

**APLIKASI RANSOMFORGE SEBAGAI GAME EDUKASI UNTUK
MENGOPTIMALKAN KESADARAN KEAMANAN SIBER**

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana pada
Program Studi Pendidikan Sistem dan Teknologi Informasi



Oleh

Adinda Maulida Tsani

NIM 2000654

**PROGRAM STUDI
PENDIDIKAN SISTEM DAN TEKNOLOGI INFORMASI
KAMPUS UPI DI PURWAKARTA
UNIVERSITAS PENDIDIKAN INDONESIA
2024**

LEMBAR HAK CIPTA
APLIKASI *RANSOMFORGE* SEBAGAI *GAME* EDUKASI UNTUK
MENGOPTIMALKAN KESADARAN KEAMANAN SIBER

Oleh:

Adinda Maulida Tsani
NIM 2000654

Sebuah skripsi yang diajukan untuk syarat memperoleh gelar Sarjana Pendidikan
pada program studi Pendidikan Sistem dan Teknologi Informasi

© **Adinda Maulida Tsani**

Universitas Pendidikan Indonesia

Agustus 2024

Hak cipta dilindungi undang-undang.

Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,
dicetak ulang, difoto kopi, atau cara lainnya tanpa ijin dari peneliti.

LEMBAR PENGEASAHAN

ADINDA MAULIDA TSANI

**APLIKASI *RANSOMFORGE* SEBAGAI *GAME* EDUKASI UNTUK
MENGOPTIMALKAN KESADARAN KEAMANAN SIBER**

disetujui dan disahkan oleh pembimbing:

Pembimbing I



Rizki Hikmawan, S.Pd., M.Pd.

NIPT. 920171219880731101

Pembimbing II



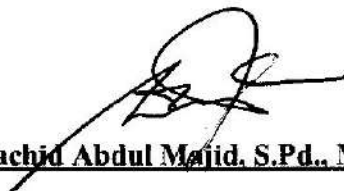
Ir. Nuur Wachid Abdul Majid, S.Pd., M.Pd., IPM., ASEAN Eng.

NIPT. 920171219910625101

Mengetahui,

Ketua Program Studi

Pendidikan Sistem dan Teknologi Informasi



Ir. Nuur Wachid Abdul Majid, S.Pd., M.Pd., IPM., ASEAN Eng.

NIPT. 920171219910625101

LEMBAR PERNYATAAN KEASLIAN SKRIPSI

Bismillahirrahmaanirrahiim.

Saya yang bertanda tangan di bawah ini:

Nama Mahasiswa : Adinda Maulida Tsani

NIM : 2000654

Program Studi : Pendidikan Sistem dan Teknologi Informasi

Dengan ini saya menyatakan bahwa skripsi dengan judul "**Aplikasi *RansomForge* sebagai *Game* Edukasi untuk Mengoptimalkan Kesadaran Keamanan Siber**" ini beserta seluruh isinya adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung risiko/sanksi apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Purwakarta, 20 Agustus 2024

Yang Membuat Pernyataan



Adinda Maulida Tsani

NIM. 2000654

KATA PENGANTAR

Bismillahirrahmaanirrahiim

Dengan mengucapkan alhamdulillah rabbil aalamiin, segala puji dan syukur penulis panjatkan kekhadirat Allah SWT yang melimpahkan berkat rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “Aplikasi *RansomForge* sebagai *Game* Edukasi untuk Mengoptimalkan Kesadaran Keamanan Siber”. Penulis mempersembahkan karya skripsi ini sebagai hasil dari perjalanan panjang yang penuh dengan tantangan dan pembelajaran. Penulisan skripsi ini merupakan bagian penting dalam menyelesaikan masa studi di program sarjana, yang telah memberikan banyak pengalaman berharga dan pengetahuan baru.

Penulis menyadari bahwa perjalanan ini tidak selalu mudah. Banyak rintangan yang harus dihadapi. Setiap tahap dalam proses penulisan ini telah memberikan pelajaran yang berharga dan memperkuat kemampuan penulis dalam melakukan penelitian.

