PLATFORM EDUKASI KEAMANAN SIBER BERBASIS WEB BERDASARKAN KERANGKA GLOBAL LITERASI DIGITAL UNESCO

Nilam Qolbi[1)], Herman Kabetta[2)]
email: herman.kabetta@poltekssn.ac.id
[1] Badan Siber dan Sandi Negara, Indonesia
[2] Program Studi Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara

Ringkasan

Perkembangan teknologi informasi yang cepat diiringi dengan meningkatnya risiko serangan siber. Pada tahun 2023 tercatat lebih dari 400 juta serangan siber ke Indonesia. Rendahnya kesadaran masyarakat mengenai keamanan siber menjadi salah satu penyebab utama meningkatnya serangan tersebut. Pada penelitian ini dikembangkan sebuah aplikasi edukasi berbasis web yang diharapkan dapat menjadi media sosialisasi kesadaran keamanan informasi. Aplikasi dikembangkan berdasarkan kerangka global literasi digital dari UNESCO yaitu, A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2. Penelitian ini menggunakan tiga dari empat tahapan model penelitian dan pengembangan four-d model yaitu tahap define, design, dan develop untuk menjabarkan area kompetensi safety ke dalam bentuk indikator dan pertanyaan. Penjabaran variabel menyesuaikan aturan dalam Taksonomi Bloom pada ranah kognitif, kemudian dilakukan uji validitas dan reliabilitas meliputi pengujian validitas butir soal dan kevalidan soal, serta pengujian reliabilitas terhadap 50 responden menggunakan rumus perhitungan KR 20. Hasil pengujian menunjukkan bahwa indikator dan pertanyaan yang digunakan dinyatakan valid dan reliabel, dengan nilai koefisien reliabilitas sebesar 0,788. Pengujian ini memastikan bahwa, instrumen dalam aplikasi dapat secara konsisten mengukur tingkat pemahaman dan kesadaran keamanan informasi pengguna. Penilaian terhadap aplikasi dilakukan menggunakan user acceptance test dengan hasil persentase penerimaan sebesar 81,11%. Hasil ini membuktikan bahwa aplikasi diterima dengan baik oleh pengguna, baik dari segi kemudahan penggunaan maupun relevansi konten, sehingga berpotensi efektif sebagai media sosialisasi. Secara keseluruhan, hasil pengujian reliabilitas dan tingkat penerimaan pengguna mendukung pencapaian tujuan utama aplikasi, yaitu meningkatkan kesadaran masyarakat terhadap keamanan informasi melalui media edukasi yang dikembangkan.

Kata Kunci : digital literacy, web-based, keamanan siber.

1. PENDAHULUAN

Perkembangan teknologi informasi membawa banyak peningkatan di berbagai bidang, salah satunya terletak pada bidang keamanan siber. Perkembangan tersebut berbanding lurus dengan risiko kejahatan yang kemungkinan dapat terjadi. Pada tahun 2023, tercatat 403.990.813 serangan siber yang terjadi [1] di Indonesia meliputi *Trojan Activity, Information Gathering,* dan *Web Application Attack*. Berdasarkan banyaknya jenis dan kasus serangan siber, serangan pada layanan daring di masyarakat menjadi salah satu kasus yang sering terjadi. Hal ini melibatkan pertukaran informasi pribadi berupa alamat rumah, akun internet *banking* hingga detail kartu kredit, interaksi dengan situs web yang tidak aman [2], pembuatan kata sandi yang lemah [3], dan mengunduh berkas dari *website* yang berbahaya [4]. Menurut Fattah et al. [5] dalam survei yang dilakukan, menyatakan bahwa kesadaran masyarakat dalam kejahatan siber, praktik keamanan siber, serta peran pemerintah dan organisasi dalam memastikan keamanan informasi di internet masih sangat terbatas. Hal serupa didukung dengan pendapat Tan et al [6] yang melakukan survei terhadap mahasiswa, hasil survei menyatakan bahwa responden memiliki kesadaran keamanan siber yang rendah. Rendahnya tingkat literasi keamanan siber ini memperbesar kerentanan terhadap kejahatan siber, seperti pencurian data pribadi dan keuangan, yang berdampak signifikan pada individu dan organisasi.

