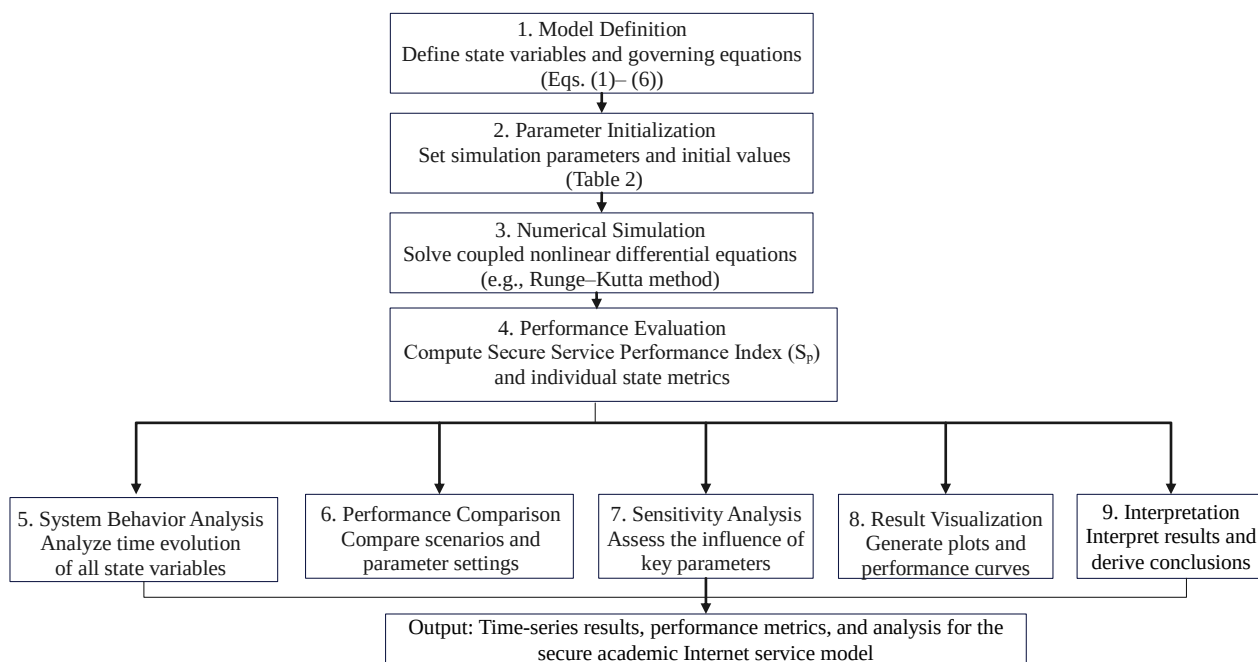


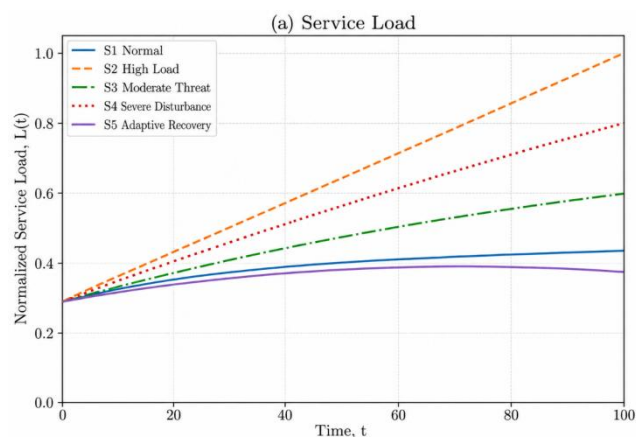
Fig. 3. Computational Evaluation Workflow