Akhir kata, terimakasih kepada diri saya sendiri untuk segala usaha, kerja keras dan kepercayaan diri sehingga dapat menyelesaikan skripsi ini. Penulis berharap bahwa segala usaha dan kerja keras yang telah dicurahkan dalam penulisan skripsi ini dapat memberikan hasil yang memuaskan dan menjadi inspirasi bagi mahasiswa lainnya untuk terus berjuang dan berkarya. Penulis juga berharap bahwa skripsi ini dapat menjadi salah satu bentuk kontribusi nyata khususnya di bidang pendidikan, dan menjadi referensi bagi penelitian-penelitian selanjutnya. Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan untuk perbaikan dan penyempurnaan di masa mendatang.

Purwakarta, 20 Agustus 2024



Adinda Maulida Tsani

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan ke kehadiran Allah SWT, karena atas rahmat dan hidayah-Nya penulis akhirnya dapat menyelesaikan skripsi ini tepat pada waktunya. Perjalanan ini bukanlah sebuah usaha individual semata, tetapi merupakan hasil dari sinergi, bantuan, dan inspirasi dari banyak pihak. Adapun dalam kesempatan ini penulis ingin mengucapkan banyak terimakasih kepada:

1. Mengucapkan puji syukur kepada Allah SWT atas berkat dan rahmat-Nya yang selalu melimpah, memberikan kekuatan dan ketabahan dalam setiap langkah proses penelitian ini. Tanpa izin-Nya, karya ini tak mungkin terwujud.
2. Kedua orang tua tercinta Ayahanda saya Muhidin dan Ibunda Ernawangsih yang senantiasa memberikan dukungan tanpa batas baik dukungan moral maupun materil. Terima kasih atas kasih sayang, doa, motivasi dan semangat yang tak pernah surut. Kalian adalah sumber inspirasi terbesar dalam hidup penulis. Gelar sarjana ini penulis persembahkan untuk kedua orang tua tercinta.
3. Kakak Moehammad Azhizi Ramdhani dan Natasha Sofa Marwah, yang senantiasa memberikan dukungan, kasih sayang, sumber inspirasi dan motivasi bagi saya untuk terus maju dan menyelesaikan penelitian ini dengan sebaik mungkin. Tak lupa juga untuk keponakan kecilku Arcilla Gracellina Azna. Meski masih bayi, kehadiranmu telah membawa kebahagiaan dan menjadi semangat bagi saya dalam menyelesaikan penelitian ini.
4. Keluarga Besar Abah Jumsit, terutama nenek, tante, om, dan sepupu-sepupu tercinta. Dukungan, kasih sayang, dan kebersamaan kalian selalu memberikan semangat dan kenyamanan bagi saya. Terima kasih telah menjadi bagian penting dalam perjalanan saya menyelesaikan penelitian ini.
5. Prof. Dr. Yayan Nurbayan, M.Ag, selaku Direktur Universitas Pendidikan Indonesia Kampus di Purwakarta yang selalu memberikan segala fasilitas dan dukungan selama penulis menempuh pendidikan di universitas ini.
6. Rizki Hikmawan, S.Pd., M.Pd, selaku dosen wali sekaligus pembimbing 1 yang selalu memberikan ilmu pembelajaran yang sangat bermakna, yang dengan sabar dan penuh perhatian memberikan bimbingan, masukan, motivasi dan meluangkan waktunya selama proses penyusunan skripsi ini. Dukungan dan

arahan yang diberikan sangat berarti dalam penyelesaian skripsi ini maupun dalam pembelajaran selama jenjang perkuliahan.

7. Ir. Nuur Wachid Abdulmajid, S.Pd., M.Pd., IPM., ASEAN Eng, selaku ketua Program Studi Pendidikan Sistem dan Teknologi Informasi sekaligus dosen pembimbing 2 yang selalu memberikan masukan berharga dan saran yang membangun serta selalu memberikan arahan dan dukungan bagi kemajuan akademik.
8. Segenap dosen dan staf akademik di Program Studi Pendidikan Sistem dan Teknologi Informasi yang telah memberikan ilmu dan bantuan selama masa studi.
9. Lutfiah Anisa Sholaihah, Memei Sri Mulyani, Mia Tri Praciska selaku sahabat yang telah menjadi sumber dukungan dan inspirasi selama masa studi ini. Terima kasih atas kebersamaan, dukungan, dan semangat yang telah diberikan.
10. Mayda Fuar selaku teman yang sama-sama berjuang kebersamai dan memberikan banyak bantuan dalam penulisan skripsi.
11. Teman seperjuangan PSTI angkatan 2020 yang saling memberikan dukungan, penguatan dan motivasi selama proses penyelesaian skripsi.
12. Seluruh pihak yang tidak dapat disebutkan satu per satu, yang telah memberikan dukungan, baik secara langsung maupun tidak langsung. Setiap bantuan, saran, dan doa yang diberikan sangat berarti bagi penulis.

