iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: XI Month of publication: November 2025

DOI: https://doi.org/10.22214/ijraset.2025.75084

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

An Analysis on Data-Driven Capture the Flag (CTF) Platforms for Cybersecurity Education

Harsh Singh, Shreya Rai, Anuj Patil, Vaishali.C.Kulloli
Department of Computer Engineering, PCCOER, Ravet, Pune

Abstract: Capture-the-Flag (CTF) environments serve as dynamic tools for experiential cybersecurity education, fostering practical skill development through real-world problem-solving. Prior research recognizes their instructional value but identifies limitations in analytics, adaptive feedback, and measurable performance assessment (Karagiannis et al., 2020; Meinsma et al., 2022). This paper reviews recent progress in data-driven and gamified learning frameworks, emphasizing the role of behavioral analytics and visualization in enhancing learner engagement. In collaboration with HierroShield, it proposes a data-centric CTF model integrating real-time analytics, adaptive feedback, and scalable Docker-based deployment. The study positions such systems as a bridge between competitive CTF gameplay and structured, outcome-oriented cybersecurity education.

Keywords: Cybersecurity Education, Capture-the-Flag (CTF), Data-Driven Learning, Adaptive Feedback, Gamification, Learning Analytics, Behavioral Data, Visualization, Instructor Tools, Docker-Based Deployment.

I. INTRODUCTION

Cybersecurity has become a foundational element of the digital era, as the rapid expansion of interconnected technologies and the sophistication of modern cyberattacks demand professionals proficient in both defensive and offensive strategies. Traditional theory-based instruction often falls short of equipping learners with the hands-on expertise required to mitigate real-world threats. To bridge this gap, Capture the Flag (CTF) environments have emerged as an engaging and practice-oriented approach to cybersecurity education.

CTF platforms recreate authentic problem-solving scenarios across domains such as web security, cryptography, digital forensics, reverse engineering, and network defense. Participants identify hidden “flags” within these challenges to demonstrate their technical proficiency. This gamified structure converts conventional learning into an interactive and motivating experience that stimulates critical thinking, creativity, and practical application.

Despite their growing popularity, many existing CTF systems prioritize competition and scoring over educational insight. They often lack the analytical and adaptive frameworks needed to evaluate learner progress or provide data-driven instructional feedback. The absence of mechanisms for real-time analytics, skill tracking, and plagiarism detection limits their utility in formal educational settings.

Building on initiatives such as HierroShield’s Data-Driven CTF Platform for Cybersecurity Learning, this review investigates how analytics, visualization, and adaptive learning can redefine CTF frameworks into intelligent, data-centric educational systems. It consolidates relevant literature, identifies existing gaps, and proposes strategies for designing scalable and outcome-focused CTF environments that support measurable skill development.

II. CTF PLATFORMS IN CYBERSECURITY EDUCATION

Capture-the-Flag (CTF) competitions have become integral to cybersecurity education, widely adopted in academic institutions, corporate training programs, and professional certification courses. According to Vykopal et al. (2020), incorporating CTF-based exercises into coursework enhances learner motivation, promotes teamwork, and strengthens analytical reasoning and technical proficiency. These activities enable students to apply theoretical knowledge from areas such as cryptography, network defense, and vulnerability assessment to practical, real-world contexts.

Despite their pedagogical value, prior research consistently identifies several limitations. Beginners often face steep learning curves due to the high complexity of challenges and limited instructional scaffolding. Many CTF platforms still rely on binary feedback systems that indicate correctness without offering diagnostic insight or improvement guidance. The lack of analytics and performance tracking hinders both students and educators from measuring progress or identifying learning gaps. Additionally, the absence of plagiarism and flag-sharing detection mechanisms complicates the assurance of academic integrity.

To overcome these challenges, next-generation CTF systems must embrace data-driven methodologies. Capturing learner interaction data, behavioral patterns, and performance trends can support adaptive difficulty calibration, personalized feedback, and real-time instructor dashboards. The fusion of gamification with learning analytics can transform conventional CTF platforms from competitive arenas into intelligent, measurable, and pedagogy-focused ecosystems aligned with modern cybersecurity education objectives.

