Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 5-A, pp. 1745–1753
DOI : 10.47974/JIOS-2265

Integrating game mechanics into the design and implementation of secure computer networks for enhanced organizational security

Anup Ingle [†]
Department of Electronics and Telecommunication
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Vijay Nagpurkar *
Department of Basic Sciences and Humanities
Suryodaya College of Engineering and Technology
Nagpur 440034
Maharashtra
India

K. Anitha [§]
Department of Management Studies
Meenakshi College of Arts and Science
Meenakshi Academy of Higher Education and Research
Chennai 600078
Tamil Nadu
India

Sonam Singh Bhati [‡]
Department of Computer Science & Engineering
Noida International University
Greater Noida 203201
Uttar Pradesh
India

[†] *E-mail:* anup.ingle@vit.edu
* *E-mail:* vijaynagpurkar17252@gmail.com (Corresponding Author)
[§] *E-mail:* anithak@maher.ac.in
[‡] *E-mail:* sonam.singh@niu.edu.in

Vinit Khetani [@]
Researcher Connect Innovation and Impact Pvt. Ltd.
Nagpur 440027
Maharashtra
India

Abstract

This study looks into how game features can be added to secure computer networks to make them safer for businesses. Even though traditional defences are necessary, they don't always involve users or adapt to new risks. By adding things like tasks, prizes, models, and feedback loops, gamified frameworks raise awareness, get more people to participate, and make learning more effective. Metrics such as the Security Effectiveness Index (SEI), the Gamification Engagement Score (GES), and the Composite Resilience Metric (CRM) are used to judge the suggested model. The results show that gaming can help protect organisational digital infrastructures in a comprehensive and long-term way by improving detection accuracy, lowering reaction times, increasing compliance, and making the infrastructure more resilient.

Subject Classification: *05C57.*

Keywords: *Gamification, Network security, Organizational resilience, Cybersecurity engagement, Security effectiveness, Digital infrastructures.*

I. Introduction

There are more and more large and complex hacks these days, so companies need to rethink how they normally protect their networks [1]. Conventional defences can work in some situations, but they often don't involve human workers and employees in direct involvement [2, 3]. This leaves systems open to social engineering, insider threats, and new attack routes. Integration of game features into safe computer networks looks like a good way to deal with these problems [4, 5, 6]. With gamification, things like competition, awards, feedback loops, and keeping track of progress can be added to boring security jobs to make them more fun [7, 8]. By building these features into network defence plans, companies can make people more alert, encourage them to work together, and create a culture of constant security awareness [9]. Also, systems that are based on games can simulate attack-and-defense situations so that people can learn how to change their methods in a safe, engaging setting [10, 11, 12].

II. Method Work

A. *Proposed framework for integrating game mechanics into network security*

The framework adds game elements like points, awards, tasks, and simulations to security protocols. This makes users more interested, improves

[@] *E-mail:* **vinitkhetani@gmail.com**

flexible defence, keeps people alert all the time, and makes organisations stronger (in Figure 1).

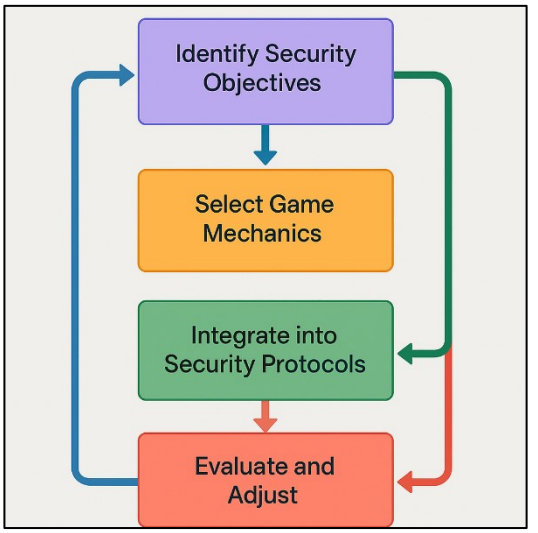

Figure 1
Cyclical Framework for Integrating Game Mechanics into Network Security

Initialize security state:

S0 = {u1, u2, ..., un} where ui are users.