Akhirnya, penulis hanya bisa mengucapkan terimakasih atas bantuannya dan semoga dibalas dengan kelimpahan berkah Allah SWT. Aamiin.

APLIKASI RANSOMFORGE SEBAGAI GAME EDUKASI UNTUK MENGOPTIMALKAN KESADARAN KEAMANAN SIBER

Adinda Maulida Tsani

NIM 2000654

ABSTRAK

Keamanan digital menjadi semakin penting seiring dengan meningkatnya ketergantungan pada teknologi, terutama dalam melindungi aset digital yang bernilai strategis. Di Indonesia, ancaman siber seperti *ransomware* terus meningkat, sementara kesadaran masyarakat terhadap ancaman ini masih rendah, terutama karena kurangnya edukasi yang memadai. Penelitian ini bertujuan untuk merancang dan mengembangkan aplikasi *RansomForge*, sebuah game edukasi yang menggunakan metode pengembangan *Game Development Life Cycle* (GDLC) dan didasarkan pada hasil analisis dekomposisi *ransomware*. Game ini dirancang untuk memberikan pengalaman interaktif yang mendalam, meningkatkan kesadaran, serta pemahaman masyarakat tentang cara kerja dan risiko *ransomware*. Tahapan *Game Development Life Cycle* (GDLC), yang mencakup tahap inisiasi, pra-produksi, produksi, pengujian alpha, pengujian beta, dan rilis. Pada tahap pengujian alpha menggunakan *black box testing* oleh pengembang sendiri. Pengujian beta dilakukan dengan metode *one-on-one validation* dengan melibatkan dua tester. Hasil pengujian alpha menunjukkan aplikasi berfungsi sesuai harapan, sedangkan pengujian beta menghasilkan umpan balik positif dengan beberapa revisi. Meskipun perbaikan telah dilakukan, penelitian ini hanya mencapai tahap beta, sehingga belum dapat dipastikan seberapa efektif aplikasi ini dalam meningkatkan kesadaran keamanan siber secara luas. Dengan berfokus pada pengembangan berbasis pengguna dan iterasi berulang, penelitian ini diharapkan dapat menjadi landasan bagi pengembangan lebih lanjut game edukasi serupa, sekaligus menyediakan dasar untuk evaluasi efektivitas dalam meningkatkan kesadaran masyarakat luas terhadap ancaman siber.

Kata kunci: Keamanan Siber, *Ransomware*, Game Edukasi, *Game Development Life Cycle* (GDLC).

RANSOMFORGE APPLICATION AS AN EDUCATIONAL GAME TO OPTIMIZE CYBERSECURITY AWARENESS

Adinda Maulida Tsani

NIM 2000654

ABSTRACT

Digital security is becoming increasingly important as the reliance on technology increases, especially in protecting digital assets of strategic value. In Indonesia, cyber threats such as ransomware continue to increase, while public awareness of these threats is still low, mainly due to the lack of adequate education. This research aims to design and develop the RansomForge application, an educational game that uses the Game Development Life Cycle (GDLC) development method and is based on the results of decompilation analysis ransomware. This game is designed to provide an immersive interactive experience, increase awareness, and public understanding of how ransomware works and risks. The Game Development Life Cycle (GDLC) stages, which include initiation, pre-production, production, alpha testing, beta testing, and release. At the alpha testing stage using black box testing by the developers themselves. Beta testing was carried out using the one-on-one validation method involving two testers. The results of alpha testing showed that the application functioned as expected, while beta testing resulted in positive feedback with some revisions. Although improvements have been made, this research only reached the beta stage, so it is not yet certain how effective this application is in increasing cybersecurity awareness at large. By focusing on user-driven development and iterative iteration, this research is expected to serve as a foundation for further development of similar educational games, as well as provide a basis for evaluating their effectiveness in raising awareness of cyber threats among the general public.