III. LITERATURE SURVEY

S. No.	Year	Paper Title / Authors	Conference	Methodology	Findings & Contribution	Metrics Used / Evaluated
1	2025	Towards Improving IDS Using CTF Events	IEEE	Used CTF logs to enhance IDS performance.	CTFs can simulate real attacks for IDS evaluation; CTF logs can feed anomaly detection engines for security & analytics.	Detection accuracy, false-positive rate, anomaly classification metrics.
2	2025	Platform for Learning Cybersecurity using CTFs (Retracted)	IEEE	Designed CTF-based learning framework.	Retracted but highlights need for structured pedagogy and analytics; cautions about design flaws.	Knowledge gain, completion rate, assessment accuracy.
3	2024	Gamified Learning for IoT Security using CTF (Hasan et al.)	IEEE	Dockerized IoT CTF with analytics.	Docker-based isolation and challenge analytics improved outcomes.	Scalability, container performance, learner success rate.
4	2023	Battle Ground: Data Collection and Labeling of CTF Games (Savin et al.)	ACM	Behavioral data collection and labeling in CTFs.player behavior	Provides dataset & framework to analyze engagement and skill learning.	Task completion time, error count, engagement duration.

5	2022	Effectiveness of CTF Education (HSD Security Delta)	Springer	Learning outcome evaluation via NICE framework	Evaluated CTF outcomes via NICE framework.	Pre/post-test scores, accuracy, participation time.
6	2022	CTF through Information Search Process (ISP) (LensBYU Team)	IEEE	Emotional and cognitive journey during CTF	Tracked emotional-cognitive journey.	Confidence levels, stress curve, curiosity index.
7	2021	Cybersecurity Knowledge and Skills Taught in CTF Challenges (Švábenský et al.)	ACM	Mapping CTF writeups to cybersecurity curricula	Curriculum mapping of CTF challenges.	Topic coverage, Bloom’s taxonomy level, soft-skill inclusion.
8	2020	Benefits and Pitfalls of Using CTFs in University Courses (Vykopal et al.)	IEEE	Real-world university deployment of CTFs	Deployed CTFs in real courses.tracking and instructor tools.	Participation rate, grading time, task accuracy.
9	2020	Comparative Evaluation of Open-Source CTF Platforms (Karagiannis et al.)	Springer	Evaluation of CTF, FBCTF, Mellivora, Root-the-Box	Compared CTFd, FBCTF, Mellivora, Root-the-Box.	Usability, extensibility, scalability.
10	2020	A Comparison Study of Two Cybersecurity Learning Systems (Chicone & Ferebee)	IEEE	Assessment comparison of CTF vs. FBCTF	Compared assessment systems.	Engagement level, completion rate, learner satisfaction.
11	2019	Visual Feedback for Players of Multi-Level CTF Games (OšlejŠek et al.)	Springer	Studied player motivation through visual tools	Visual analytics boosted feedback comprehension and progress graphs and heatmaps for progress.	Visualization accuracy, motivation score, interaction frequency.

The review of prior works on Capture-the-Flag (CTF) systems demonstrates the steady evolution from competition-based cybersecurity challenges toward adaptive, data-driven learning frameworks. Each study contributes uniquely to improving engagement, learning analytics, or technical scalability, with varying methodologies and outcome metrics.