4. RESULTS AND DISCUSSION

4.1 Nonlinear Service-Load and Delay Behaviour

The level of service is significantly different depending from the five operating scenarios. As observed in Figure 4(a) and detailed in Table 3, the normal case model keeps an average load of 0.39 while the high load case peaks upward to an average load of 0.65 and gets closer to the normalized capacity limit at the end of the simulation. Moderate threat and severe disturbance have loads of 0.47 and 0.55 respectively, while adaptive recovery only permits an average load of 0.37. This is illustrated by the delay behavior of Figure 4(b). The average delay value has been raised from 0.18 when operating normally to 0.43 when heavily loaded and 0.51 during severe disturbance. With the adaptive-recovery scenario,

average delay is decreased to 0.22, with better stabilization after the defense is activated. The findings validate the fact that there is a nonlinear relationship between the growth of service demand, congestion and delay response.



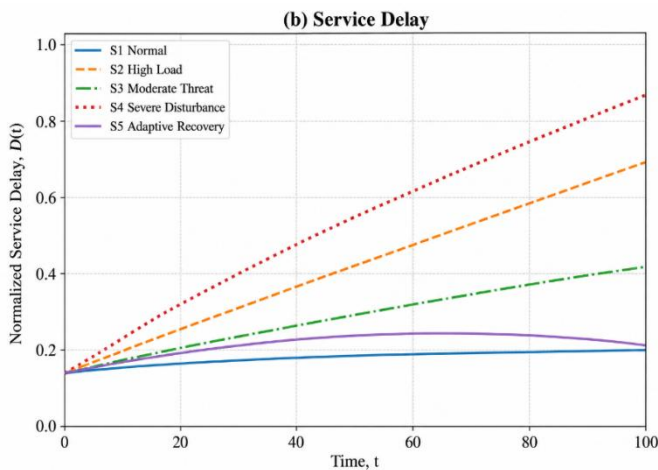


Fig. 4. (a) Service Load; (b) Service Delay under Different Operating Scenarios.

4.2 Cyber-Threat Evolution and Security Response

The threat is low at normal operation with a maximum value of 0.10 (as in Figure 5(a)) and moderate and severe scenarios value 0.42 and 0.82 respectively. The escalation of cyber-threat in this case is therefore to the highest degree of severity. For adaptive recovery, the threat in the beginning is raised, but reaches a maximum value of 0.21, as stated in Table 3. In Figure 5(b) the highest level of security response corresponds to the highest level of threat. With increased activation of the defending system under adaptive-recovery condition, further development of threat is inhibited and recovery of the system is facilitated. The cascading effect of cyber threat intensity and adaptive security response is shown in the combination of Figures 5(a) and 5(b).

