

CyberYuruGu: An Interpretative Gameplay Model Grounded in African Epistemology for Explainable Cybersecurity Reasoning and Human–AI Sense-Making

Thami Sithole, Phil van Deventer and Mike wa Nkongolo

Department of Informatics, Faculty of Engineering, Build Environment and Information Technology, University of Pretoria, Pretoria, South Africa

u22835416@tuks.co.za

phil.vandeventer@up.ac.za

mike.wankongolo@up.ac.za

Abstract. Cybersecurity education and serious games have long been dominated by Western-centric paradigms, leaving limited space for indigenous epistemologies that emphasise interpretative reasoning. To address this gap, CyberYuruGu is developed in this study as a cybersecurity game inspired by the Dogon Fox tradition. Unlike abductive reasoning or Bayesian inference, the Dogon Fox system encodes uncertainty through symbolic spatial traces, requiring interpretative reconstruction rather than probabilistic prediction. This resonates with Bachelard’s notion of epistemological rupture, where disruption and discontinuity are not obstacles but productive sources of new knowledge. Embedded within a socio-technical framework informed by constructivist pedagogy and ethno-informatics, the game enables participants and a large language model (LLM) to collaboratively interpret gameplay data. This design allows them to reconstruct multi-layered attack scenarios under conditions of uncertainty. Developed in Python using Pygame, OpenGL, and WebGL, CyberYuruGu records gameplay traces as participants place attack and defence tokens, infer adversarial intent, and construct defensive narratives. Results revealed a cognitive bias toward protective reasoning, as defence paths achieved higher cumulative scores (8) than attack paths (5). While participants occasionally formed strong offensive sequences, defensive reasoning remained more consistent and complete. Thus, the Dogon Fox model contributes a relational and cosmological logic of trace interpretation that complements but is not captured by conventional probabilistic or abductive models.

Keywords. Cybersecurity game, Ethno-informatics, Epistemology, Artificial intelligence

1. Introduction

Cybersecurity extends beyond technical expertise to include behavioural awareness, enabling users to recognise, prevent, and respond to incidents (Hasan et al., 2026). As digital systems expand, awareness becomes central to digital literacy because human behaviour remains a major attack surface exploited through social engineering. Several serious games such as, CyberMoraba, CyberCIEGE, CyberStart, CTRL-ALT-Hack, R00tz Asylum, and CyberShield (Poovizhi et al., 2026) support cybersecurity awareness but largely emphasise technical problem-solving (Table 1). These approaches overlook indigenous epistemic perspectives, leaving symbolic reasoning and contextual interpretation underrepresented. This study addresses that gap by integrating Dogon Fox divination knowledge into serious game design to advance explainable cybersecurity decision-making (XCDM).

2. Literature Review

2.1 Dogon fox Divination System

The Dogon Fox divination knowledge originates from the Dogon people of Mali in West Africa and is grounded in Dogon cosmology through the figure of Yurugu (the Pale Fox), associated with disorder, knowledge, and revelation (Ani, 1994). The divination process employs a sand grid prepared at dusk, where sticks, grains, or seeds are spatially arranged to encode questions concerning uncertainty in social, personal, or environmental life. These questions are not expressed linguistically but symbolically through placement and orientation, forming a relational configuration within a cosmological framework (Figure 1). During the night, Yurugu is believed to traverse the grid, leaving traces that are interpreted at dawn, so that meaning arises from transformation rather than the initial state. In cybersecurity forensics, analysts reconstruct adversarial behavior from fragmented logs and incomplete traces, often using abductive reasoning or Bayesian inference to reduce uncertainty to a single explanatory path. By contrast, Dogon reasoning treats uncertainty as a generative condition: meaning arises relationally from Yurugu’s disrupted traces, embedded in a cosmological framework. This differs from forensic log analysis, which is probabilistic and reductionist, by emphasising symbolic and contextual reconstruction. Drawing on Bachelard’s philosophy of epistemological rupture (Gaukroger, 1976), the Dogon model frames disruption not as error but as the very ground of insight. Just as Bachelard argued that scientific progress emerges through breaks and discontinuities, Yurugu’s traces exemplify how uncertainty itself

can become productive, enabling interpretative reconstruction rather than deterministic closure. Thus, the Dogon Fox model contributes a relational and cosmological logic of trace interpretation that complements but is not captured by conventional probabilistic or abductive models. This epistemic approach aligns closely with cybersecurity analysis, where adversarial actions must be inferred from incomplete logs, fragmented traces, and anomalous system states. We operationalise this logic computationally by proposing the CyberYuruGu game, which requires players to infer attack–defense narratives from final board states rather than directly observed actions, making the game compatible with explainable cybersecurity forensics (XCF) and trace-based adversarial analysis (TbAN). From an ethno-informatics perspective, the Dogon Fox system functions as a symbolic information-processing framework that transforms encoded inputs into interpretable knowledge through contextual reasoning. This structure closely resembles modern artificial intelligence (AI) pipelines in which large language models (LLMs) integrate symbolic representations, probabilistic inference, and explanatory narratives to support decision-making under uncertainty.