Salah satu tantangan utama dalam meningkatkan keamanan siber adalah kurangnya pengetahuan masyarakat tentang cara melindungi informasi pribadi. Serangan siber yang menargetkan individu maupun perusahaan seperti *phishing*, *ransomware*, dan *malware* semakin meningkat, hal ini disebabkan karena individu maupun perusahaan tidak cukup memahami risiko keamanan siber. Selain itu, faktor kelalaian dalam menjaga privasi data juga memicu terjadinya kebocoran data yang dapat memberi kerugian, baik secara finansial maupun terhadap reputasi [7]. Edukasi menjadi sangat penting untuk meminimalkan risiko-risiko ini dan memastikan masyarakat terhindar dari serangan berbahaya yang menyebabkan kerugian.

Upaya peningkatan kesadaran publik mengenai keamanan siber menjadi penting. Oleh karena itu, diperlukan sebuah inisiatif berbasis teknologi yang tidak hanya memberikan informasi, tetapi juga mampu meningkatkan keterlibatan aktif masyarakat dalam memahami keamanan siber. Edukasi berbasis digital menjadi salah satu pendekatan yang efektif [8], dengan mempertimbangkan tingginya penggunaan teknologi informasi di Indonesia. Selain memberikan informasi teoritis, penggunaan aplikasi berbasis web sebagai media edukasi juga memungkinkan pengguna untuk berlatih dan menguji pemahaman mereka melalui simulasi dan tes interaktif [9], [10].

Dengan mengacu pada kerangka global literasi digital dari UNESCO yaitu *A Global Framework of Reference on Digital Literacy Skills for Indicator* 4.4.2 [11], aplikasi yang dikembangkan diharapkan dapat memberikan pemahaman komprehensif mengenai pentingnya keamanan informasi. Adanya *pre-test* dan *post-test/quiz* dalam media edukasi ini juga memungkinkan dilakukannya evaluasi terhadap peningkatan kesadaran dan pemahaman masyarakat terkait keamanan siber [12]. Selain itu, dilakukan juga pengujian reliabilitas untuk menunjukkan bahwa indikator dan pertanyaan dalam aplikasi, memiliki konsistensi yang baik, dan instrumen yang digunakan dalam aplikasi (seperti pertanyaan atau modul) dapat dipercaya untuk mengukur pemahaman atau kesadaran keamanan informasi secara konsisten.

Aplikasi yang dikembangkan diharapkan dapat menjadi potensi efektif sebagai media sosialisasi, yang dapat dilihat dari indikator terhadap kesediaan pengguna untuk menggunakannya dan sesuai dengan kebutuhan terkait kesadaran keamanan informasi. Oleh karena itu, pada penelitian ini juga dilakukan pengujian terhadap penerimaan pengguna (*user acceptance test*) untuk membuktikan hal tersebut.

2. KAJIAN PUSTAKA

Perkembangan teknologi informasi membawa banyak peningkatan di berbagai bidang, salah satunya terletak pada bidang keamanan siber. Perkembangan tersebut berbanding lurus dengan risiko kejahatan yang kemungkinan dapat terjadi. Pada tahun 2023, tercatat 403.990.813 serangan siber yang terjadi [1] di Indonesia meliputi *Trojan Activity, Information Gathering,* dan *Web Application Attack*. Berdasarkan banyaknya jenis dan kasus serangan siber, serangan pada layanan daring di masyarakat menjadi salah satu kasus yang sering terjadi. Hal ini melibatkan pertukaran informasi pribadi berupa alamat rumah, akun internet *banking* hingga detail kartu kredit, interaksi dengan situs web yang tidak aman [2], pembuatan kata sandi yang lemah [3], dan mengunduh berkas dari *website* yang berbahaya [4]. Menurut Fattah et al. [5] dalam survei yang dilakukan, menyatakan bahwa kesadaran masyarakat dalam kejahatan siber, praktik keamanan siber, serta peran pemerintah dan organisasi dalam memastikan keamanan informasi di internet masih sangat terbatas. Hal serupa didukung dengan pendapat Tan et al [6] yang melakukan survei terhadap mahasiswa, hasil survei menyatakan bahwa responden memiliki kesadaran keamanan siber yang rendah. Rendahnya tingkat literasi keamanan siber ini memperbesar kerentanan terhadap kejahatan siber, seperti pencurian data pribadi dan keuangan, yang berdampak signifikan pada individu dan organisasi.

