SNESTIK

Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika

https://ejurnal.itats.ac.id/snestik dan https://snestik.itats.ac.id

Informasi Pelaksanaan :
SNESTIK IV - Surabaya, 27 April 2024
Ruang Seminar Gedung A, Kampus Institut Teknologi Adhi Tama Surabaya

Informasi Artikel:
DOI : 10.31284/p.snestik.2024.5860

Prosiding ISSN 2775-5126

Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya
Gedung A-ITATS, Jl. Arief Rachman Hakim 100 Surabaya 60117 Telp. (031) 5945043
Email : snestik@itats.ac.id

Kajian Literatur: Gamifikasi Edukasi Keamanan Siber dengan Konsep Capture the Flag

Haifan Naqi Rafdhaizmar Syah, Fayruz Rahma, Sheila Nurul Huda

Jurusan Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
e-mail: 20523075@students.uii.ac.id[1]

ABSTRACT

Cybersecurity is a serious challenge in today's world of information technology, with threats to individuals, companies, and countries. Cybersecurity education is still rare, causing a lack of understanding among students. Capture the Flag (CTF) style gamification can increase student interest and understanding. CTF provides an interactive and challenging learning experience similar to real situations faced by cybersecurity professionals. However, selecting an effective game genre and adapting it to the target participants and relevant cybersecurity topics is necessary. This research reviews the literature on cyber security educational games with a CTF approach. In this research, we discuss what game genres are suitable for cyber security education and their relation to target participants, target participants for cyber security education, and their relation to the topics discussed. This research was conducted by grouping several studies to analyze the game genres that are most often used, the participants who are most often targeted for education, and the cybersecurity topics that most often appear in CTF games. Most cyber security education with the CTF concept focuses on students, with the most popular genre being Adventure and the discussion topics being quite diverse.

Keywords: *Cybersecurity education; Capture the Flag (CTF); game genre; target audience; cybersecurity topics.*

ABSTRAK

Keamanan siber merupakan tantangan serius dalam dunia teknologi informasi saat ini, dengan ancaman terhadap individu, perusahaan, dan negara. Edukasi keamanan siber masih rendah, menyebabkan ketidakpahaman, terutama di kalangan pelajar. Penggunaan gamifikasi ala Capture the Flag (CTF) dapat

meningkatkan minat dan pemahaman siswa. CTF memberikan pengalaman belajar yang interaktif dan menantang, mirip dengan situasi nyata yang dihadapi oleh para profesional keamanan siber. Namun, perlu pemilihan genre gim yang efektif dan penyesuaian dengan target peserta serta topik keamanan siber yang relevan. Penelitian ini meninjau literatur yang berkaitan dengan gim edukasi keamanan siber dengan pendekatan CTF. Pada penelitian ini akan dibahas: genre gim apa yang cocok digunakan untuk edukasi keamanan siber serta kaitannya dengan target peserta, target peserta edukasi keamanan siber serta kaitannya dengan topik keamanan siber yang dibahas. Penelitian ini dilakukan dengan cara mengelompokan beberapa penelitian untuk menganalisis genre gim yang paling sering dipakai, peserta yang paling sering menjadi target edukasi, dan topik keamanan siber yang paling sering muncul dalam gim CTF. Didapatkan bahwa sebagian besar edukasi keamanan siber dengan konsep CTF fokus ke mahasiswa, dengan genre terpopuler adalah *Adventure* dan topik bahasan cukup beragam.

Kata kunci: *Capture the Flag* (CTF); edukasi keamanan siber; genre gim; target peserta; topik keamanan siber.

PENDAHULUAN

Keamanan siber merupakan aspek krusial dalam dunia teknologi informasi saat ini. Dengan kemajuan pesat dalam teknologi dan konektivitas global, ancaman siber telah berkembang menjadi tantangan serius bagi individu, perusahaan, dan bahkan negara-negara. Ancaman siber dapat berupa serangan terhadap infrastruktur kritis, pencurian data pribadi, atau sabotase sistem yang dapat mengganggu kehidupan sehari-hari mereka.