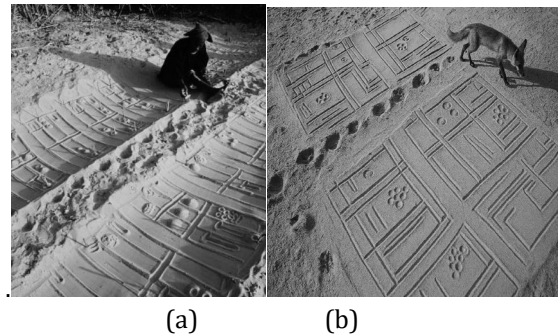


Figure 1: (a) The diviner sets question. (b) Yurugu is believed to communicate directly with the supreme Dogon god Ama (Ani, 1994). Figure 1(b) is AI-generated

Table 1: Comparative analysis of cybersecurity and narrative game systems

Dimension	CyberMoraba	CyberCIEGE	CyberStart	CTRL-ALT-Hack	R00tz Asylum	CyberShield	CyberYuruGu
Foundation	Puzzle logic	Procedural simulation	Gamified challenges	Attacker mindset	Hacker culture	Defense scenarios	Dogon epistemology, relational inference, Bachelard's rupture
Gameplay	Quiz mechanics	Networks simulation	Progressive	Card game	Hack labs	Training	Post-hoc interpretative
Learning	Cyber awareness	Risk management	Technical skill	Engineering	Hacker ethics	Strategies	Explainable human–AI collaboration
Uncertainty	Predefined answers	Deterministic	Fixed	Fixed	Open-ended	Predefined	Traces reconstructed narratively
AI	None	Limited	None	None	None	None	LLM-assisted judgment + ML analysis
Target	Students	Professional	Intermediate	Students	Teens	Workforce	IT professionals, researchers

Dimension	CyberMoraba	CyberCIEGE	CyberStart	CTRL-ALT-Hack	R00tz Asylum	CyberShield	CyberYuruGu
Novelty	Awareness through local cultural game	Enterprise simulation	Online platform	Attacker roleplay	Hacker camp pedagogy	Awareness training	Ethno-informatics paradigm, cultural inclusivity

While the Dogon Fox model illustrates how knowledge can emerge from relational inference, most cybersecurity approaches remain bound to deterministic paradigms focused on compliance and predefined metrics. Yet adversarial behaviour unfolds through uncertainty, partial visibility, and emergent patterns that resist static classification. Without frameworks for reconstructing meaning from incomplete traces, such systems struggle to support adaptive learning. CyberYuruGu addresses this gap by embedding Dogon epistemic logic into a socio-technical context, shifting analysis from reactive detection to interpretative post-hoc reasoning. By requiring participants to infer attack–defence narratives from final board states, the game cultivates reasoning under uncertainty, bridging technical precision with human interpretive insight. This integration strengthens explainable cybersecurity forensics and introduces a culturally inclusive paradigm for sense-making in complex digital environments (Krisnasari et al., 2025).

2.2 Large Language Models in Cybersecurity Games

Traditional narrative games rely on procedural logic to guide story progression, whereas LLM-driven games support emergent storytelling (Park, et al., 2023; B. Wang et al., 2026). A large language model (LLM) is trained on extensive datasets of text, images, and videos to learn statistical patterns for natural language understanding and generation (Figure 2). While LLMs increase narrative flexibility, they often lack interpretability (Table 1). Transformer architectures enable context-aware outputs for dialogue, summarization, translation, and reasoning, but unconstrained generation can lead to inconsistency and weak narrative structure. Post-hoc correction methods such as LLM-as-judge or persona fine-tuning can improve coherence while maintaining interpretability (Table 1). Our study presents a serious game environment—a simulated cyber board inspired by African epistemology, where narrative reasoning and interpretative reconstruction are supported by LLM-based judgment, independent of equilibrium assumptions (Figure 2).