Salah satu tantangan utama dalam meningkatkan keamanan siber adalah kurangnya pengetahuan masyarakat tentang cara melindungi informasi pribadi. Serangan siber yang menargetkan individu maupun perusahaan seperti *phishing*, *ransomware*, dan *malware* semakin meningkat, hal ini disebabkan karena individu maupun perusahaan tidak cukup memahami risiko keamanan siber. Selain itu, faktor kelalaian dalam menjaga privasi data juga memicu terjadinya kebocoran data yang dapat memberi kerugian, baik secara finansial maupun terhadap reputasi [7]. Edukasi menjadi sangat penting untuk meminimalkan risiko-risiko ini dan memastikan masyarakat terhindar dari serangan berbahaya yang menyebabkan kerugian.

Upaya peningkatan kesadaran publik mengenai keamanan siber menjadi penting. Oleh karena itu, diperlukan sebuah inisiatif berbasis teknologi yang tidak hanya memberikan informasi, tetapi juga mampu meningkatkan keterlibatan aktif masyarakat dalam memahami keamanan siber. Edukasi

berbasis digital menjadi salah satu pendekatan yang efektif [8], dengan mempertimbangkan tingginya penggunaan teknologi informasi di Indonesia. Selain memberikan informasi teoritis, penggunaan aplikasi berbasis web sebagai media edukasi juga memungkinkan pengguna untuk berlatih dan menguji pemahaman mereka melalui simulasi dan tes interaktif [9], [10].

Dengan mengacu pada kerangka global literasi digital dari UNESCO yaitu *A Global Framework of Reference on Digital Literacy Skills for Indicator* 4.4.2 [11], aplikasi yang dikembangkan diharapkan dapat memberikan pemahaman komprehensif mengenai pentingnya keamanan informasi. Adanya *pre-test* dan *post-test/quiz* dalam media edukasi ini juga memungkinkan dilakukannya evaluasi terhadap peningkatan kesadaran dan pemahaman masyarakat terkait keamanan siber [12]. Selain itu, dilakukan juga pengujian reliabilitas untuk menunjukkan bahwa indikator dan pertanyaan dalam aplikasi, memiliki konsistensi yang baik, dan instrumen yang digunakan dalam aplikasi (seperti pertanyaan atau modul) dapat dipercaya untuk mengukur pemahaman atau kesadaran keamanan informasi secara konsisten.

Aplikasi yang dikembangkan diharapkan dapat menjadi potensi efektif sebagai media sosialisasi, yang dapat dilihat dari indikator terhadap kesediaan pengguna untuk menggunakannya dan sesuai dengan kebutuhan terkait kesadaran keamanan informasi. Oleh karena itu, pada penelitian ini juga dilakukan pengujian terhadap penerimaan pengguna (*user acceptance test*) untuk membuktikan hal tersebut.

3. METODE PENELITIAN

Pengembangan aplikasi web edukasi keamanan siber menggunakan metodologi pengembangan *prototyping* yang memiliki beberapa tahap pengembangan meliputi perencanaan, analisis desain sistem dan implementasi.

Perencanaan

Pada tahap *define*, peneliti melakukan studi literatur berdasarkan area kompetensi *safety* pada pedoman *A Global Framework of Reference on Digital Literacy Skills for Indicator* 4.4.2 untuk menentukan turunan kompetensi dan indikator pembelajaran. Pada tahap selanjutnya yaitu *design*, peneliti menyusun instrumen pembelajaran dengan menurunkan indikator pada tahap *define* kedalam bentuk pertanyaan-pertanyaan. Pada tahap *develop*, peneliti melakukan uji validitas dan reliabilitas terhadap pertanyaan yang dihasilkan pada tahap *design*.

Pada uji validitas, peneliti menguji validitas logis dan reliabilitas mengacu pada penelitian Maisari [16]. Uji validitas logis dilakukan pada Kelompok PKIP (Proteksi Keamanan Informasi Publik, Badan Siber dan Sandi Negara) dengan memberikan formulir pengujian yang berisi analisis validitas butir soal. Sedangkan untuk uji reliabilitas, dilakukan dengan memberikan soal yang telah dinyatakan valid pada uji validitas logis terhadap 50 responden, terdiri dari 10 siswa Sekolah Menengah Pertama (SMP), 10 siswa Sekolah Menengah Atas (SMA), dan 30 mahasiswa Politeknik Siber dan Sandi Negara (Poltek SSN). Perhitungan data yang didapat menggunakan rumus Kuder Richardson (KR) [17].