Banyak dari pelajar yang tidak mengetahui atau memahami keamanan siber. Hal tersebut dikarenakan tingkat pemahaman dan kemampuan pengajar untuk mengajar keamanan siber masih rendah [1]. Akibatnya, pengajar belum siap untuk mengajar mata pelajaran terkait keamanan siber. Bidang keamanan siber penuh dengan prinsip-prinsip yang kompleks dan terus berubah. Ancaman siber terus berkembang dan para pelaku jahat selalu mencari cara baru untuk mengeksploitasi sistem.

Dalam upaya untuk mengatasi tantangan ini dan meningkatkan minat belajar dalam keamanan siber, dapat dipertimbangkan cara penyampaian pembelajaran, yaitu dengan penggunaan gamifikasi dengan konsep "Capture the Flag" (CTF) [1]. CTF adalah permainan yang umumnya digunakan dalam dunia keamanan siber. Dalam CTF, peserta diuji dengan serangkaian tantangan yang mencakup pemecahan masalah keamanan, seperti menemukan celah dalam kode program atau menganalisis data forensik untuk mengidentifikasi serangan. CTF menyediakan lingkungan belajar yang interaktif dan menantang, mirip dengan situasi nyata yang dihadapi oleh para profesional keamanan siber.

Sebuah penelitian [1] menyatakan bahwa Kompetisi CTF bagi siswa sekolah menengah merupakan sarana penting untuk memperkenalkan berbagai topik keamanan siber dan menumbuhkan minat mereka terhadap bidang ini. Platform kompetitif ini memungkinkan siswa untuk menerapkan pengetahuan teknis mereka dan membangun kepercayaan diri untuk berpartisipasi dalam kompetisi serupa di masa depan. Lebih dari itu, kompetisi CTF dapat menarik minat siswa ke bidang STEM (*science, technology, engineering, and mathematics*), mendorong pemikiran kreatif, dan meningkatkan kemampuan pemecahan masalah mereka. Namun dalam penelitian tersebut tidak dibahas bentuk gamifikasi yang cocok untuk diberikan terhadap siswa.

Oleh karena itu, agar penggunaan konsep CTF pada edukasi keamanan siber ini dapat diterapkan dengan baik, perlu dilakukan pemberian ruang lingkup. Beberapa di antaranya adalah pemilihan genre gim dan topik keamanan siber yang dibahas. Genre yang menawarkan platform paling efektif untuk pengembangan keterampilan dan pengetahuan perlu dikaji. Selain itu, diperlukan pula penentuan target edukasi. Hal tersebut untuk menyesuaikan mekanik dan konten yang akan digunakan. Penting halnya untuk menentukan peserta serta preferensi peserta. Hal itu adalah kunci untuk memaksimalkan manfaat penggunaan konsep CTF pada edukasi keamanan siber.

