Journal Homepage: www.ijarpr.com ISSN: 3049-0103 (Online)

International Journal of Advance Research Publication and Reviews

Vol 02, Issue 07, pp 519-523, July 2025

A Comparative Study of Capture the Flag (CTF) Platforms

***Umme E Rubab*[1]**

[*1]*Department of Computer Science & IT, University of Engineering & Technology Peshawar, Pakistan*
[*]*Rubabumme664@gmail.com*

ABSTRACT

Capture the Flag (CTF) platforms have evolved, and these platforms have become a vital resource in cybersecurity education, providing participants with practical and hands-on knowledge in various sectors, including web exploitation, reverse engineering, cryptography, and binary analysis. This research thesis focuses on existing CTF platforms, analyzing their technical features and user satisfaction levels. To address the key observations in the current existing platforms, a comprehensive and detailed CTF framework is also proposed that integrates the major functionalities of the existing platforms to enhance usability for both educational and professional purposes. The proposed platform also incorporates adaptive and engaging learning pathways for individuals to enhance the learning experience. This study will improve the effectiveness of the CTF platforms by aiding professional and academic organizations, as independent learners, by contributing to the development of a skilled cybersecurity workforce.

Keywords: Capture the Flag (CTF), Survey of CTFs, Ethical Hacking Events

1. INTRODUCTION

The Technology is evolving rapidly, enabling organizations to optimize resource management efficiently and enhance productivity through advanced innovations. The emergence of technological trends, such as cloud computing, the Internet of Things (IoT), data mining, and artificial intelligence (AI), offers organizations immediate insights into customer needs and preferences, enabling companies to make data-driven decisions for creating innovative services and products. However, the rapid growth has resulted in a heap of cybersecurity threats across the globe that compromise the confidentiality, integrity, and availability of information systems. According to a study conducted by Deloitte [1], approximately 40% of organizations in Ecuador experienced security breaches, and around 70% expressed uncertainty about their ability to respond to cybersecurity incidents.

Furthermore, the shortage of professionals in cybersecurity further aggravates the situation. According to a 2019 report issued by ISC² [2], a total demand of 4.07 million cybersecurity specialists was projected. The COVID-19 pandemic exacerbated this challenge, with a notable increase in various cyberattacks targeting the broader community, including individuals, businesses, government sectors, and, most importantly, infrastructure [3]. During the first four months of 2020, INTERPOL [4], reported over 737 malware incidents, 48000 malicious URLs, and around 900000 spam messages related to COVID-19 alone.

To address these cybersecurity issues, not only is advancement in the technological field required, but also skilled and well-trained professionals are required against evolving and emerging attacks. As the need for hands-on skill-based environments is increasing, Capture the Flag platforms have gained popularity as an innovative method for teaching cybersecurity[5]. These gamified CTF platforms provide challenge-based scenarios that mimic attacks and real-world

vulnerabilities, allowing the participants to build and enhance their critical thinking, technical expertise, and to build their problem-solving skills in a competitive and controlled environment [6]**.**

2. METHODOLOGY

This section describes the research methodology followed to conduct the analysis of current Capture the Flag (CTF) platforms and propose the best framework for CTF events.

This research will follow both qualitative and quantitative elements. A detailed and comparative analysis of existing CTF platforms will be carried out first, followed by a user feedback form based on properly designed questionnaire in several events of CTF. The data which is collected is thoroughly analyzed using statistical techniques[7].

- Research Design Justification: This research study follows a mixed method of approach, integrating quantitative and qualitative methods.
- Qualitative Methods: Used for usability feedback, user experience evaluation and expert reviews.
- Quantitative Methods: Used for security validation, performance benchmarking and scalability testing.

This type of hybrid approach ensures a comprehensive and detailed evaluation of user management, platforms' functionality and security measures.

3. RESEARCH QUESTIONS

The research explores the following research questions:

RQ-1. What strategies do existing Capture the Flag (CTF) platforms use to overcome scalability issues when dealing with numerous participants, and what are the current constraints in sustaining optimal performance and user satisfaction?