Analisis Desain Sistem

Pada tahap ini, peneliti melakukan analisis kebutuhan dalam proses pengembangan aplikasi media edukasi keamanan siber. Analisis kebutuhan dijelaskan sesuai dengan kebutuhan pada setiap tahap prototipe aplikasi. Terdapat dua jenis kebutuhan yang akan dianalisis, yaitu kebutuhan fungsional dan non-fungsional yang disusun berdasarkan hasil dari wawancara terhadap Kelompok PKIP. PKIP merupakan unit di BSSN yang memiliki tugas salah satunya adalah melaksanakan edukasi keamanan siber [18]. Hasil analisis kemudian dimodelkan menggunakan salah satu diagram *Unified Modeling Language* (UML) yaitu *Use Case Diagram*.

Implementasi dan Pengujian

Pada tahap implementasi, peneliti melakukan pengembangan aplikasi berdasarkan dokumen perancangan yang dilakukan pada tahap-tahap sebelumnya ke dalam bentuk *source code* menggunakan bahasa pemrograman PHP. Perancangan dan pembangunan aplikasi menggunakan Komputer *Notebook* dengan spesifikasi RAM 4 GB dan *harddisk* 1 TB dilengkapi dengan sistem operasi Windows 10 serta aplikasi pengembangan seperti Visual Studio Code, Enterprise Architect, dan XAMPP. Implementasi aplikasi dilakukan dalam dua siklus *prototyping*.
Setelah tahap Implementasi, kemudian dilakukan pengujian *User Acceptance Testing*. *User Acceptance Testing* menggunakan Skala Likert melalui survei dengan penyebaran formulir yang berisi pertanyaan

mengenai aplikasi dan menghasilkan data interval yang kemudian diolah menggunakan perhitungan berikut [19].

$$Perhitungan\ Nilai\ Rata-Rata\ Aplikasi = \frac{\sum(a \times b)}{c \times d} \times 100\% \quad (1)$$

Keterangan :
a : total responden memilih b c : total responden
b : skor pilihan responden d : skor tertinggi

Persamaan di atas digunakan untuk menghitung persentase penerimaan pengguna untuk setiap pertanyaan yang diajukan. Sedangkan untuk menghitung nilai keseluruhan penerimaan pengguna (*user acceptance test*), digunakan persamaan di bawah ini.

$$Perhitungan\ Nilai\ Aplikasi\ Keseluruhan = \frac{\sum x}{y \times c \times d} \times 100\% \quad (2)$$

Keterangan:
x : total skor pilihan responden c : total responden
y : total pertanyaan d : skor tertinggi

4. HASIL DAN PEMBAHASAN

Pada penelitian ini dikembangkan sebuah aplikasi edukasi keamanan siber yang diberi nama KLiKS (Kampanye Literasi Keamanan Siber).

Perencanaan

Konten pada aplikasi KLiKS mengacu pada pedoman *A Global Framework of Reference on Digital Literacy Skills for Indicator* 4.4.2. Masing-masing area kompetensi memiliki cakupan materi yang berbeda, kemudian akan dilakukan studi literatur untuk memahami materi sehingga dapat disusun dalam konten pembelajaran aplikasi edukasi keamanan siber. Berdasarkan hasil dari studi literatur, diklasifikasikan ke dalam bentuk kompetensi dan indikator. Kompetensi disesuaikan dengan penjabaran area kompetensi yang tertera pada pedoman yang digunakan. Indikator disusun berdasarkan taksonomi Bloom pada ranah kognitif, dijelaskan pada Tabel 1.

Tabel 1. Area kompetensi aplikasi KLiKS

No.	Area Kompetensi	Kompetensi	Indikator
1	Melindungi perangkat	Mengetahui risiko dan ancaman di lingkungan digital	Menyebutkan risiko dan ancaman pada lingkungan digital
		Memahami risiko dan ancaman di lingkungan digital	Menjelaskan definisi setiap risiko dan ancaman pada lingkungan digital
		Menerapkan langkah-langkah keselamatan terhadap risiko dan ancaman pada lingkungan digital	Menentukan langkah-langkah keselamatan terhadap risiko dan ancaman pada lingkungan digital
		Memahami langkah-langkah melindungi perangkat	Menjelaskan definisi langkah-langkah dalam melindungi perangkat
2	Melindungi data pribadi dan privasi	Memahami cara melindungi data pribadi dan privasi pada lingkungan digital	*Menjelaskan definisi dari data pribadi dan hal yang berhubungan degan data pada session cookies*
		Menerapkan cara menggunakan dan membagikan informasi pribadi pada lingkungan digital	*Menentukan langkah dalam menggunakan dan membagikan informasi pribadi pada lingkungan digital*
		Memahami bahwa layanan digital menggunakan "Kebijakan privasi" untuk menginformasikan bagaimana data pribadi digunakan	Menjelaskan bagaimana dapat mengubah *privacy option*
3	Melindungi kesehatan dan kesejahteraan	Memahami risiko kesehatan dan ancaman psikologis saat menggunakan teknologi digital (*cyberbullying*)	Menjelaskan definisi *cyberbullying* dan dampaknya
		Mengetahui langkah untuk melindungi diri dari bahaya pada lingkungan digital	Menyebutkan etika berkomunikasi dalam dunia digital
		Menerapkan tindakan terkait adanya *cyberbullying*	Menentukan tindakan terhadap adanya *cyberbullying*
4	Melindungi lingkungan	Memahami dampak lingkungan dari penggunaan teknologi digital	Menjelaskan dampak positif dan negatif dari penggunaan teknologi digital dengan benar
		Menerapkan tindakan pencegahan dari dampak lingkungan yang ditimbulkan dari penggunaan teknologi digital	Menentukan *green computing* dalam berbagai bidang dengan benar