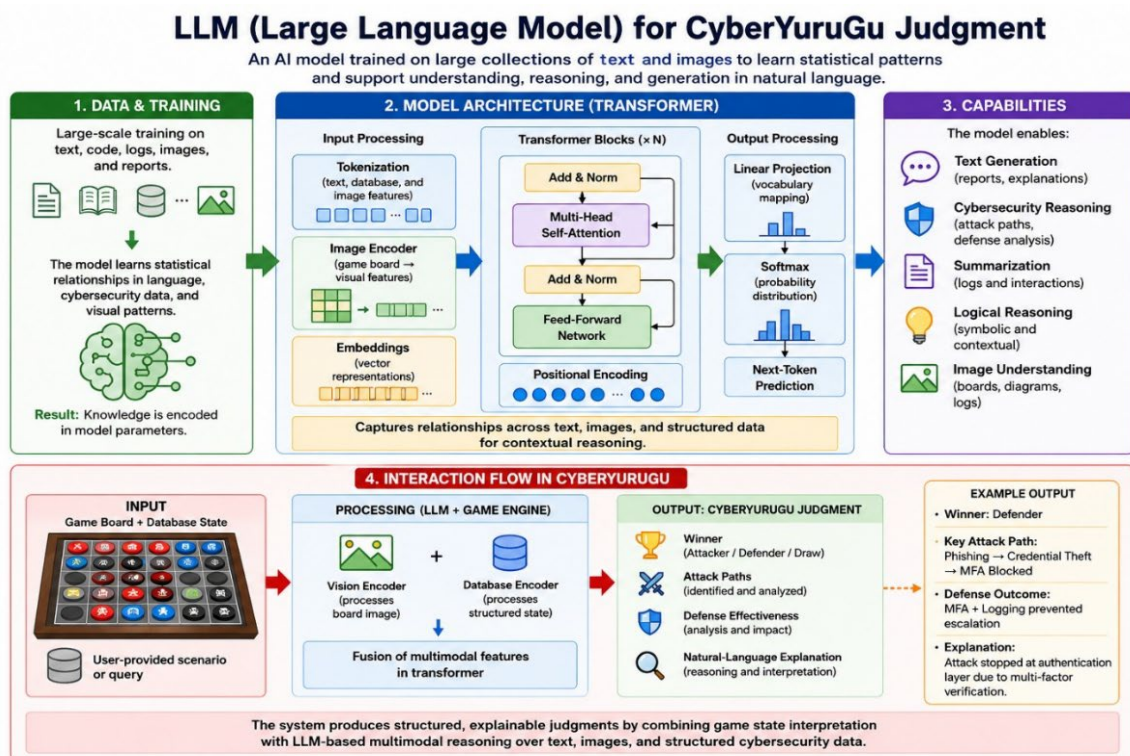


Figure 2: Proposed LLM architecture with socio-technical lens. *Image generated with AI*

2.3 Explainable AI in Cybersecurity and Educational Games

Recent advances in explainable AI (XAI) highlight the importance of interpretability in machine learning (ML) models. Techniques such as LIME and SHAP provide transparency by explaining classifier predictions and feature importance. While these methods emphasise mathematical fidelity, CyberYuruGu extends explainability into the interpretative domain, reconstructing traces narratively rather than reducing them to feature weights. This positions CyberYuruGu as complementary to XAI, treating uncertainty as a generative source of meaning rather than a statistical gap. In cybersecurity, surveys (Charmet et al., 2022; Dehbashi Sani & Olapojoye, 2026) note that most XAI applications remain limited to technical transparency, constrained by scalability and adversarial robustness. CyberYuruGu responds by embedding Dogon epistemology into forensic reasoning, showing how cultural logics of disruption and relational inference enrich explainable cybersecurity beyond transparency, toward contextual and narrative reconstruction. Educational game design has also evolved to support cybersecurity awareness. Reviews (Weeratunge et al., 2025; Matus, Berríos, & Isla, 2026) highlight that most games emphasise procedural challenges rather than interpretative reasoning. CyberYuruGu diverges by introducing post-hoc interpretative gameplay, where players reconstruct attack–defence narratives from traces. This aligns with constructivist pedagogy and interpretative learning theory, offering a novel paradigm that treats uncertainty as epistemically productive.

3. Methodology

Thirty IT professionals (25–48 years, mean = 34; 60% male, 40% female) with at least two years of IT security or system administration experience were recruited via industry mailing lists. Each provided informed consent and played individually in sessions of about 25 minutes (15 minutes gameplay, 10 minutes evaluation). Participants placed attacker and defender tokens on a layered grid, producing final board states. Defence scored when attacks were disrupted; attack scored when reaching the data layer. Outcomes were validated through human evaluation and the LLM_JUDGE algorithm. The algorithm mapped gameplay traces (tokens, layers, adjacency) into heuristic rules, reconstructing attack paths and defensive disruptions with natural-language explanations. It operated post-hoc to ensure reproducibility and transparency. Data were pre-processed and split into training (80%) and testing (20%) subsets (Table 2). Two ML models classified and predicted cybersecurity knowledge levels, providing quantitative insights into reasoning patterns.

Table 2: Gameplay data

Game_id	Player	Token	Row	Column	Layer	Time	Label	Code
1779584000	Attack	Misconfig	4	1	Network	20 minutes	Attack_path	1
1889584111	Attack	Zero-day	2	0	User	23 minutes	Partial (draw)	2
1999584222	Defence	Zero-trust	6	3	Application	22 minutes	Defence_path	0

3.1 Socio-technical and Constructivist Theory

CyberYuruGu is implemented through a socio-technical lens informed by constructivist pedagogy and ethno-informatics (Wang, 2026). Rather than immediate win/lose outcomes, players build narratives evaluated in a post-game judgment phase, mirroring real cybersecurity incident reconstruction. This reflects experiential learning theory, where knowledge emerges through interpretation of situated experiences. The gameboard represents a layered network, with each cell as a potential action or vulnerability point. The interface, built in Python with OpenGL, renders game states, while reasoning, scoring, and evaluation occur in a separate logic layer. Tokens are displayed as red (attacker) and blue (defender) shapes (Figure 3).

3.2 Game Phases and Complexity

During *initialisation*, the gameboard is created as a layered grid representing the *User (U)*, *Network (N)*, *Application (A)*, and *Data (D)* domains (Figure 3). Let the total number of available cells be G , where $G = U + N + A + D$ and U, N, A, D , denote the number of cells in each respective layer. In the current implementation, each layer comprises eight cells, giving $G = 32$. The attacker places k_A red tokens representing offensive tactics such as phishing, misconfiguration, or zero-day exploits (Figure 3). The number of ways to choose these tokens from the grid is given by the binomial coefficient:

$$\binom{G}{k_A} = \frac{G!}{k_A! \cdot (G - k_A)!}$$

For $G = 32$ and $k_A = 5$,

$$\binom{32}{5} = 201,376$$

This represents all possible attacker configurations when order is irrelevant. If sequential attack paths are considered, the permutation form applies:

$$P(G, k_A) = \frac{G!}{(G - k_A)!}$$

The defender places blue tokens representing security controls such as multifactor authentication (MFA), firewalls, or encryption (Figure 3). The number of possible placements is similarly defined as $\binom{G}{k_D} = \frac{G!}{k_D! \cdot (G - k_D)!}$ since attacker tokens occupy part of the grid, the defender's available space becomes $G - k_A$. Thus,

$$\binom{G - k_A}{k_D} = \frac{(G - k_A)!}{k_D! \cdot (G - k_A - k_D)!}$$

For $G = 32$, $k_A = 5$, and $k_D = 5$:

$$\binom{27}{5} = 80,730$$

The combined attacker–defender configuration (C) is the product of both combinatorial sets

$$C = \binom{G}{k_A} \cdot \binom{G - k_A}{k_D}$$

Substituting the values yields $C = \binom{32}{5} \cdot \binom{27}{5} = 201,376 \times 80,730 \approx 16,229,000,480$. The game produces over 16 billion unique configurations, highlighting the interpretative complexity of trace-based reasoning. This combinatorial richness makes exhaustive deterministic computation infeasible, thereby justifying the use of LLM-augmented evaluation. The game ends once all tokens are placed on the board, after which the judgment phase begins, where an LLM (ChatGPT) analyses attacker and defender traces to reconstruct possible attack paths from the User to the Data layer; defenders score if they disrupt a path, otherwise attackers gain points. In the evaluation phase, players compare human scoring with the LLM-generated report, concluding with winner determination and feedback on attack strategies, defensive gaps, and improvements through a human-in-the-loop LLM-assisted framework.

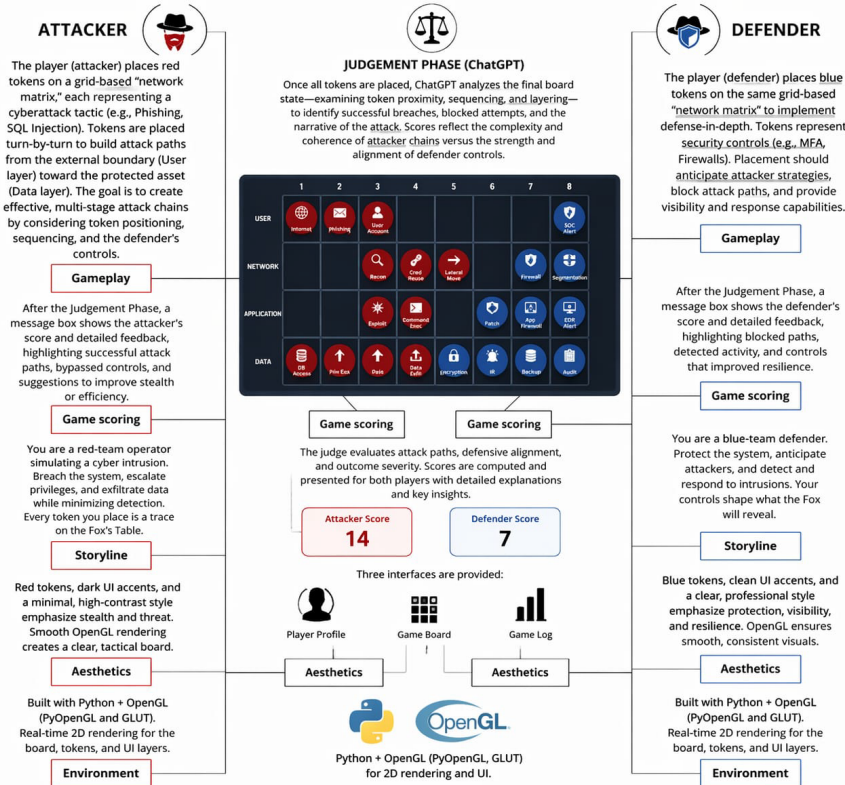


Figure 3: Proposed gameplay. Image generated with AI

3.3 Entity Heuristic Mapping

The LLM judges gameplay by mapping relational entities in the database (Figure 4) to interpretative heuristics rather than isolated actions. The board enforces structural constraints across layers while rounds provide context and roles define token sequences for coherence. Token attributes—type, layer position, adjacency, and sequence—support heuristic reconstruction of attack paths, including blocking, bypassing, detection, and response. Combined with outcome and feedback data, these elements enable graded judgments (Algorithm 1).