This research question identifies different scalability techniques that are used by the current platforms, including distributed server architectures and load balancing. The projected framework incorporates the existing strategies and new methodology, like cloud-based infrastructure, to safeguard seamless performance during a heavy load of participants. The platform's efficiency under various conditions will be validated by usability testing [8].

RQ-2. What security weaknesses or flaws are usually recognized in current CTF platforms, and how can these issues be resolved in future platform designs?

The current CTF platforms have common vulnerabilities, like a lack of data encryption and insufficient authentication mechanisms. The proposed solution will address the issues by instigating robust security measures, like end-to-end encryption, multifactor authentication (MFA), and continuous security audits to prevent data breaches or unauthorized access [9].

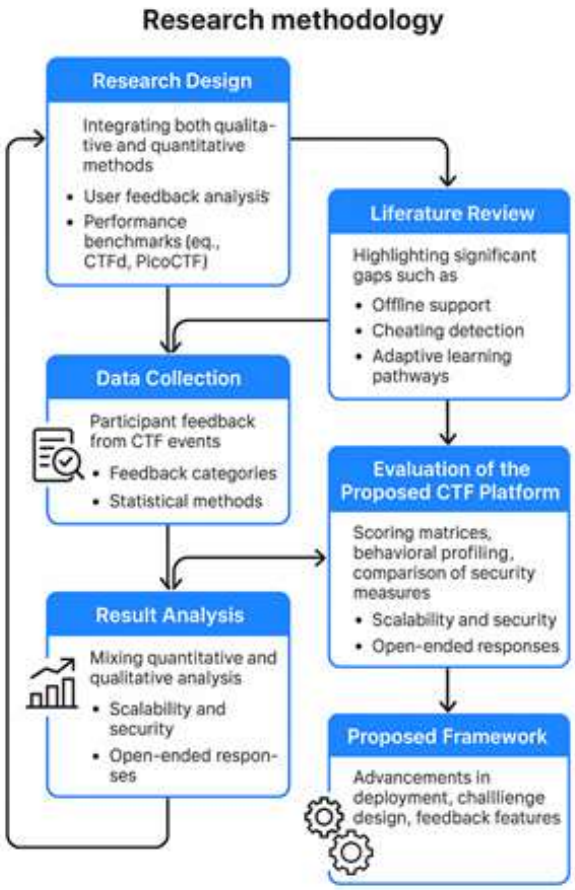

Figure 1: Research Methodology

4. RESULTS

This section presents the findings of our analysis conducted to address the research questions mentioned in Section III. The results are derived from the analysis of existing Capture the Flag (CTF) platforms, user feedback forms, expert opinions, practical evaluations of security, accessibility, challenge diversity, scalability, and offline functionality. This section builds insights from the proposed framework and systematic literature review, providing a comprehensive and structured discussion on each research question, supported by figures, empirical data, and tables.