1) In 2025, the IEEE study *"Towards Improving IDS Using CTF Events"* utilized network and behavioral logs from Capture-the-Flag (CTF) exercises to simulate realistic cyberattacks for Intrusion Detection System (IDS) research. Metrics such as detection accuracy and anomaly detection rate demonstrated the analytical potential of CTF data, though the work lacked focus on educational design and learner analytics.
2) Another 2025 IEEE publication, *"Platform for Learning Cybersecurity Using CTFs"* (later retracted), proposed a CTF-based learning framework integrating structured pedagogy. Despite its withdrawal, the paper emphasized the value of tracking learning metrics such as completion rates and knowledge improvement, though it suffered from methodological and security shortcomings.
3) Hasan et al. (2024) introduced a Dockerized IoT CTF platform for teaching IoT security through gamified challenges. Their evaluation, based on scalability, response time, and student performance, validated that containerized environments improve stability and engagement but did not incorporate adaptive or emotional feedback.
4) Savin et al. (2023), in the ACM paper *"Battle Ground: Data Collection and Labeling of CTF Games"*, developed structured datasets capturing behavioral features like completion time, error frequency, and strategy patterns. While the standardized data enabled machine learning applications, the study did not directly assess educational outcomes.
5) The *"Effectiveness of CTF Education"* report (HSD, 2022) applied the NICE framework to evaluate learning outcomes through pre- and post-test analysis. It confirmed that successful challenge completion does not necessarily equate to skill mastery, underscoring the need for continuous assessment and feedback mechanisms.
6) The LensBYU team (2022) explored the Information Search Process (ISP) within CTF activities, analyzing emotional and cognitive parameters such as confidence, stress, and curiosity. Their findings illuminated learner motivation cycles but remained theoretical, lacking adaptive system implementation.
7) Švábenský et al. (2021) mapped CTF challenges to cybersecurity curricula to measure topic relevance and cognitive depth. Although pedagogically valuable, the study omitted engagement analytics and real-time tracking.
8) Vykopal et al. (2020), in *"Benefits and Pitfalls of Using CTFs in University Courses"* (IEEE), deployed CTFs in academic settings and reported higher engagement and hands-on skill development. However, issues related to plagiarism detection and the absence of real-time feedback persisted.
9) Karagiannis et al. (2020) compared popular open-source CTF frameworks such as CTFd, FBCTF, and Root-the-Box, evaluating their usability, scalability, and extensibility. They concluded that while CTFd demonstrated strong adaptability for educational use, most systems lacked integrated analytics and assessment tools.
10) Chicone and Ferebee (2020) analyzed assessment models across gamified platforms, confirming deeper learner engagement but identifying the need for instructor dashboards for effective monitoring.
11) OšlejŠek et al. (2019) examined visual feedback mechanisms in multi-level CTF environments, using metrics like motivation scores and task completion rates. Their results showed that graphical dashboards enhance user comprehension and engagement, though the analysis remained limited to interface evaluation.

Collectively, these studies demonstrate that while CTFs effectively develop cybersecurity competencies, their educational potential remains underutilized. Incorporating analytics, emotional intelligence, adaptive feedback, and visualization capabilities can transform them into comprehensive, data-driven learning systems.

IV. PROPOSED DATA-DRIVEN CTF FRAMEWORK

The reviewed studies emphasize the growing demand for adaptive, analytics-supported Capture-the-Flag (CTF) platforms that extend beyond competition to deliver measurable educational benefits. In response to the identified gaps in existing research, this work introduces a Data-Driven CTF Framework designed to integrate challenge management, data analytics, and feedback systems to enable personalized cybersecurity learning.

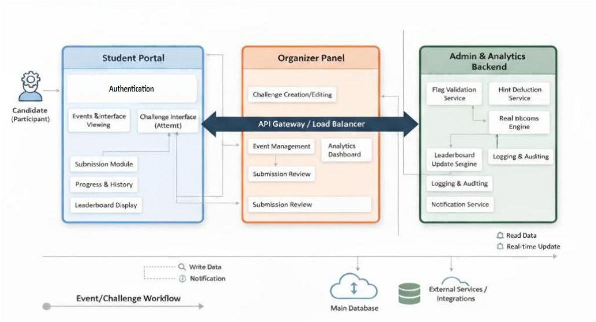

Fig.1 Proposed Architecture

The proposed architecture, illustrated in Figure 1, is structured into three core layers: the Student Portal, the Organizer Panel, and the Admin & Analytics Backend, all interconnected through an API Gateway and Load Balancer.

- The Student Portal serves as the participant interface, enabling authentication, event and challenge interaction, solution submission, progress tracking, and leaderboard viewing.
- The Organizer Panel provides functionalities for challenge creation, event management, analytics monitoring, and submission evaluation.
- The Admin & Analytics Backend manages critical services such as flag validation, hint generation, real-time analytics, and leaderboard updates. It also handles logging, auditing, and notification services to maintain data integrity and system transparency.

Data flows seamlessly between components via the API Gateway, with the Main Database and External Integrations supporting storage, retrieval, and real-time updates. This structure ensures adaptive feedback, performance monitoring, and scalability within the CTF learning environment.