Keywords: *Cybersecurity, Ransomware, Educational Games, Game Development Life Cycle (GDLC).*

DAFTAR ISI

LEMBAR HAK CIPTA	ii
LEMBAR PENGEASAHAN	iii
LEMBAR PERNYATAAN KEASLIAN SKRIPSI	iv
KATA PENGANTAR.....	v
UCAPAN TERIMA KASIH	vi
ABSTRAK	viii
<i>ABSTRACT</i>	ix
DAFTAR ISI	x
DAFTAR TABEL.....	xii
DAFTAR GAMBAR	xiii
DAFTAR LAMPIRAN	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Penelitian	1
1.2 Rumusan dan Batasan Masalah Penelitian.....	6
1.3 Tujuan Penelitian.....	7
1.4 Manfaat / Signifikansi Penelitian	7
1.5 Struktur Organisasi Skripsi.....	8
BAB II KAJIAN PUSTAKA	10
2.1 <i>Cyber Security</i> (Keamanan Siber).....	10
2.2 <i>Ransomware</i>	17
2.3 <i>Computer Based Learning</i>	24
2.4 <i>Game</i>	26
2.5 Penelitian Relevan.....	30
BAB III METODE PENELITIAN.....	33
3.1 Jenis Penelitian	33
3.2 Desain Penelitian	34
3.3 Prosedur Penelitian.....	34
3.4 Subjek Penelitian.....	38
3.5 Instrumen Penelitian.....	38
3.6 Analisis Data.....	39

BAB IV TEMUAN DAN PEMBAHASAN	40
4.1 Temuan	40
4.2 Pembahasan	75
BAB V SIMPULAN, IMPLIKASI, DAN REKOMENDASI	83
5.1 Simpulan.....	83
5.2 Implikasi.....	84
5.3 Rekomendasi	85
DAFTAR PUSTAKA	86
LAMPIRAN.....	91
RIWAYAT HIDUP	129

DAFTAR TABEL

Tabel 3.1 Kisi-kisi Instrumen Observasi	39
Tabel 4.1 Indikator Keberhasilan	48
Tabel 4.2 <i>Storyboard Game</i>	54
Tabel 4.3 Pengumpulan Aset.....	57
Tabel 4.4 <i>Black Box Testing</i>	71
Tabel 4.5 Pengujian Beta.....	74
Tabel 4.6 Perbaikan dan Penyempurnaan	80

DAFTAR GAMBAR

Gambar 1.1 Grafik Trafik Anomali Januari - Desember 2023	2
Gambar 1.2 Top 10 Trafik Anomali Tahun 2023	3
Gambar 1.3 Aktivitas <i>Ransomware</i> yang terjadi di Indonesia Tahun 2023	3
Gambar 1.4 Contoh Kasus Serangan <i>Ransomware</i>	4
Gambar 3.1 Tahapan GDLC.....	34
Gambar 3.2 Prosedur Penelitian.....	34
Gambar 4.1 Kode Program Generasi Kunci	40
Gambar 4.2 Kode Program Enkode Kunci Publik	41
Gambar 4.3 Kode Program Payload Enkripsi	42
Gambar 4.4 Kode Program Payload Dekripsi.....	46
Gambar 4.5 <i>Flowchart</i>	52
Gambar 4.6 Import Material dan Asset.....	60
Gambar 4.7 Proses Konstruksi Material dan Asset.....	61
Gambar 4.8 Tampilan Menu Utama	62
Gambar 4.9 Tampilan Opening	62
Gambar 4.10 Tampilan Pilih Level/Target	63
Gambar 4.11 Tampilan Prolog dan Epilog	63
Gambar 4.12 Tampilan Kuis	64
Gambar 4.13 Tampilan <i>Feedback</i> Jawaban Benar	64
Gambar 4.14 Tampilan Berhasil Melewati <i>Stage</i>	65
Gambar 4.15 Tampilan <i>Feedback</i> Jawaban Salah & Kunci Jawaban	65
Gambar 4.16 Tampilan Gagal Melewati <i>Stage</i>	66
Gambar 4.17 Tampilan Waktu Pengerjaan Habis	66
Gambar 4.18 Tampilan Berhasil Melewati Misi	67
Gambar 4.19 Tampilan Pengaturan	67
Gambar 4.20 Tampilan Panduan	68
Gambar 4.21 Langkah <i>Export</i>	69
Gambar 4.22 <i>Build Setting</i>	69
Gambar 4.23 <i>Player Setting</i>	70
Gambar 4.24 Pilih Lokasi Penyimpanan File	70