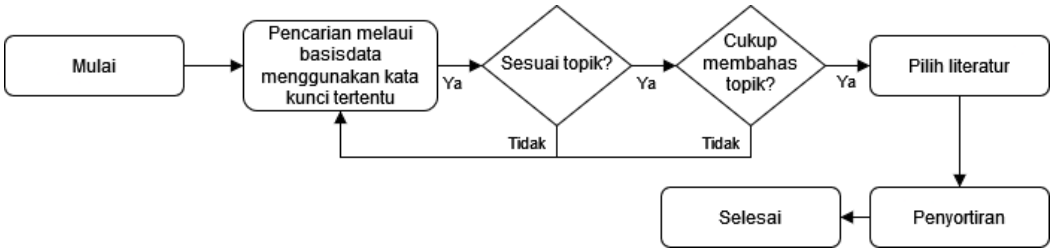
LANDASAN TEORI

Pada awalnya, kompetisi keamanan komputer Capture The Flag (CTF) berasal dari konvensi peretas terbesar di dunia, DEF CON. DEF CON adalah acara tahunan yang diadakan di Las Vegas, Nevada, yang pertama kali dimulai pada Juni 1993. Pada DEF CON, para peretas berkumpul untuk berbagi pengetahuan, keterampilan, dan teknik terbaru dalam keamanan komputer [2]. Dalam perkembangannya, para peretas di DEF CON mulai mengadakan kompetisi Capture The Flag sebagai bagian dari acara tersebut. Kompetisi CTF di DEF CON menjadi semakin populer dan menarik minat para peserta untuk menunjukkan kemampuan mereka dalam menyelesaikan tantangan keamanan komputer yang rumit [2]. Dengan demikian, dapat dikatakan bahwa awal mula CTF berasal dari DEF CON, kompetisi ini menjadi salah satu bagian yang menarik dan menantang bagi para peretas untuk menguji dan meningkatkan keterampilan keamanan komputer mereka.

CTF memiliki beragam format dan kategori yang disesuaikan dengan tingkat kesulitan dan target peserta. Salah satunya adalah *Learning Round*, yaitu tahap di mana konsep-konsep keamanan seperti rekayasa perangkat lunak, forensik, keamanan aplikasi web, dan keamanan aplikasi diunggah dan peserta harus menggunakan pembelajaran tersebut untuk memahami konsep tersebut. Lalu ada *Jeopardy Round*, ditujukan untuk menguji pengetahuan peserta tentang konsep keamanan komputer melalui serangkaian pertanyaan atau tantangan. Peserta harus menyelesaikan pertanyaan-pertanyaan tersebut untuk membuktikan pemahaman mereka tentang berbagai aspek keamanan komputer. Pada ronde ini, peserta akan diuji berdasarkan konsep keamanan yang telah diperkenalkan sebelumnya. Terakhir ada *Interactive Round*, bertujuan untuk menerapkan konsep keamanan siber dalam skenario dunia nyata. Pada ronde ini, setiap tim diberikan sebuah flag unik yang harus mereka pertahankan, dan poin diberikan berdasarkan keberhasilan menyerang dan mempertahankan sistem [1].

METODE

Penelitian ini menggunakan metode peninjauan literatur yang berkaitan dengan gim edukasi keamanan siber dengan pendekatan CTF. Diagram alir dari tinjauan disajikan pada Gambar 1.



Gambar 1 Diagram alir metodologi

Pencarian jurnal berasal dari beberapa sumber antara lain Google Scholar dan ScienceDirect. Dalam pencarian jurnal, digunakan beberapa kata kunci yaitu "CTF Game" dan "Cybersecurity Educational Game". Pencarian dilakukan dalam waktu satu minggu pada bulan November 2023 dengan menyeleksi jurnal-jurnal yang relevan menggunakan metode inklusi dan eksklusi, dengan kriteria inklusi yaitu: (1) menggunakan pendekatan CTF, dan (2) subjek relevan yang dibahas adalah keamanan siber.

Terdapat 23 jurnal yang relevan dengan topik, tetapi penulis memilih kembali 20 dari 23 literatur tersebut karena tiga jurnal sisanya kurang relevan untuk memberi penjelasan yang dibutuhkan. Analisis literatur dilakukan atas tiga aspek: genre gim, target gim, dan topik gim.

HASIL DAN PEMBAHASAN

Genre Gim

Mendalami pemahaman terhadap berbagai genre gim dalam konteks gim keamanan siber sangatlah penting. Genre gim dapat memengaruhi cara proses pembelajaran berlangsung. Sebagai contoh, gim dengan genre simulasi dapat memberikan kesan imersif terhadap penggunaan CTF, sedangkan gim dengan genre teka-teki dapat memberikan peluang untuk pemecahan masalah.

Selain itu, genre gim juga dapat memengaruhi tingkat motivasi siswa. Beberapa siswa mungkin lebih menyukai unsur kompetitif dalam gim dengan adanya fitur *leaderboard*, sementara lainnya mungkin lebih menyukai adanya unsur naratif dalam sebuah gim. Dengan memahami pengaruh dan keunggulan masing-masing genre, pengajar dapat meningkatkan pengalaman belajar siswa, memotivasi mereka untuk memahami konsep-konsep keamanan siber dengan lebih baik.