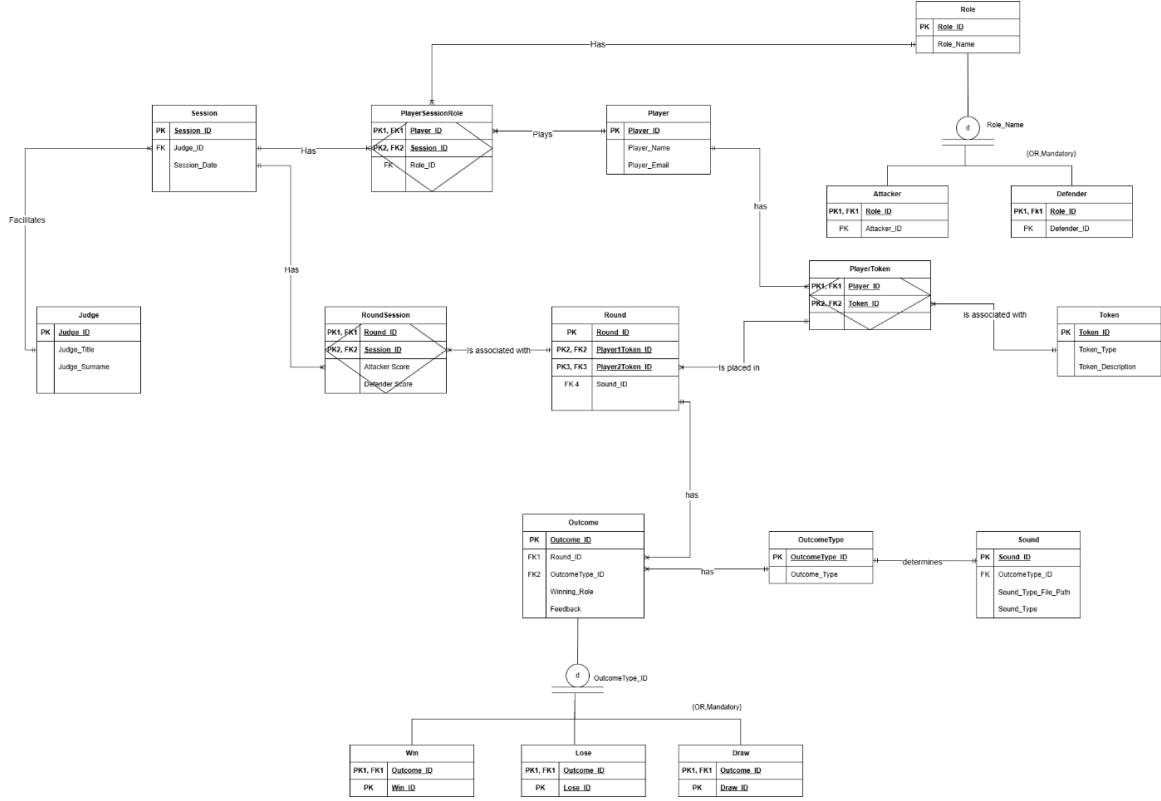


Figure 4: Extended entity relationship diagram (EERD) of CyberYuruGu

Algorithm: LLM_JUDGE

Input:

GameState $G = (\text{Board}, \text{Layers}, \text{Round}, \text{Sessions}, \text{Roles}, \text{Tokens})$. Let $G = (B, L, R, S, \rho, T)$ where B is the board matrix with 4 layers $L = \{L_1, L_2, L_3, L_4\}$ (Figure 5), R is the set of rounds, S the set of sessions, ρ the set of roles (attacker, defender), and T the set of tokens. Each token $t_i \in T$ is defined by a tuple $t_i = (\varphi_i, \theta_i, \gamma_i)$ where φ_i denotes its layer position, θ_i its types (attack-defense), and γ_i its adjacency relation to other tokens.

Output:

Outcome $\in \{\text{Win}, \text{Draw}, \text{Lose}\}$ with feedback ($F(G)$)

1. Validation phase

The algorithm first ensures consistency: $\forall r \in R, |\rho_r| = 2, |\rho_r^{\text{attacker}}| = |\rho_r^{\text{defender}}| = 1$ and verifies cardinality: $|T^{\text{attacker}}| = k_A, |T^{\text{defender}}| = k_D$ ensuring mandatory participation and balanced gameplay (Figure 6).

2. Frame phase

Mapping function is implemented: $f_L: L_i \rightarrow L_{i+1}$ which establishes admissible transitions between consecutive L (Figure 6). The adjacency matrix A encodes valid token connections (Table 3):

$$A_{ij} = \begin{cases} 1, & \text{if token } t_i \text{ can transition to } t_j \\ 0, & \text{otherwise} \end{cases}$$

3. Paths reconstruction

To reconstruct the path, all plausible attacker paths are inferred using adjacency and sequence constraints:

$$P_A = \{p_k | p_k = (t_1, t_2, t_3, \dots, t_n), A_i, i + 1 = 1, \theta_i = \text{attack}\}$$

The total number of possible paths is bounded by the combinatorial space:

$$|P_A| \leq \binom{G}{k_A}$$

4. Path evaluation

For each path $p_k \in P_A$, the algorithm defines the blocking function (Table 3):

$$\beta(p_k) = \begin{cases} 1, & \text{if } \exists t_d \in T^{\text{defender}} \text{ s.t. } \varphi_d = \varphi_a \text{ and } \theta_d \text{ blocks } \theta_a \\ 0, & \text{otherwise} \end{cases}$$

The propagation rule is as follows: $p_k^{\text{next}} = \begin{cases} \text{terminate}, & \beta(p_k) = 1 \\ F_L(p_k), & \beta(p_k) = 0 \end{cases}$

5. Impact assessment

In this phase, the algorithm defines the impact function

$$I(p_k) = \begin{cases} w_A, & \text{if } p_k \text{ reaches Data (D) layer} \\ w_D, & \text{if } p_k \text{ terminates before D} \end{cases}$$

where w_A , and w_D are weighted scores for attacker success and defender prevention.