DAFTAR LAMPIRAN

Lampiran 1. Surat Keputusan Pembimbing Skripsi.....	91
Lampiran 2. Kartu Bimbingan	94
Lampiran 3. Tabel Simbol dan Fungsi <i>Flowchart</i>	96
Lampiran 4. Butir-Butir Soal	97
Lampiran 5. Hasil Pengujian Beta Testing.....	118
Lampiran 6. Dokumentasi.....	128

DAFTAR PUSTAKA

- Abdul, M., Ys, F., Parga Zen, B., & Wasitarini, D. E. (2023). *Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpunas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi* (Vol. 6, Issue 2).
- Aditama, W. B., Ramdani, A., & Khairunnisa, K. (2021). Penerapan Computer Based Instruction Model Simulasi dalam Pembelajaran IPA Sekolah Dasar. *Journal of Classroom Action Research*, 3(1), 30–45. <https://doi.org/10.29303/jcar.v3i1.651>
- Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politika Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, 13(2), 222–238. <https://doi.org/10.22212/jp.v13i2.3299>
- Alfarabi Helpendi, & Eko Purnomo. (2024). Game Multimedia tentang Sistem Tata Surya Berbasis Android sebagai Media Edukasi pada Anak Usia 6-12 Tahun. *Jurnal Riset Rumpun Seni, Desain Dan Media*, 3(1), 239–247. <https://doi.org/10.55606/jurrsendem.v3i1.2662>
- Badan Siber dan Sandi Negara. (2023). *Lanskap Keamanan Siber Indonesia 2023*.
- Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, 3, 223–234. <https://doi.org/10.54706/senastindo.v3.2021.141>
- Budi Warsito, A. (2023). LockBit Black Ransomware On Reverse Shell: Analysis of Infection Ransomware LockBit Black di Dalam Reverse Shell: Analisis Infeksi. *Cogito Smart Journal* |, 9(2). <https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/>
- Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency. *Riwayat Artikel Diterima*, 10(2). <https://doi.org/10.22212/jp.v10i1.1447>
- Cicala, F., & Bertino, E. (2022). Analysis of Encryption Key Generation in Modern Crypto Ransomware. *IEEE Transactions on Dependable and Secure Computing*, 19(2), 1239–1253. <https://doi.org/10.1109/TDSC.2020.3005976>
- Cloramidine, F., & Badaruddin, M. (2023). MENGUKUR KEAMANAN SIBER INDONESIA MELALUI INDIKATOR PILAR KERJASAMA DALAM