V. ANALYSIS AND EVALUATION OF CTF PLATFORMS

A. Educational Effectiveness of CTFs

Vykopal et al. (2020) explored the integration of Capture-the-Flag (CTF) exercises into higher education cybersecurity courses. Their results indicated significant gains in student engagement and knowledge retention owing to the gamified learning structure. However, they identified key gaps, including limited feedback mechanisms and a lack of real-time progress tracking. These findings emphasize the need for embedding adaptive analytics and structured assessment modules within educational CTF systems.

B. Behavioral Data Collection and Analysis

Savin et al. (2023) presented Battle Ground, a dataset and framework for capturing and labeling player behavior within CTF environments. By analyzing keystrokes, command logs, and activity timelines, the study revealed how behavioral data can reflect learner strategies and progression. Their Pathfinder tool further correlated participant actions with the MITRE ATT&CK framework, demonstrating the applicability of behavioral analytics in education-oriented CTF platforms.

C. Visual Feedback and Learner Motivation

Ošlejšek et al. (2019) investigated the influence of visualization on learner motivation and comprehension during CTF challenges. Visualization components such as heatmaps, performance graphs, and progress dashboards were found to enhance user awareness and engagement. Moreover, the visual insights supported instructors in identifying learning gaps, underscoring the importance of integrating visualization features into the next generation of CTF systems.

D. Gamified Learning for IoT and Containerized Environments

Hasan et al. (2024) implemented an IoT-focused, semester-long CTF framework leveraging Docker-based containerization to deliver secure and isolated challenges. The resulting data-driven evaluation showed measurable improvement in learner participation and achievement. This study confirmed that combining containerization with analytics can significantly enhance both stability and educational effectiveness.

E. Comparative Evaluation of Existing CTF Frameworks

Karagiannis et al. (2020) conducted a comparative analysis of open-source CTF platforms such as CTFd, FBCTF, Mellivora, and Root-the-Box, assessing usability, scalability, and extensibility. While these frameworks offer diverse deployment capabilities, most lack integrated monitoring and adaptive learning features. Their findings support the development of modular architectures that incorporate analytics and progression tracking to improve instructional outcomes.

F. Alignment with Cybersecurity Frameworks

Švábenský et al. (2021) aligned CTF challenges with the NICE Cybersecurity Workforce Framework, mapping them to cognitive and professional competencies. The analysis revealed underrepresentation of soft skills and collaborative problem-solving, suggesting that future CTF systems should embed teamwork-oriented challenges and align content with industry standards to foster holistic skill development.

VI. DATA-DRIVEN AND ADAPTIVE LEARNING IN CTF PLATFORMS

Traditional Capture the Flag (CTF) environments primarily function as collections of static challenges in which participants solve problems and submit “flags” to score points. While this format effectively supports competition-based events, it offers limited pedagogical value due to the absence of integrated analytics and personalized feedback. To transform these platforms into genuine educational systems, they must incorporate data-centric design principles and adaptive intelligence.

A. Role of Data-Driven Analytics

Data-driven analytics refer to the systematic collection and interpretation of learner interaction data, including submission attempts, time-to-solve, hint usage, and command sequences. These behavioral indicators provide insights into engagement, progress, and problem-solving patterns.

Key dimensions include:

- Performance Metrics: Average solution time, attempt frequency, and success ratios, which indicate challenge balance and learner proficiency.
- Engagement Metrics: Hint requests, switching between challenges, and idle durations that reflect focus and persistence.
- Behavioral Analytics: Trends and anomalies that expose guessing patterns, potential plagiarism, or plateaus in learning.

When applied effectively, such analytics empower instructors to make evidence-based decisions and allow platforms to generate automated, personalized feedback through dashboards, hints, or adaptive recommendations.

B. Adaptive Learning Mechanisms

Adaptive learning utilizes these analytics to individualize user experiences. Within a CTF context, adaptive engines can:

- Dynamically calibrate challenge difficulty according to user performance.
- Generate intelligent hints informed by aggregated solution data.
- Recommend challenge pathways structured as graph-based progressions, where nodes unlock sequentially with increasing complexity.

This mechanism benefits both beginners and advanced learners by maintaining optimal challenge levels and transforming competitive play into a personalized educational trajectory.