6. Comparative evaluation

The overall game outcome is determined by comparing cumulative impacts:

$$\nabla(G) = \sum_{p_k \in P_A}^n I(p_k) \text{ and applying role-conditioned heuristics:}$$

$$\Delta(G) = \begin{cases} \text{Win}_A, & \nabla(G) > \mu_A \\ \text{Win}_D, & \nabla(G) < \mu_D \\ \text{Draw}, & \mu_D \leq \nabla(G) \leq \mu_A \end{cases}$$

where μ_A and μ_D are threshold parameters learned or tuned by the LLM.

7. Decision and feedback generation

In this phase, the LLM generates feedback $F(G) = \psi(\nabla(G), P_A, T^{\text{defender}})$ where ψ is a multimodal reasoning function combining textual, visual, and symbolic traces to produce natural-language explanations (NLE).

8. Final output

Finally, the algorithm returns outcome with feedback:

$$\text{Outcome} = \Delta(G), \text{ feedback} = F(G)$$

Algorithm 1. LLM judge specification.

4. Results

4.1 Game Prototype

Participants provided informed consent, and all gameplay data were anonymised to ensure privacy. The LLM was used strictly as a decision-support tool within the experimental setup, maintaining ethical and responsible human–AI interaction. The LLM_JUDGE algorithm goes beyond statistical classification by mirroring the Dogon Fox divination principle, where meaning arises relationally from disrupted traces rather than direct observation. In this framework, adjacency, sequence, and layer transitions function as symbolic relations that reconstruct

narratives under uncertainty. Incomplete traces are treated not as noise to be eliminated but as epistemic conditions that generate new interpretative insight, reflecting a cultural logic of disruption and transformation.

Collision detection. When four adjacent blocks of the same colour collide, they form a cluster that is removed, refreshing the board for new token placement (Figure 5).

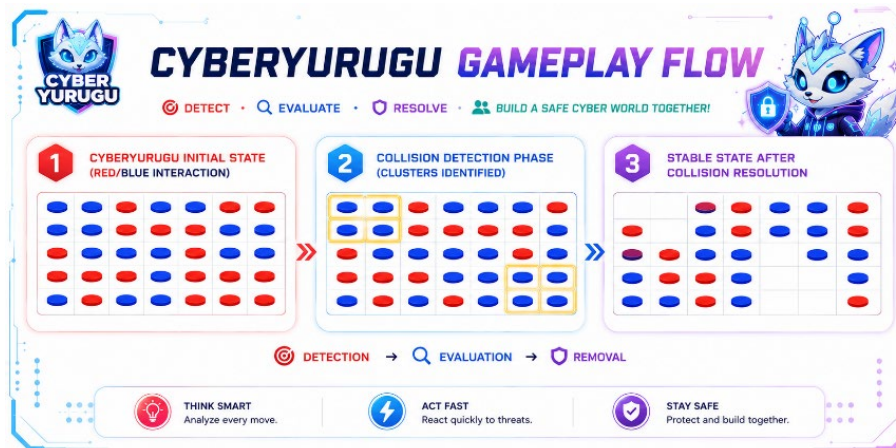


Figure 5: Collision detection

This removal is accompanied by a burst animation symbolising conflict resolution, where homogeneous entities neutralise each other. The effect provides visual feedback and metaphorically represents the completion of a cybersecurity interaction cycle, creating space for new engagements within the simulation (Figures 6–7).