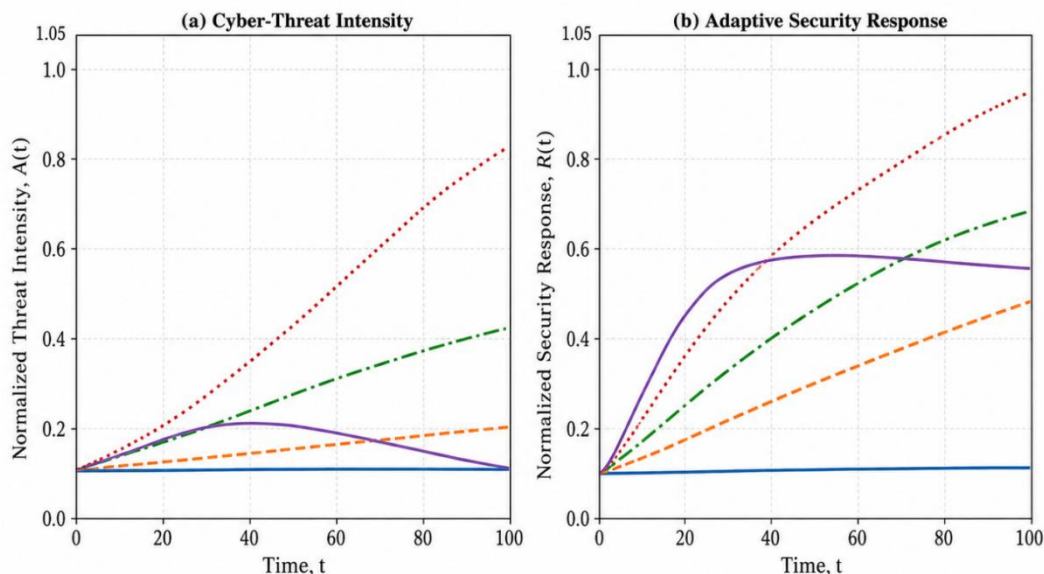


Fig. 5. (a) Cyber-Threat Intensity; (b) Adaptive Security Response over Time.

4.3 Trust Degradation and Recovery

The higher the level of cyber threats and service delay, the lower the level of service trust. Table 3 presents quantitative results indicating that the minimum trust is 0.86 for normal operation, 0.72 for high load operation, and 0.64 for moderate threat operation. Under the severe-disturbance scenario, the minimum trust is 0.43 due to the highest degradation. Adaptive security intervention significantly enhances trust behaviour. In S5 Adaptive Recovery, minimum trust goes up to 0.78, whereas, it is 0.43 in severe disturbance and recovery time is reduced to 24 (from 52) for S5 Adaptive Recovery.

These findings indicate that threat suppression and service delay decrease both trust restoration speed and service delay perception, and these are directly linked to them.

4.4 Scenario-Based Performance Comparison

Table 3 shows a summary of quantitative results for all five scenarios. S1 Normal has an average load of 0.39, peak threat of 0.10, average delay of 0.18, minimum trust of 0.86 and Secure Service Performance Index S_{Pof} of 0.86. As stress to services and security grows, service quality suffers. The recorded peak threat is 0.82, the average delay is 0.51, the lowest trust is 0.43, the recovery time is 52

time units and the lowest S_{Pof} is 0.52 for S4 Severe Disturbance. In contrast, with S5 Adaptive Recovery, peak threat is reduced to 0.21, average delay to 0.22 and recovery time to 24 time units, and minimum

trust to 0.78 and S_{Pto} to 0.80. The comparison is therefore revealing of a clear performance improvement with activation of adaptive security response.

Table 3. Comparative Results of the Five Operating Scenarios

Scenario	Avg. Load	Peak Threat	Avg. Delay	Minimum Trust	Recovery Time	S_p
S1 Normal	0.39	0.10	0.18	0.86	—	0.86
S2 High Load	0.65	0.20	0.43	0.72	38	0.70
S3 Moderate Threat	0.47	0.42	0.29	0.64	31	0.68
S4 Severe Disturbance	0.55	0.82	0.51	0.43	52	0.52
S5 Adaptive Recovery	0.37	0.21	0.22	0.78	24	0.80

4.5 Stability, Sensitivity, and Overall Discussion

The results of the scenario runs show that threat intensity, service load, delay, and response adaptation are parameters which are related to more stable operating behavior. A "normal" situation and "adaptive-recovery" situation yield relatively good levels of services while a "severe disturbance" results in extended low levels of threat, delay, trust and recovery capability. Other models parameterizations suggest that increasing the attack-growth parameter μ leads to increased threat escalation, increasing the security-response parameter δ leads to increased threat suppression, increasing the service-capacity parameter k leads to increased congestion, increasing the trust-recovery parameter η leads to increased trust restoration, and increasing the load-delay parameter p leads to increased non-linear congestion effects. However, it is not recommended to report exact percentages of the parameter-sensitivity unless they are based on the final simulation. So the present analysis is not to be viewed as a complete numerical sensitivity study, but as a recognition of the stability tendencies and influences of the parameters. The results demonstrate the ability of the cyber threats and service demand to work together and impact delay, trust, and resilience for academic libraries and research-data repositories. The nonlinear formulation will include the saturation, feedback and recovery behaviour which can be missed by static linear descriptions. However, this is still a controlled simulation study performed by computation, with assumed parameters and is not validation of an academic network deployed.