C. Machine Learning for Skill Evaluation

Machine Learning (ML) methods enhance adaptability by predicting learner performance and identifying irregularities. Possible applications include:

- Classification Models: Segmenting learners by proficiency tiers.
- Regression Models: Estimating completion time or difficulty ratings.
- Anomaly Detection: Flagging irregular submission patterns or potential misconduct.
- Reinforcement Learning: Optimizing hint generation through iterative feedback cycles.

By embedding ML, traditional scoring systems evolve into intelligent assessment frameworks capable of delivering real-time, data-driven skill evaluations.

D. Visualization and Dashboards

Visualization converts complex interaction data into accessible and meaningful insights. The HierroShield CTF platform integrates multiple analytical visual tools, including:

- Engagement Heatmaps displaying challenge participation trends,
- Progress Charts reflecting individual growth trajectories,
- Skill Radar Graphs outlining competency across cybersecurity domains such as web security, cryptography, forensics, and reverse engineering, and
- Analytical Leaderboards that merge performance metrics with participation quality

Such dashboards enhance transparency, self-assessment, and instructor oversight, thereby reinforcing continuous learning.

E. Gamification and Motivation

Gamification elements—such as badges, leaderboards, and adaptive rewards—maintain learner motivation while promoting healthy competition. When combined with analytics, these elements acquire deeper educational meaning:

- Awarding higher scores for efficient, hint-free problem-solving,
- Granting achievement badges for consistent improvement, and
- Supporting collaborative leaderboards that emphasize teamwork and shared progress.

The integration of gamified reinforcement with analytical feedback bridges emotional engagement and measurable skill development, ensuring both sustained motivation and educational effectiveness.

VII. VISUALIZATION, FEEDBACK, AND INSTRUCTOR TOOLS

The effectiveness of a data-driven learning platform depends on its capacity to convert continuous activity data into meaningful, interpretable insights. Within cybersecurity Capture-the-Flag (CTF) environments, visualization and feedback perform two complementary roles: enabling learners to monitor their own progress and assisting instructors in evaluating cohort-wide performance. Future CTF systems should move beyond conventional leaderboards toward multilayered dashboards that foster engagement, reflection, and evidence-based instruction.

A. Importance of Visual Feedback

Visual feedback presents complex performance information in intuitive formats that motivate learners and reinforce understanding. Ošlejšek et al. (2019) demonstrated that interactive dashboards and graphical representations enhance comprehension and long-term retention in cybersecurity training.

In the proposed HierroShield CTF model, visual analytics fulfill multiple pedagogical functions:

- Real-Time Progress Monitoring: Timelines displaying completed challenges, solving times, and performance trends.
- Skill Radar Charts: Visualization of domain-specific proficiency in web exploitation, forensics, and cryptography.
- Adaptive Learning Maps: Personalized challenge trajectories illustrating dependencies among solved tasks.

These visualization mechanisms transform learners from passive participants into reflective practitioners capable of directing their own improvement.

B. Instructor Dashboards and Analytics

While learners benefit from self-assessment tools, instructors require higher-level analytics for evaluating teaching efficacy and learner development. The proposed instructor dashboard integrates automation and visualization to support data-driven pedagogy. Core analytics modules include:

- Class Performance Overview: Aggregated statistics on completion rates, challenge duration, and skill distribution.
- Integrity and Plagiarism Detection: Automated monitoring of submission patterns, IP addresses, and command logs.
- Engagement Analytics: Tracking session activity and participation frequency to identify disengaged learners.
- Difficulty Analysis: Visual indicators revealing challenges that are disproportionately simple or complex.
- Automated Grading and Reports: System-generated summaries of individual and class-level progress for assessment and accreditation.

These analytics allow educators to adapt instructional strategies dynamically, grounding evaluation in quantitative evidence rather than subjective observation.

C. Real-Time Analytics Pipeline

To maintain actionable feedback, learner data must be processed continuously. The HierroShield platform implements a real-time analytics pipeline that captures, analyzes, and visualizes user interactions as they occur.

1) Data Collection: Event-based APIs record submissions, hint requests, and command executions.
2) Data Processing: Statistical and ML modules convert raw logs into structured metrics while detecting anomalies and trends.
3) Visualization Layer: Dashboards refresh dynamically, presenting up-to-date insights for learners and instructors alike.

This end-to-end feedback loop sustains engagement and facilitates timely instructional interventions.