Tabel 1. Genre yang digunakan dalam literatur

No.	Genre	Literatur
1	Adventure	[3][4][5][6][1]
2	Quiz based	[7][8][9][10][11]
3	Simulator	[12][13][14][15]
4	RPG	[12][13][11]
5	Board Game	[16][17]
6	Augmented Reality	[18][19]
7	Point and Click	[7][9]
8	Escape Room	[20]

Berdasarkan Tabel 1, dapat dilihat bahwa beberapa gim memiliki banyak genre. Genre yang paling banyak dipakai adalah *Adventure*, kemudian diikuti dengan *Quiz Based*, dan *Simulator*. Genre *Adventure* lebih banyak dipakai karena sifatnya yang luas dan fleksibel. *Adventure* mencakup elemen eksplorasi, pemecahan teka-teki, dan pengembangan cerita, yang membuatnya mudah diadaptasi ke berbagai gaya permainan dan *setting*. Genre ini juga bisa dikombinasikan dengan genre lain sehingga menarik audiens yang lebih luas. Sementara itu, genre *Quiz Based* dipakai karena peserta bisa mendapatkan pengalaman yang sederhana, namun tetap merasakan dampaknya. Hal tersebut bisa menjadi pertimbangan jika peserta ingin belajar dan bermain, tetapi tidak ingin menatap layar. Genre *Simulator* juga memiliki banyak peminat karena peserta dapat merasakan simulasi dari topik CTF yang dibahas. Hal tersebut tentunya memungkinkan pemain mendapatkan pengalaman yang imersif.

Target Peserta

Menentukan target peserta yang tepat merupakan langkah krusial dalam memaksimalkan manfaat program atau kegiatan. Pemahaman ini menjadi kunci untuk merancang berbagai aspek penting, seperti materi, metode pembelajaran, strategi komunikasi, dan evaluasi. Dengan memahami target peserta, dapat disesuaikan konten, penyampaian, dan pendekatan belajar agar sesuai dengan kebutuhan, tingkat pengetahuan, minat, dan gaya belajar mereka. Hal ini akan meningkatkan efektivitas dan efisiensi program, serta membantu mencapai tujuan yang diinginkan.

Salah satu karakteristik target peserta adalah latar belakang pendidikan. Dengan memahami faktor tersebut, dapat diidentifikasi kelompok peserta yang paling tepat untuk mengikuti program atau kegiatan sehingga manfaatnya dapat dimaksimalkan.

Tabel 2. Target peserta edukasi

No.	Target	Literatur
1	Mahasiswa	[3][18][4][13][19][14][15][6]
2	Siswa SD	[7][8][9]
3	Orang Umum	[18][12]
4	Pegawai	[16][10]
5	Siswa SMA	[20]
6	Siswa SMP	[1]

Berdasarkan Tabel 2, dapat dilihat bahwa beberapa literatur cenderung menunjukkan target edukasi keamanan siber lebih dominan pada mahasiswa. Banyaknya mahasiswa yang menjadi target edukasi karena rata-rata materi keamanan siber yang diberikan sudah tingkat lanjut. Materi yang kompleks dapat menjadi hambatan bagi siswa SMP untuk belajar keamanan siber. Selain itu, umumnya mahasiswa memiliki keterampilan teknis yang lebih dibandingkan siswa SMP. Meskipun begitu, siswa SMP butuh edukasi keamanan siber karena mereka cukup aktif berinteraksi di internet. Siswa SMP dapat menjadi target pengembangan gim edukasi keamanan siber ke depan karena masih sedikitnya fasilitas untuk mereka dengan penyesuaian kompleksitas keamanan siber yang dibahas.

Berdasarkan Tabel 1 dan Tabel 2, dapat diidentifikasi preferensi genre dari setiap target peserta. Mahasiswa biasanya bermain genre: *Adventure*, *Board Game*, *Simulator*, *dan AR*. Sementara itu, siswa SMA bermain: *Escape Room*. Lalu, siswa SMP: *Adventure*. Siswa SD: *Quiz based*. Sisanya: *Adventure*, *Board Game*, *AR*, dan *RPG*. Dapat ditarik kesimpulan bahwa genre *Adventure* sangat populer di kalangan target peserta.