- GLOBAL CYBERSECURITY INDEX (GCI). In *Jurnal Sosial dan Humaniora* (Vol. 8, Issue 1).
- Darman, & Hasnawati. (2021). Pengembangan Media Pembelajaran Berbasis Komputer Berorientasi Model Drills And Praticce. *Decode: Jurnal Pendidikan Teknologi Informasi*, 1(1), 1–7. <https://doi.org/10.51454/decode.v1i1.1>
- Darmawan, B. I. (2019). *Simulasi dan Analisis Encryption Based Ransomware untuk Memetakan Evolusi Ransomware*. Universitas Islam Indonesia.
- Darmawan, B. I., & Yudha, F. (2019). *Simulasi dan Analisis Encryption Based Ransomware untuk Memetakan Evolusi Ransomware*.
- Fameska, E., Okra, R., & Antoni Musril, H. (2023). PERANCANGAN MEDIA PEMBELAJARAN BERBASIS GAME EDUKASI MENGGUNAKAN MIT APP INVENTOR PADA PELAJARAN PAI. In *Jurnal Mahasiswa Teknik Informatika* (Vol. 7, Issue 1).
- Febrian, V., Ramadhan, M. R., Faisal, M., & Saifudin, A. (2020). *Pengujian pada Aplikasi Penggajian Pegawai dengan menggunakan Metode Blackbox*. 5(1), 2622–4615. <http://openjournal.unpam.ac.id/index.php/JTSI/index61>
- Ginanjar, Y. (2022). STRATEGI INDONESIA MEMBENTUK CYBER SECURITY DALAM MENGHADAPI ANCAMAN CYBER CRIME MELALUI BADAN SIBER DAN SANDI NEGARA. *Jurnal Dinamika Global*, 7(02), 291–312. <https://doi.org/10.36859/jdg.v7i02.1187>
- Hamasi, H. F., & Anggapuspa, M. L. (2024). ANALISIS VISUAL DESAIN KARAKTER MOTH PADA GAME ONLINE SKY CHILDREN OF THE LIGHT. *Jurnal Barik*, 6(2), 145–158. <https://ejournal.unesa.ac.id/index.php/JDKV/>
- Harahap, A. H., Difa Andani, C., Christie, A., Nurhaliza, D., & Fauzi, A. (2023). Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder. *Jurnal Manajemen Dan Pemasaran Digiti (JMPD)*, 1(2), 73–83.
- Hartono, B. (2023a). *Ransomware: Memahami Ancaman Keamanan Digital*. *Bincang Sains Dan Teknologi*, 2(02), 55–62. <https://doi.org/10.56741/bst.v2i02.353>
- Hartono, B. (2023b). *Ransomware: Memahami Ancaman Keamanan Digital*. *Bincang Sains Dan Teknologi*, 2(02), 55–62. <https://doi.org/10.56741/bst.v2i02.353>
- Hidayatulloh, S., Praherdhiono, H., & Wedi, A. (2020). Pengaruh Game Pembelajaran Terhadap Peningkatan Hasil Belajar Pemahaman Ilmu Pengetahuan Alam. *JKTP: Jurnal Kajian Teknologi Pendidikan*, 3(2), 199–206. <https://doi.org/10.17977/um038v3i22020p199>

- Hoshmand, M. O., Ratnawati, S., & Korespondensi, E. P. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. *Jurnal Sains Dan Teknologi*, 5(2), 679–686. <https://doi.org/10.55338/saintek.v5i2.2347>
- Ikhwanul Uzlah, L., & Adi Saputra, R. (2024). DETEKSI SERANGAN SIBER PADA JARINGAN KOMPUTER MENGGUNAKAN METODE RANDOM FOREST. In *Jurnal Mahasiswa Teknik Informatika* (Vol. 8, Issue 3). <https://bit.ly/CyberSecurityAttacks>.
- Islami, M. J. (2017). *TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN GLOBAL CYBERSECURITY INDEX*.
- Kamal, M. (2020). Research and Development (R&D) tadribat/drill madrasah aliyah class x teaching materials arabic language. *Pendidikan Dan Humaniora*, 4(1), 10–18. <https://doi.org/10.36526/js.v3i2>
- Kertopati, L. (2017, May 13). Dua Rumah Sakit di Jakarta Kena Serangan Ransomware WannaCry . *CNN Indonesia*.
- Kunto, I., Ariani, D., Widyaningrum, R., & Syahyani, R. (2021). Ragam Storyboard Untuk Produksi Media Pembelajaran. *Jurnal Pembelajaran Inovatif*, 4(1), 108–120. <https://doi.org/10.21009/jpi.041.14>
- Lalu, A., Kendaraan, L., Berbasis, B., Faris, A., Argadiraksa, R., & Windriyani, P. (2022). *Pengembangan Gim Edukasi 2D* (Vol. 8, Issue 1).
- Luthfah, D. (2021). Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia (Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law). *TerAs Law Review : Jurnal Hukum Humaniter Dan HAM*, 3(1), 11–22. <https://doi.org/10.25105/teras-lrev.v3i1.10742>
- Manoppo, V. A., Lumenta, A. S. M., & Karouw, S. D. S. (2020). Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi. *Jurnal Teknik Elektro Dan Komputer*, 9(3), 181–188.
- Martono, K. T. (2015). Pengembangan game dengan menggunakan game engine game maker. *Jurnal Sistem Komputer*, 5(1), 23–30.
- Menora, T., Primasari, C. H., Wibisono, Y. P., Sidhi, T. A. P., Setyohadi, D. B., & Cininta, M. (2023). *Implementasi Pengujian Alpha dan Beta Testing pada Aplikasi Gamelan Virtual Reality* (Vol. 3, Issue 1).
- Muhajarah, K., & Rachmawati, F. (2019). Game edukasi berbasis Android: Urgensi penggunaan, pengembangan dan penguji kelayakan. *Justek: J*, 2(2), 29–36. *Jurnal Sains Dan Teknologi*, 2(2), 29–36. <https://doi.org/10.31764/justek.vXiY.3733>
- Noralia Purwa Yunita, Prof. R. E. I. (2022). *GAMIFICATION: Membuat Belajar Seasyik Bermain Game*. Andi.