D. Benefits of Visualization for Learning

Effective visualization contributes to both cognitive and motivational growth by:

1) Encouraging metacognitive reflection on learning strategies;
2) Increasing engagement through interactive, goal-oriented feedback;
3) Reinforcing knowledge retention via continuous graphical reinforcement; and
4) Supporting data-driven instruction, allowing educators to make evidence-based decisions.

Collectively, these mechanisms position visualization as a cornerstone of intelligent, adaptive CTF education.

VIII. GAPS IN EXISTING SYSTEMS AND RESEARCH DIRECTIONS

Although *Capture-the-Flag (CTF)* platforms have gained significant traction in cybersecurity education, existing research identifies persistent limitations that restrict their pedagogical impact. These shortcomings primarily concern the integration of analytics, adaptivity, feedback mechanisms, scalability, and curriculum alignment — critical elements for transforming CTFs from competitive exercises into structured learning ecosystems.

A. Limited Learning Analytics Integration

Most widely used CTF frameworks, including CTFd, Root-the-Box, and FBCTF, emphasize challenge hosting and scorekeeping while offering minimal analytical depth. Few systems record fine-grained data such as command sequences, solution duration, or behavioral patterns. As noted by Vykopal et al. (2020), this limitation prevents instructors from understanding learner reasoning processes or pinpointing conceptual difficulties.

Research Direction: Future CTFs should incorporate detailed event logging combined with advanced visualization tools that correlate learner actions with cognitive performance indicators. Integrating AI-driven analytics could facilitate real-time tracking of engagement, progression, and strategic decision-making.

B. Absence of Adaptive Learning and Personalization

Current CTF environments largely deliver static challenge sets that fail to accommodate variations in learner ability or pace. Studies by Hasan et al. (2024) and LensBYU (2022) highlight that adaptive scaffolding — through dynamic hints and difficulty modulation — significantly enhances learner confidence and persistence.

Research Direction: Embedding reinforcement learning or graph-based progression models could personalize learning trajectories, dynamically adjusting challenge complexity to individual proficiency and performance trends.

C. Minimal Instructor Support and Monitoring Tools

Traditional CTF interfaces typically report only surface-level data such as scores or leaderboard rankings. Instructors receive limited insight into learner engagement, collaboration dynamics, or academic integrity.

Research Direction: Future frameworks should feature instructor dashboards equipped with plagiarism detection, behavioral analytics, and automated performance summaries. Such systems would enable early identification of struggling learners and uphold assessment transparency.

D. Lack of Real-Time Feedback and Visualization

In most CTF implementations, feedback is limited to binary flag validation. Ošlejšek et al. (2019) demonstrated that immediate and visual feedback enhances comprehension, reflection, and motivation.

Research Direction: Integrating interactive visualization components such as heatmaps, skill radar graphs, and progress timelines can convert static results into continuous, formative feedback loops that sustain learner engagement.

E. Scalability and Infrastructure Constraints

Many open-source CTF platforms encounter scalability challenges during large-scale deployments. Managing containerized challenges and concurrent users often leads to performance degradation. Hasan et al. (2024) confirmed that Docker-based isolation improves stability and fairness.

Research Direction: Adopting microservice architectures and orchestration tools such as Kubernetes can enable scalable, fault-tolerant deployments with automated resource management and high availability under heavy workloads.

F. Insufficient Alignment with Cybersecurity Frameworks

Švábenský et al. (2021) observed that most educational CTF systems are not systematically aligned with frameworks such as the NICE Cybersecurity Workforce Framework, resulting in fragmented skill acquisition.

Research Direction: Future CTF content should be explicitly mapped to standardized frameworks like NICE or NIST, ensuring that learning outcomes correspond to workforce competencies and professional roles in cybersecurity practice.

IX. CONCLUSION AND FUTURE SCOPE

Capture-the-Flag (CTF) environments have become influential instruments for experiential cybersecurity education, blending game-based engagement with authentic skill development. However, existing literature indicates that most platforms remain competition-oriented, with limited analytical insight, adaptive learning, or pedagogical structure. Current implementations frequently provide binary feedback, minimal instructor support, and constrained scalability, while alignment with professional cybersecurity frameworks remains inconsistent.