Topik Keamanan Siber

Topik keamanan siber sangat luas dan mencakup berbagai aspek, mulai dari cara melindungi data pribadi, perangkat elektronik, hingga jaringan internet. Oleh karena itu, penting untuk membedakan topik keamanan siber bagi setiap target peserta. Berikut ragam topik keamanan siber dengan batasan tiap target peserta:

1. Mahasiswa: *Basic terminal operations*[13], *Digital forensics*[13], *Network intrusion*[13], dan *Cyber Security threat*[19],
2. Siswa SMA: *Cryptography*[20] dan *Open source intelligence*[20],
3. Siswa SMP: *Cryptography*[1], *Cryptanalysis*[1], *Web investigation*[1], dan *Steganography*[1],
4. Siswa SD: *Basic Security*[7], *Privacy*[7],*Cyberbullying*[8], *Data privacy*[8], *Online reputation*[8], *Privacy and ethics*[8], dan *Fact checking*[8],
5. Lainnya: *Cyber awareness*[16].

Dalam format CTF pada jurnal yang disebutkan pada Tabel 1 atau Tabel 2, kebanyakan topik keamanan siber yang diangkat adalah seputar *ethical hacking* dan *penetration testing* sehingga topik tersebut masuk ke ruang lingkup mahasiswa. Kurangnya topik ringan seperti *cryptography, online privacy*, *phishing awareness*, *malware and viruses*, dsb., menyebabkan kurangnya edukasi keamanan siber pada lingkup siswa SMP.

KESIMPULAN

Berdasarkan hasil kajian literatur ini, dapat disimpulkan bahwa genre *Adventure* merupakan genre gim yang paling banyak digunakan dalam edukasi keamanan siber dengan konsep CTF, diikuti oleh genre *Quiz Based* dan *Simulator*. Kemudian target edukasi yang paling umum dalam literatur adalah mahasiswa dibanding dengan siswa sekolah. Topik seperti *ethical hacking* dan *penetration testing* lebih cocok untuk mahasiswa ataupun siswa SMA, sedangkan topik seperti *online privacy*, *phishing awareness*, dan *malware* lebih cocok untuk siswa SMP dan siswa SD. Oleh karena itu, dapat dipertimbangkan untuk menambah program edukasi keamanan siber dengan konsep CTF yang lebih spesifik untuk siswa SMP dan siswa SD.

UCAPAN TERIMA KASIH

Terima kasih kepada Program Studi Informatika - Program Sarjana, Fakultas Teknologi Industri, Universitas Islam Indonesia atas dukungannya dalam publikasi karya ilmiah ini.

DAFTAR PUSTAKA

[1] A. Haziq *et al.*, “A Scenario CTF-Based Approach in Cybersecurity Education for Secondary School Students 1,” 2021.

[2] A. D. Bin Ibrahim, A. H. Ashrofie Hanafi, H. Rokman, M. N. Ahmad Zawawi, Z. A. Ibrahim, and F. A. Rahim, “Comparative Analysis on Student’s Interest in Cyber Security among Secondary School Students using CTF Platform,” in *2020 8th International Conference on Information Technology and Multimedia, ICIMU 2020*, Institute of Electrical and Electronics Engineers Inc., Aug. 2020, pp. 73–77. doi: 10.1109/ICIMU49871.2020.9243561.

[3] S. Karagiannis and E. Magkos, “Adapting CTF Challenges into Virtual Cybersecurity Learning Environments,” 2020.

[4] A. Jaffray, C. Finn, and J. Nurse, *SherLOCKED: A Detective-themed Serious Game for Cyber Security Education*, vol. 613. in IFIP Advances in Information and Communication Technology, vol. 613. Cham: Springer International Publishing, 2021. doi: 10.1007/978-3-030-81111-2.

[5] T. Chen, L. Dabbish, and J. Hammer, “Self-efficacy-based game design to encourage security behavior online,” in *Conference on Human Factors in Computing Systems - Proceedings*, Association for Computing Machinery, May 2019. doi: 10.1145/3290607.3312935.