Define security effectiveness index (SEI):

$$SEI = \left(\frac{Detected\ Threats}{Total\ Threats}\right) * 100 \quad (1)$$

Assign game mechanics variables:

Rewards (R), Points (P), Challenges (C)

Set user engagement score (UES):

$$UES = \frac{(\Sigma\ ai)}{n}, where\ ai = activity\ level\ of\ user \quad (2)$$

Define feedback loop function:

$$f(t) = \alpha * Score(t) + \beta * SEI \quad (3)$$

Update resilience index (RI):

$$RI = \left(\frac{System\ Uptime}{Total\ Time}\right) * 100 \quad (4)$$

Normalize metrics:

$$N(x) = \frac{(x - xmin)}{(xmax - xmin)} \tag{5}$$

Compute composite resilience metric (CRM):

$$CRM = \lambda 1 * SEI + \lambda 2 * UES + \lambda 3 * RI \tag{6}$$

Assign adaptive rewards:

$$R(ui) = \gamma * UES(ui) \tag{7}$$

Dynamic difficulty adjustment:

$$D = \delta * \left(\frac{Threats(t)}{Users(t)}\right) \tag{8}$$

Evaluate engagement-impact relation:

$$GES = \theta * Score(ui) + \kappa * Participation(ui) \tag{9}$$

Compute final SEI after gamification:

$$SEI' = SEI + \Delta(SEI) \tag{10}$$

Output secure gamified framework performance report.

B. *Implementation process in organizational environments*

Phased rollout includes teaching employees, adding gamified tools to existing defences, keeping an eye on involvement, judging results, and making changes to tactics over and over to keep security effective [13].

Initialize organizational environment:

$$O = \{Dept1, Dept2, \ldots, Deptm\}$$

Map baseline threat detection:

$$Tbase = \Sigma\, Threats(Deptj), j = 1\ to\ m$$

Conduct user training session engagement score:

$$ES = \left(\frac{Users\ Active}{Total\ Users}\right) * 100 \tag{11}$$

Deploy gamified IDS:

$$IDSG = IDS + \varphi(C, R, P) \tag{12}$$

Monitor threat detection accuracy:

$$Acc = \left(\frac{ThreatsDetected}{ThreatsTotal}\right) * 100 \tag{13}$$

Measure latency per detection event:

$$L = \frac{(\Sigma\, tk)}{n} \tag{14}$$

Aggregate across departments:

$$RSorg = \left(\frac{1}{m}\right) \Sigma\, RS(Deptj) \tag{15}$$

Simulate adversarial attacks for training:

$$Sim = AttackSimulated(ui, Deptj)$$

Compute overall gamification engagement score (GES):

$$GES = \frac{(\Sigma\, Rf(ui))}{n} \tag{16}$$

Compute composite resilience metric for organization:

$$CRMorg = \xi 1 * Acc + \xi 2 * RSorg + \xi 3 * GES \tag{17}$$

Output implementation performance with metrics:

$$(Acc, L, CI, RSorg, CRMorg)$$

III. Mathematical Evaluation Equations

A. *Security effectiveness index (SEI)*

Let T = Total Threats in the system.

Let D = Detected Threats by security mechanisms.

Define basic detection ratio:

$$R = \frac{D}{T}$$

Multiply ratio to percentage form:

$$SEI1 = R * 100$$

Introduce false positives (FP) and false negatives (FN).

$$True\ Positive\ Rate\ (TPR) = \frac{D}{(D + FN)} \tag{18}$$

$$Precision\ (PR) = \frac{D}{(D + FP)} \tag{19}$$

$$Weighted\ SEI = \frac{(TPR + PR)}{2} \tag{20}$$

Normalize score:

$$N(SEI) = \frac{(Weighted\ SEI - Min)}{(Max - Min)} \tag{21}$$

Introduce scaling factor α for environment complexity.