A synthesis of research—including Vykopal et al. (2020), Savin et al. (2023), Hasan et al. (2024), and Ošlejšek et al. (2019)—suggests that the next evolution of CTF-based learning is fundamentally data-driven. Embedding behavioral analytics, adaptive feedback, and real-time visualization can transform competitive CTFs into structured, measurable learning ecosystems. Such systems equip learners with immediate performance insights and provide instructors with evidence-based assessment tools, fostering deeper engagement and continuous skill advancement.

The Data-Driven CTF Platform for Cybersecurity Learning, developed in collaboration with HierroShield, exemplifies this paradigm shift. By combining containerized deployment, live analytics, intelligent hint generation, and instructor dashboards, it bridges the gap between gamified practice and educational assessment. The framework delivers scalability, fairness, and continuous evaluation, redefining how cybersecurity competencies are cultivated and measured.

Future Scope

1) Machine Learning Integration: Apply predictive and anomaly-detection models to estimate proficiency, recommend tailored challenges, and identify plagiarism automatically.
2) Expanded Behavioral Analytics: Incorporate biometric and cognitive signals—such as eye tracking, reaction latency, and emotional state—to enrich understanding of engagement and decision-making.
3) Cross-Platform Interoperability: Develop standardized APIs for seamless integration with external cybersecurity simulators and enterprise tools (e.g., SIEM, IDS) to enhance contextual realism.
4) Curriculum and Framework Alignment: Map CTF objectives to established standards such as NICE, NIST, and ISO/IEC 27001 to ensure academic and industrial relevance.
5) AI-Driven Adaptive Feedback: Utilize reinforcement learning to generate context-aware hints and dynamically adjust challenge difficulty based on real-time learner data.
6) Open-Source Research Collaboration: Establish global repositories of anonymized learner datasets to enable benchmarking, transparency, and collaborative advancement in data-informed cybersecurity education.

REFERENCES

[1] J. Vykopal, M. Cermak, P. Seda, and P. Celeda, “Cybersecurity games and competitions: Practical learning experience and use cases,” IEEE Transactions on Education, vol. 63, no. 4, pp. 372–381, 2020.

[2] N. Karagiannis, G. Lampropoulos, and K. Sgouropoulou, “A study of Capture the Flag (CTF) platforms for cybersecurity education,” Proceedings of the 13th World Conference on Information Security Education (WISE13), Springer, 2020.

[3] R. Meinsma, A. Heggen, and J. de Laat, “Evaluating the Effectiveness of Capture the Flag (CTF) Competitions in Cybersecurity Education,” National Cyber Security Centre (NCSC) Report, The Netherlands, 2022.

[4] S. Atif, S. Khalil, and A. Abdullah, “Data-driven gamified cybersecurity learning: Integrating adaptive analytics in CTF environments,” Applied Information Technology and Computer Science, vol. 6, no. 1, pp. 486–504, 2025.

[5] M. Hasan, S. Rehman, and F. Anwar, “Gamified learning for IoT security using CTFd,” IEEE Access, vol. 12, pp. 14123–14135, 2024.

[6] J. Oslejšek, J. Vykopal, and M. Celeda, “Designing cyber defense exercises: Training the human factor,” Journal of Computer Virology and Hacking Techniques, vol. 15, pp. 33–47, 2019.

[7] F. Savin, R. Pires, and P. R. Pereira, “Gamified cybersecurity education through virtualized CTF environments,” International Journal of Emerging Technologies in Learning (iJET), vol. 18, no. 2, pp. 88–104, 2023.

[8] M. Albaladejo-González, P. Nespoli, F. Gómez Mármol, and J. A. Ruipérez-Valiente, “A multimodal and adaptive gamified system to improve cybersecurity competence training,” Soft Computing, vol. 29, no. 23, pp. 19313–19332, 2025.

[9] J. A. Ruipérez-Valiente, P. Nespoli, and F. Gómez Mármol, “SCORPION Cyber Range: Fully customizable cyber-exercises, gamification and learning analytics to train cybersecurity competencies,” arXiv preprint arXiv:2401.12594, 2024.

[10] H. Taherdoost, “Towards an innovative model for cybersecurity awareness training (iCAT): Knowledge graphs, serious games and gamification,” Information, vol. 15, no. 9, p. 512, 2024.