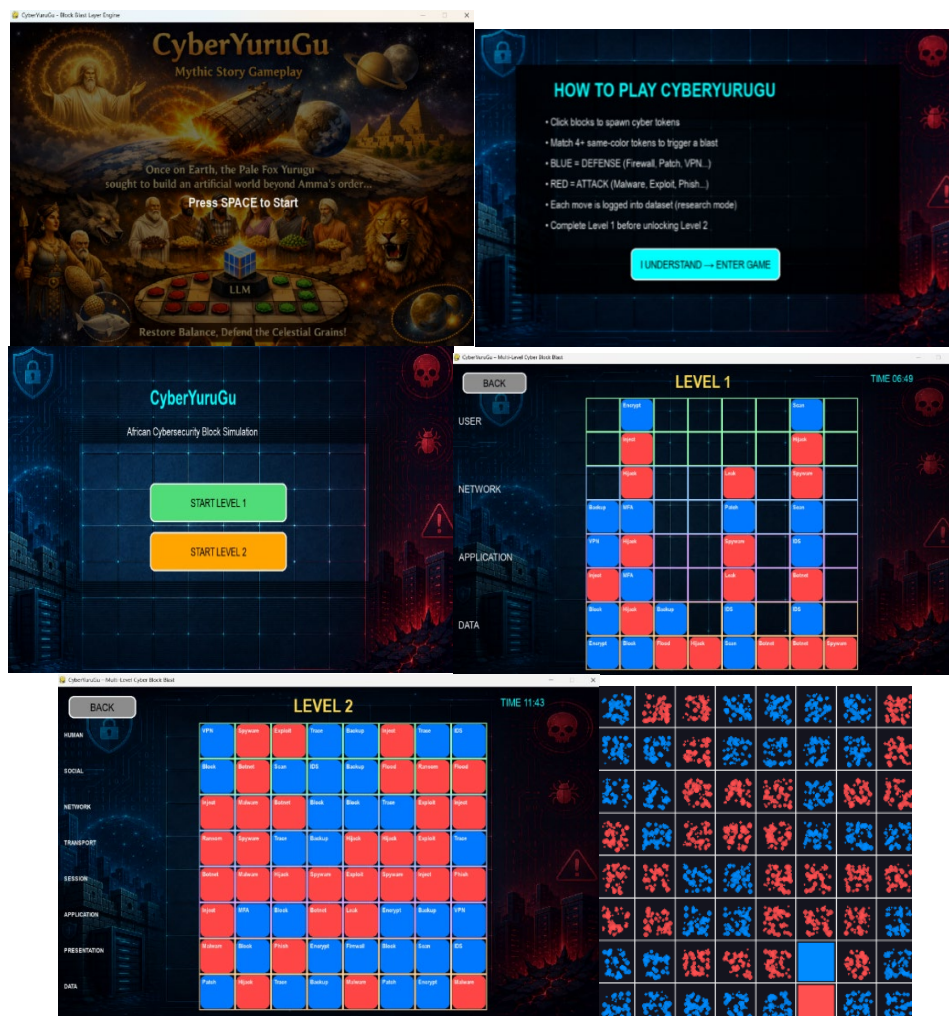


Figure 6: Gameplay with blast animation

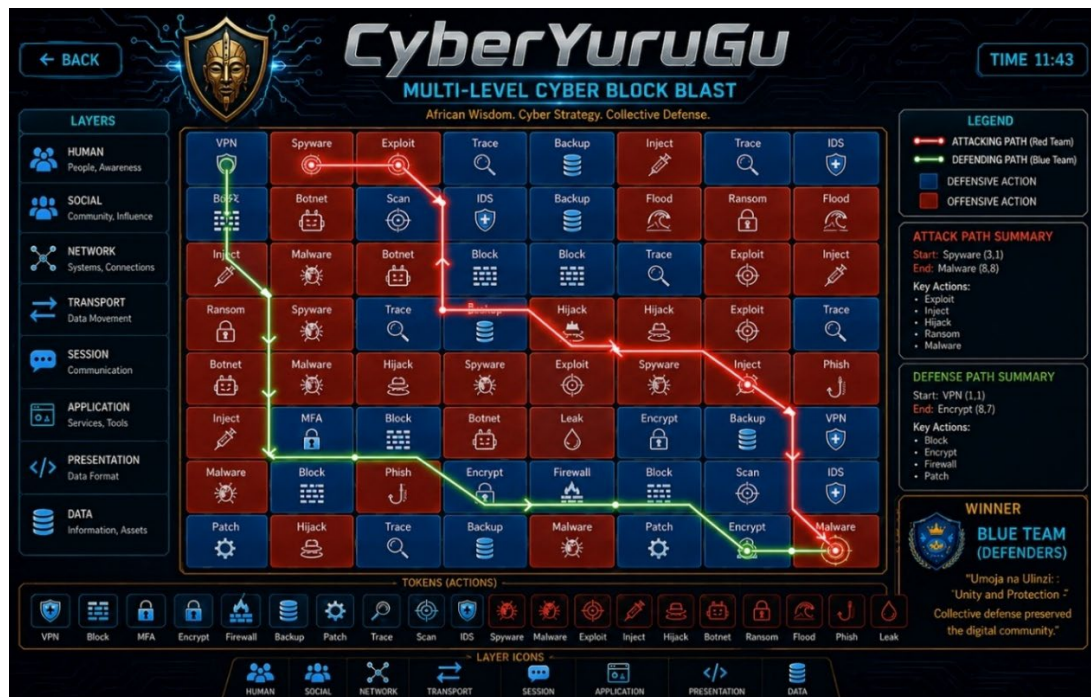


Figure 7: CyberYuruGu level 2 gameplay visualisation

4.2 Cybersecurity Awareness Evaluation

Figure 8 shows participants' cybersecurity awareness predictions using ML models (Table 3). The CNN included three convolutional layers with ReLU and max-pooling, while the RNN used two LSTM layers with dropout and a dense output. Both were trained with Adam (learning rate 0.001) on 535 records, split 80/20 for training and testing. Although results reported 100% accuracy, precision, recall, and F1-score, this likely reflects overfitting given the small dataset and absence of cross-validation. Future work will expand data and apply stratified validation to improve robustness. Despite these limitations, both models consistently revealed a cognitive bias toward defensive reasoning: defence tokens were more frequent and strongly associated with successful outcomes, achieving higher cumulative scores (8) than attack paths (5). LLM analysis confirmed defenders disrupted attack chains through layered coordination, demonstrating the interpretative richness of the CyberYuruGu framework (Figures 7).