[6] S. Ros, S. Gonzalez, A. Robles, L. L. Tobarra, A. Caminero, and J. Cano, “Analyzing Students’ Self-Perception of Success and Learning Effectiveness Using Gamification in an Online Cybersecurity Course,” *IEEE Access*, vol. 8, pp. 97718–97728, 2020, doi: 10.1109/ACCESS.2020.2996361.

[7] F. Giannakas, A. Papasalouros, G. Kambourakis, and S. Gritzalis, “A comprehensive cybersecurity learning platform for elementary education,” *Information Security Journal*, vol. 28, no. 3, pp. 81–106, May 2019, doi: 10.1080/19393555.2019.1657527.

[8] S. Maqsood and S. Chiasson, “Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens,” *ACM Transactions on Privacy and Security*, vol. 24, no. 4, Nov. 2021, doi: 10.1145/3469821.

[9] B. Zahed, G. White, and J. Quarles, *Play It Safe An Educational Cyber Safety Game for Children in Elementary School*. 2019.

[10] F. Abu-Amara, R. Almansoori, S. Alharbi, M. Alharbi, and A. Alshehhi, "A novel SETA-based gamification framework to raise cybersecurity awareness," *International Journal of Information Technology (Singapore)*, vol. 13, no. 6, pp. 2371–2380, Dec. 2021, doi: 10.1007/s41870-021-00760-5.

[11] S. Scholefield and L. A. Shepherd, "Gamification Techniques for Raising Cyber Security Awareness," 2019.

[12] Z. A. Wen, Z. Lin, R. Chen, and E. Andersen, "What.Hack: Engaging Anti-Phishing Training through a Role-playing Phishing Simulation Game," in *Conference on Human Factors in Computing Systems - Proceedings*, Association for Computing Machinery, May 2019. doi: 10.1145/3290605.3300338.

[13] S. Karagiannis and E. Magkos, "Engaging Students in Basic Cybersecurity Concepts Using Digital Game-Based Learning: Computer Games as Virtual Learning Environments," 2021. [Online]. Available: http://www.zachtronics.com/tis-100/

[14] M. N. Katsantonis and I. Mavridis, "Evaluation of hacklearn cofelet game user experience for cybersecurity education," *International Journal of Serious Games*, vol. 8, no. 3, pp. 3–24, 2021, doi: 10.17083/IJSG.V8I3.437.

[15] A. Mittal, M. P. Gupta, M. Chaturvedi, S. R. Chansarkar, and S. Gupta, "Cybersecurity Enhancement through Blockchain Training (CEBT) – A serious game approach," *International Journal of Information Management Data Insights*, vol. 1, no. 1, Apr. 2021, doi: 10.1016/j.jjimei.2020.100001.

[16] S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A Serious Game for Cyber Security Awareness and Education," 2020. [Online]. Available: https://www.thinkfun.com/learn-coding/

[17] A. Yasin, L. Liu, T. Li, R. Fatima, and W. Jianmin, "Improving software security awareness using a serious game," *IET Software*, vol. 13, no. 2, pp. 159–169, Apr. 2019, doi: 10.1049/iet-sen.2018.5095.

[18] M. Korkiakoski, A. Antila, J. Annamaa, S. Sheikhi, P. Alavesa, and P. Kostakos, "Hack the Room: Exploring the potential of an augmented reality game for teaching cyber security," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Mar. 2023, pp. 349–353. doi: 10.1145/3582700.3583955.

[19] H. Alqahtani and M. Kavakli-Thorne, "Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR)," *Information (Switzerland)*, vol. 11, no. 2, Feb. 2020, doi: 10.3390/info11020121.

[20] G. Costa, M. Lualdi, M. Ribaudo, and A. Valenza, "A NERD DOGMA: Introducing CTF to Non-expert Audience," in *SIGITE 2020 - Proceedings of the 21st Annual Conference on Information Technology Education*, Association for Computing Machinery, Inc, Oct. 2020, pp. 413–418. doi: 10.1145/3368308.3415405.