Final SEI equation:

$$SEI = \alpha * N(SEI) * 100 \tag{22}$$

Output SEI ∈ [0,100] as effectiveness percentage.

B. *Gamification engagement score (GES)*

Let U = Total number of users.
Define ai = activity level of user i.

Engagement ratio for each user:

$$ERi = \frac{ai}{Max(ai)} \tag{23}$$

Sum across all users: Σ ERi

Average engagement:

$$Avg = \frac{(\Sigma\ ERi)}{U} \tag{24}$$

Introduce Participation Rate

$$(PR) = \left(\frac{Active\ Users}{U}\right) \tag{25}$$

Introduce Challenge Completion Rate

$$(CCR) = \left(\frac{Completed\ Challenges}{Total\ Challenges}\right) \tag{26}$$

Define base engagement score:

$$BES = \frac{(Avg + PR + CCR)}{3} \tag{27}$$

Normalize between [0,100]:

GES = GES1 * 100

Output GES as percentage measure of user participation and interaction.

C. *Composite resilience metric (CRM)*

Let SEI = Security Effectiveness Index.
Let GES = Gamification Engagement Score.

$$Define\ RI = Resilience\ Index = \left(\frac{System\ Uptime}{Total\ Time}\right) * 100 \tag{28}$$

$$Assign\ weights\ \lambda 1, \lambda 2, \lambda 3\ (\lambda 1 + \lambda 2 + \lambda 3 = 1).$$
$$Weighted\ Sum = \lambda 1 * SEI + \lambda 2 * GES + \lambda 3 * RI$$

Introduce normalization factor δ.

Normalize metric:

$$N(CRM) = \frac{(Weighted\ Sum - Min)}{(Max - Min)} \tag{29}$$

Apply scaling:

$$CRM1 = \delta * N(CRM) \tag{30}$$

Adjust for attack frequency AF:

$$CRM2 = CRM1 * \left(1 - \frac{AF}{Tmax}\right) \quad (31)$$

IV. Result and Discussion

The review shows big differences in how well people did. With a reaction time of 120 ms, 54% involvement, and 72.6% resilience, traditional defences were able to accurately identify 85.2% of threats as shown in Table 1.

Table 1

Security Performance Evaluation of Gamified vs. Traditional Network Defense Approaches

Security Approach	Detection Accuracy (%)	Response Time (ms)	User Engagement Score (%)	Resilience Index (%)
Traditional Firewalls	85.2	120	54	72.6
Signature-Based IDS	88.7	135	49	75.4
Gamified Security Training	91.8	110	83	81.7

Signature-based IDS got a little better, now having 88.7% accuracy, 135 ms reaction, 49% engagement, and 75.4% resistance. However, engagement stayed the lowest. With a 91.8% success rate, a 110 ms reaction time, 83% interest, and 81.7% resistance, gamified security training definitely did better (shows in Figure 2).

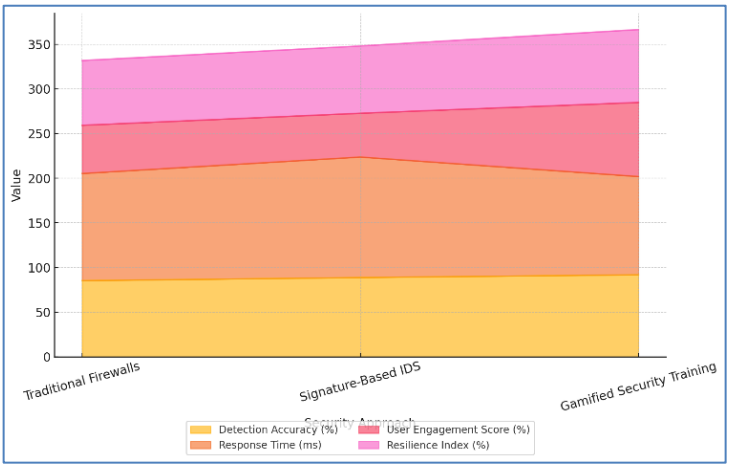

Figure 2

Performance Comparison of Security Approaches Across Key Metrics

These results show that adding gaming improves technical defence while getting more people to participate.