Indikator-indikator pada Tabel 1 kemudian menjadi dasar dalam pembuatan soal-soal pertanyaan pada aplikasi KLiKS sebanyak 20 buah soal. Soal-soal tersebut kemudian dilakukan uji validitas dan reliabilitas. Uji validitas dilakukan dengan cara uji validitas logis dengan menilai tingkat validitas berdasarkan penilaian dari *validator*, dalam hal ini dilakukan oleh perwakilan dari kelompok PKIP sebanyak dua orang. Pengujian validitas logis dilakukan dengan memberikan *form* yang berisi turunan kompetensi ke dalam indikator dan pertanyaan. Hasil uji validitas logis oleh *validator* terlihat pada Tabel 2. Berdasarkan Tabel 2, hasil dari validitas logis menyatakan bahwa terdapat 9 soal dinilai valid dan 11 soal dinilai sangat valid, sehingga indikator dan soal yang diturunkan dapat digunakan.

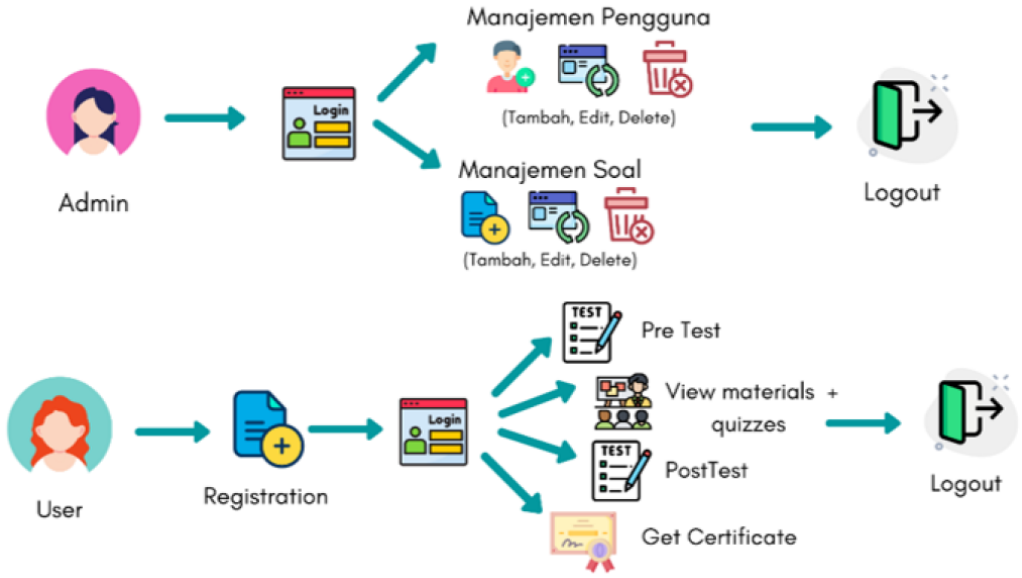
Tabel 2. Hasil validitas logis

Validator	**Jumlah soal**			**Total**
	Sangat valid	**Valid**	**Tidak valid**	
Validator 1	11	9	0	20
Validator 2	11	9	0	20

Setelah diuji validitas secara logis, kemudian dilakukan uji reliabilitas soal yang telah dinyatakan valid terhadap 50 responden. Data pengujian dituangkan ke dalam tabel perhitungan, dengan jawaban benar dituliskan dengan angka 1 dan jawaban salah dituliskan dengan angka 0. Uji reliabilitas yang dilakukan mendapatkan hasil sebesar 0,788, sehingga dinyatakan bahwa soal tersebut sudah reliabel karena sudah lebih dari batas minimal yaitu 0,70.