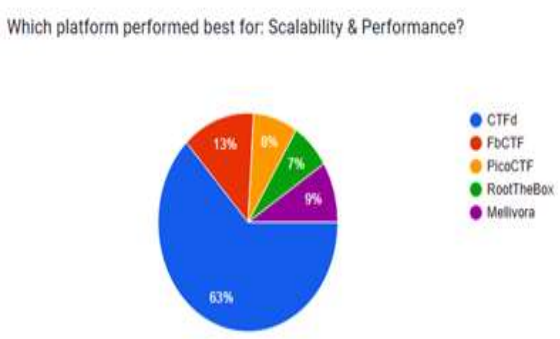

Figure 4.1 (a) : Scalability and Performance

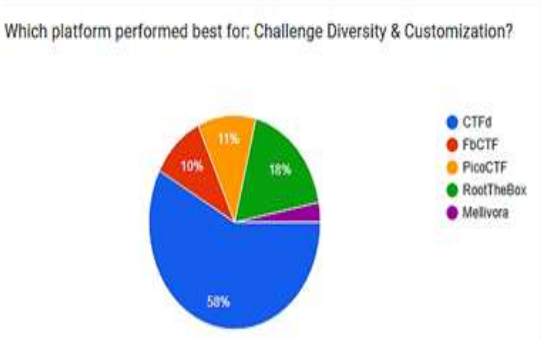

Figure 4.1 (b) : Challenge Diversity and Customization

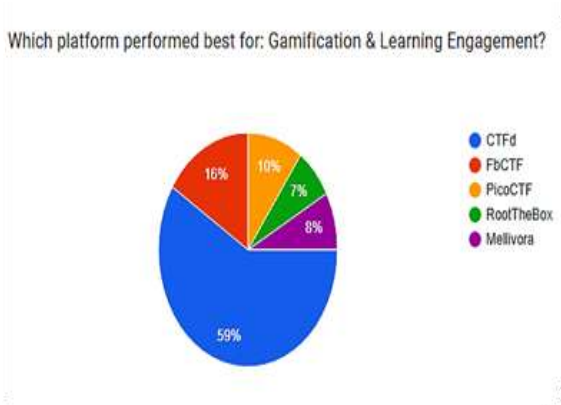

Figure 4.2 (a) : Gamification and Learning Engagement

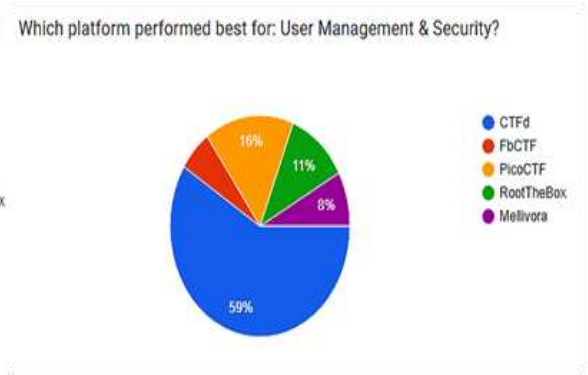

Figure 4.2 (b) : User Management & Security

5. CONCLUSION AND FUTURE WORK

This research evaluates the CTF platforms used for cybersecurity training and education, with a special focus on accessibility, educational effectiveness, scalability, comparing several existing platforms such as RootTheBox, PicoCTF, CTFD, FBCTF and Mellivora. This study identifies several limitations of existing systems, weak scalability and lack of offline accessibility in constrained environment and insufficient mechanisms for measuring user' learning outcomes and user engagement. This thesis presents research driven framework that addresses many of the limitations and challenges. The framework serves as a blueprint for designing more accessible, educationally effective and adaptive CTF environments. It outlines essential components such as support for multimedia challenges, challenge randomization, user behavior tracking and offline operability.

While this research introduces and propose a robust framework to enhance the evaluation and design of the CTF platforms, several future directions still remain open for exploration. Broader validation across diverse intuitions and larger participants pools is essential to assess its effectiveness and scalability in different contexts

References

[1] Orellana, F. D. (2020). *Cybersecurity incident response capabilities in the Ecuadorian small business sector: A qualitative study* (Doctoral dissertation, Northcentral University).

[2] Nizich, M. (2023). An introduction to the field of cybersecurity and the current workforce gap. In *The Cybersecurity Workforce of Tomorrow* (pp. 1–35). Emerald Group Publishing Limited.

[3] Antczak, J. (2022). The impact of the COVID-19 pandemic on business entity cybersecurity. *Inżynieria Bezpieczeństwa Obiektów Antropogenicznych*.

[4] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cybersecurity vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

[5] Chicone, R. G., & Ferebee, S. (2020). A comparison study of two cybersecurity learning systems: Facebook's open-source capture the flag and CTFd. *Issues in Information Systems*, *21*(1), 202–212.

[6] Beuran, R. (2025). Capture the Flag Platforms. In *Cybersecurity Education and Training* (pp. 193–219). Singapore: Springer Nature Singapore.

[7] Swann, M., Rose, J., Bendiab, G., Shiaeles, S., & Li, F. (2021, July). Open source and commercial capture the flag cybersecurity learning platforms case study. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 198–205). IEEE.

[8] Nurgaliyev, A. (2023). *Analysis of reverse engineering and cyber assaults* (Doctoral dissertation, Victoria University).

[9] Rahman, M. D. (2025). *The Art of Open Source Intelligence (OSINT): Addressing Cybercrime, Opportunities, and Challenges*.