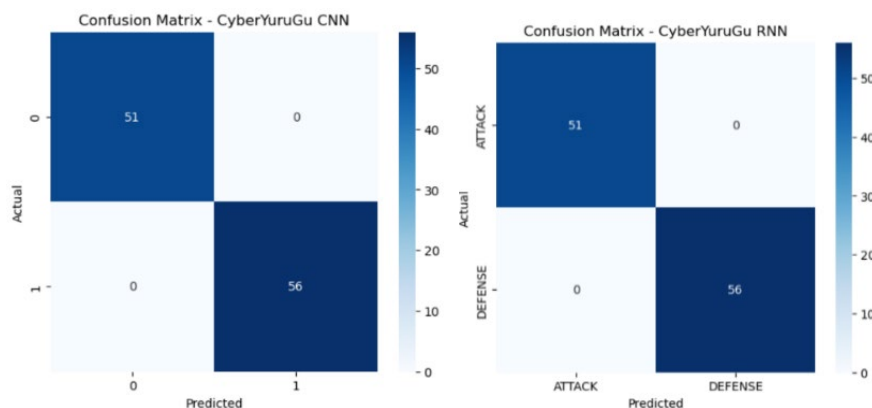


Figure 8: Participants awareness using ML results

4.3 Discussion

Conventional cybersecurity forensics often rely on abductive reasoning, Bayesian inference, or sense-making frameworks to reduce uncertainty by converging on a single explanatory path. While effective, these paradigms treat uncertainty as a deficit to be minimized. By contrast, the CyberYuruGu model, inspired by Dogon epistemology, frames uncertainty as a generative source of insight: traces left by Yurugu are disruptions that produce new relational configurations, where meaning arises from symbolic reconstruction embedded in

context. This relational logic emphasises transformation, resonating with Bachelard's notion of epistemological rupture, where discontinuity becomes the ground of new knowledge. CyberYuruGu thus shifts cybersecurity reasoning from reductionist closure toward interpretative reconstruction, embedding technical analysis within a broader paradigm that values uncertainty as epistemically productive.

Table 3: Defence vs. attack path evaluation (Figure 7)

Defence path	Score	Attack path	Score
VPN → block → MFA → trace → encryption → backup → firewall → patch	8	Exploit → malware → hijack → spyware → injection	5

5. Conclusion

This paper presents an original and thought-provoking contribution to the game-based learning and cybersecurity literature. The combination of African epistemology with Bachelardian rupture, the Dogon Fox divination tradition, explainable cybersecurity reasoning, and human–AI collaboration creates a novel conceptual foundation for serious game design. The paper extends discussions of cultural inclusivity, interpretative learning, and AI-supported gameplay beyond conventional Western-centered approaches. One of the strengths of the paper is the effort to move beyond metaphor and operationalise the Dogon Fox system as a gameplay and reasoning framework. The proposed post-hoc reasoning approach, where players reconstruct attack-defence narratives from traces rather than directly observed actions, is both innovative and pedagogically meaningful. The game design is also well described and supported by implementation details and formal specifications.

Declaration. Ethical clearance was obtained from the institutional ethics committee, and all participants provided informed consent. The game prototype is available on request.

References

- Hasan, K. F., Hughes, W., Rahman Tory, A., Campbell, C., & Turkay, S. (2026). Game On: A developmental approach to UNSW cyber escape room for cybersecurity governance and policy education. *Education Sciences*, 16(1), Article 133. <https://doi.org/10.3390/educsci16010133>
- Ani, M. (1994). *Yurugu: An African-centered critique of European cultural thought and behavior*. Africa World Press.
- Park, J. S., O'Brien, J., Cai, C. J., Morris, M. R., Liang, P., & Bernstein, M. S. (2023). Generative agents: Interactive simulacra of human behavior. In *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology* (Article 2, pp. 1–22). Association for Computing Machinery. <https://doi.org/10.1145/3586183.3606763>
- Wang, X. (2026). Ethnography about digital media. In D. Proctor (Ed.), *Practicing digital ethnography* (pp. 71–96). Routledge.
- Poovizhi, P., Shakthishreya, R., & Tamilarasi, C. (2026). CyberShield, an interactive and gamified learning platform for cybersecurity awareness. *International Journal of Engineering & Extended Technologies Research*, 8(2), 962–973.
- Wang, B., Zhou, Y., Wang, S., Xu, B., & Deng, R. (2026). Large language model-based smart agents for attack-defense game on cyber-physical power systems. *IEEE Transactions on Smart Grid*. Advance online publication. <https://doi.org/10.1109/TSG.2026.3681079>
- Krisnasari, N. K. A., Nugraha, Y., & Aminanto, M. E. (2025). Systematic mapping of cybersecurity awareness content in digital educational games for children. In *2025 IEEE 2nd International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)* (pp. 472–477). IEEE. <https://doi.org/10.1109/ICoCICs66238.2025.10928231>
- Gaukroger, S.W., 1976. Bachelard and the problem of epistemological analysis. *Studies in History and Philosophy of Science Part A*, 7(3), pp.189-244.
- Charmet, F., Tanuwidjaja, H. C., Ayoubi, S., & et al. (2022). Explainable artificial intelligence for cybersecurity: A literature survey. *Annals of Telecommunications*, 77(11–12), 789–812. <https://doi.org/10.1007/s12243-022-00926-7>
- Sani, S. D., Olapojoye, R., Salman, T., & Teixeira, M. A. (2026). XAI in cybersecurity: A survey on techniques, challenges, and future directions. *Journal of Information Security and Applications*, 102, Article 104563.
- Weeratunge, N.H., Hjelssvold, R. & Katt, B. A systematic scoping review on game-based cybersecurity awareness education. *Int. J. Inf. Secur.* 25, 71 (2026). <https://doi.org/10.1007/s10207-026-01239-9>
- Matus, N., Berrios, S., & Isla, R. (2026). From CTF to competence: UX-driven and didactic foundations for gamified cybersecurity training platforms. *Applied Sciences*, 16(12), Article 6100. <https://doi.org/10.3390/app16126100>