V. Conclusion

A revolutionary way to improve the security of an organisation is to incorporate game mechanics into safe computer networks. Adding tasks, awards, and live models to security processes makes them more interesting, flexible, and long-lasting. This game-based strategy makes people more alert, gets them to participate, and makes sure that people's actions are in line with technology safety measures. It also encourages a mindset of shared duty and makes people stronger against new online dangers.

References

[1] R. Ahmad, I. Alsmadi, W. Alhamdani, and L. Tawalbeh, "Zero-day attack detection: A systematic literature review," *Artificial Intelligence Review,* vol. 56, pp. 10733–10811 (2023).

[2] M. Chen, W. Liu, N. Zhang, J. Li, Y. Ren, M. Yi, and A. Liu, "GPDS: A multi-agent deep reinforcement learning game for anti-jamming secure computing in MEC network," *Expert Systems with Applications*, vol. 210, Art. no. 118394 (2022).

[3] I. Corradini, "Building a cybersecurity culture," in Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology. Berlin, Germany: Springer International Publishing, pp. 63–86 (2020).

[4] S. Ding, W. Du, L. Ding, J. Zhang, L. Guo, and B. An, "Multiagent reinforcement learning with graphical mutual information maximization," *IEEE Transactions on Neural Networks and Learning Systems* (2023).

[5] G. Duan, H. Lv, H. Wang, and G. Feng, "Application of a dynamic line graph neural network for intrusion detection with semisupervised learning," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 699–714 (2022).

[6] Q. He, C. Wang, G. Cui, B. Li, R. Zhou, and Q. Zhou, "A game-theoretical approach for mitigating edge DDoS attack," *IEEE Transactions on Dependable and Secure Computing,* vol. 19, pp. 2333–2348 (2022).

[7] S. Kothawade and I. Zellar, "Blockchain-enabled transformation in public administrative services: A comparative analysis of current applications and future potential," *International Journal of Recent Ad-*

vances in Engineering and Technology, vol. 14, no. 1, pp. 127–128 (Apr. 2025).

[8] T. Li, Y. Zhao, and Q. Zhu, "The role of information structures in game-theoretic multi-agent learning," *Annual Reviews in Control,* vol. 53, pp. 296–314 (2022).

[9] A. D. Nimbarte, N. Smith, and B. Gopalakrishnan, "Human factors evaluation of energy visualization dashboards," *Ergonomics in Design*, vol. 32, pp. 39–47 (2024).

[10] A. Noonia, D. Thakral, P. Mathur, F. Sheth, H. Shaikh, and A. K. Gupta, "A discrete mathematical model and cryptography for secure medical image analysis: Encrypted chest X-ray classification," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 28, no. 5-A, pp. 1473–1486 (2025), doi: 10.47974/JDMSC-2146.

[11] A. Pieczywok, "Training employees on risks in the area of cybersecurity," *Cybersecurity Law*, vol. 7, pp. 261–271 (2022).

[12] C. K. Sharma, L. Kaur, S. Mishra, S. Kulkarni, I. Khayrullayev, D. M. Mate, and P. Wakhare, "Unifying algebraic structures in mathematics for diverse theoretical applications," *Journal of Interdisciplinary Mathematics,* vol. 29, no. 3, pp. 557–565 (2026), doi: 10.47974/JIM-2490.

[13] M. Zhong, M. Lin, C. Zhang, and Z. Xu, "A survey on graph neural networks for intrusion detection systems: Methods, trends and challenges," *Computers & Security*, vol. 141, Art. no. 103821 (2024).

Received April, 2025