- Nur, R., Pusklat, R., Siber, B., & Negara, S. (2022). *Cendekia Niaga Journal of Trade Development and Studies Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia*.
- Praptono, A., & Yusuf, H. (2024). JICN: Jurnal Intelek dan Cendekiawan Nusantara Criminology Review of Extortion Crimes Using Viruses, Wannacry Ransomware as a Modern Crime. *Jurnal Intelek Dan Cendekiawan Nusantara*, *1*(2), 1660–1669. <https://jicnusantara.com/index.php/jicn>
- Rabbani, S., & Diana, D. (2023). Prediksi Kategori Serangan Siber dengan Algoritma Klasifikasi Random Forest Menggunakan Rapidminer. *SMATIKA JURNAL*, *13*(02), 284–293. <https://doi.org/10.32664/smatika.v13i02.934>
- Rahayu, D. (n.d.). *Indonesia National Cybersecurity Review: Before and After Establishment National Cyber and Crypto Agency (BSSN) Mulyadi*. www.krebsonsecurity.com
- Ramalinda, D., & Rachmat Raharja, A. (2024). Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi. *Journal of International Multidisciplinary Research*, *2*(6), 665–671. <https://journal.banjaresepacific.com/index.php/jimr>
- Sama, H., Licen, L., Saragi, J. S. D., Erline, M., Kelvin, K., Hartanto, Y., Winata, J., & Devalia, M. (2021). STUDI KOMPARASI FRAMEWORK NIST DAN ISO 27001 SEBAGAI STANDAR AUDIT DENGAN METODE DESKRIPTIF STUDI PUSTAKA. *Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab*, *6*(2), 116–121. <https://doi.org/10.36341/rabit.v6i2.1752>
- Sefina Samosir, R., & Purwandari, N. (2020). *Aplikasi Literasi Digital Berbasis Web Dengan Metode R&D dan MDLC Web-Based Digital Literacy using R&D and MDLC Methods* (Vol. 19, Issue 2).
- Suryadi, A. (2017). *Perancangan aplikasi game edukasi menggunakan model waterfall*. (Vol. 3, Issue 1).
- Syafuddin, K. (2023). PENINGKATAN LITERASI KEAMANAN DIGITAL DAN PERLINDUNGAN DATA PRIBADI BAGI SISWA DI SMPN 154 JAKARTA. *Eastasouth Journal of Impactive Community Services*, *1*(03), 122–133. <https://doi.org/10.58812/ejimcs.v1.i03>
- Wahyu Wahidin, G., & Sari, Z. (2022). Analisis Ransomware Wannacry Menggunakan Aplikasi Cuckoo Sandbox. *REPOSITOR*, *4*(1), 83–94.
- Windawati, R., & Koeswanti, H. D. (2021). Pengembangan Game Edukasi Berbasis Android untuk Meningkatkan hasil Belajar Siswa di Sekolah Dasar. *Jurnal Basicedu*, *5*(2), 1027–1038. <https://doi.org/10.31004/basicedu.v5i2.835>

APPROACH & REDESIGN METHODOLOGY IN CV. BAROKAH ABADI.

Zalukhu, A., Purba, S., Darma, D., Zalukhu¹, A., Purba², S., Darma³, D., Teknik Informatika, M., & Industri, F. T. (2023). PERANGKAT LUNAK APLIKASI PEMBELAJARAN FLOWCHART. *Jurnal Teknologi Informasi Dan Industri*, 4(1).