5. CONCLUSION

This study tackled the difficulty of modelling the behaviour of internet services in academic libraries and research data systems where the demand for the

service, the threat of the internet, latency, trust and responses to it are all in dynamic interplay. In order to model the security service, a coupled nonlinear secure-service model was developed which has five state variables: service load $L(t)$, cyber-threat intensity $A(t)$, service trust $T(t)$, service delay $D(t)$, and adaptive security response $R(t)$. The framework was developed by seven mathematical equations that reflect the dynamics of loading, the nature of the threat, the trust behavior, the growth of delay, adaptive response, on the overall performance of a secure-service, and on the equilibrium conditions. Five operating scenarios, chosen to be representative of normal service, high load, moderate threat, severe disturbance, and adaptive recovery, were used to test the model, while a stability analysis was performed. Results indicate that as the load grows and the cyber threat level increases, the delay also increases and the level of trust decreases, with severe disturbance causing the maximum service degradation. Adaptive security response, by contrast, enhances threat suppression, speeds recovery and enables better secure-service performance. The framework is also applicable to academic libraries and research-data repositories, as it offers a systematic approach to research on the interactions between resilience and service-security. The study is based, however, on computational assumptions that are controlled and is not a validation of a real deployed academic network. Future studies should comprise parameter calibration with the operational log, real repository traffic, other types of attacks, stochastic extensions, as well as validation in real-life academic information-service environments.

REFERENCES

1. Al-Suqri, M. N., & Akomolafe-Fatuyi, E. (2012). Security and privacy in digital libraries: challenges,

- opportunities and prospects. *International Journal of Digital Library Systems (IJDLS)*, 3(4), 54-61.
2. Anday, A., Francese, E., Huurdeman, H. C., Yilmaz, M., & Zengenene, D. (2012). Information security issues in a digital library environment: A literature review. *Bilgi Dünyası*, 13(1), 117-137.
 3. Andrikopoulou, A., Rowley, J., & Walton, G. (2022). Research data management (RDM) and the evolving identity of academic libraries and librarians: A literature review. *New Review of Academic Librarianship*, 28(4), 349-365.
 4. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50-58.
 5. Ashiq, M., Usmani, M. H., & Naeem, M. (2022). A systematic literature review on research data management practices and services. *Global Knowledge, Memory and Communication*, 71(8-9), 649-671.
 6. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of internet services and applications*, 4(1), 5.
 7. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, 4(6), 1802-1831.
 8. Owusu-Ansah, S., & Budu, S. (2021). Developing a Cloud Computing Framework for University. *e-Services*, 101.
 9. Singh, V., & Margam, M. (2018). Information security measures of libraries of Central Universities of Delhi: A study. *DESIDOC Journal of Library & Information Technology*, 38(2), 102-109.
 10. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, 34(1), 1-11.
 11. Raja, M. S., Muniyandy, E., Ambika, K. S., Rajeswari, P., Gadam, H., Mondal, A., & Kumar, M. (2026). Secure Routing and Attack Detection in VANETs Using BCS-DMCO Optimization. *SN Computer Science*, 7(5), 563.
 12. Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, 160, 102642.
 13. Waddington, S., Zhang, J., Knight, G., Jensen, J., Downing, R., & Ketley, C. (2013). Cloud repositories for research data-addressing the needs of researchers. *Journal of Cloud Computing: Advances, Systems and Applications*, 2(1), 13.
 14. Wang, J., & Chen, X. (2016). Efficient and secure storage for outsourced data: a survey. *Data Science and Engineering*, 1(3), 178-188.
 15. Yu, H. H. (2017). The role of academic libraries in research data service (RDS) provision: Opportunities and challenges. *The Electronic Library*, 35(4), 783-797.
 16. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, 28(3), 583-592.