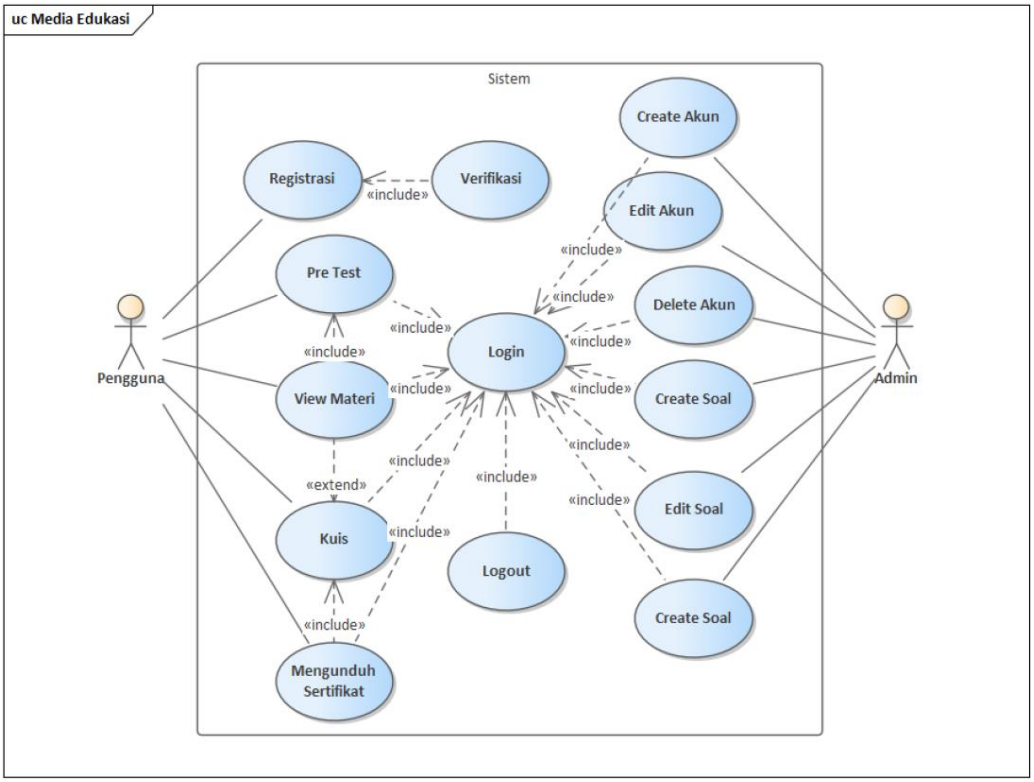
Analisis Desain Sistem

Analisis kebutuhan pengembangan aplikasi didasarkan pada diskusi dan wawancara terhadap Kelompok PKIP. Berdasarkan hasil wawancara, peneliti mendapatkan gambaran umum sistem yang akan dibangun. Sebagaimana terlihat pada Gambar 1, aplikasi KLiKS memiliki beberapa fitur selain menampilkan materi pembelajaran yaitu fitur untuk mengerjakan *pre-test*, *post-test/quiz* dan untuk membuat sertifikat secara otomatis.



Gambar 1. Gambaran umum sistem KLiKS

Gambaran umum sistem kemudian dituangkan ke dalam kebutuhan fungsional dan non-fungsional. Untuk kebutuhan fungsional, rancangan model menggunakan *Use Case Diagram* yang ditunjukkan pada gambar 2. Sedangkan kebutuhan non-fungsional ditunjukkan pada tabel 4.



Gambar 2. Use Case Diagram aplikasi KLiKS

Gambar 2 menunjukkan desain *Use Case Diagram* aplikasi KLiKS. Terdapat dua aktor yaitu Admin dan Pengguna. Admin merupakan aktor yang digunakan oleh karyawan Kelompok PKIP untuk mengelola data pengguna dan data soal. Pengguna merupakan aktor yang digunakan oleh peserta (pengguna) dalam aplikasi. Berdasarkan gambar tersebut, Admin dan Pengguna memiliki peran yang berbeda yang mana dijelaskan bahwa admin dapat melakukan *login* dan *logout*, serta beberapa fungsi

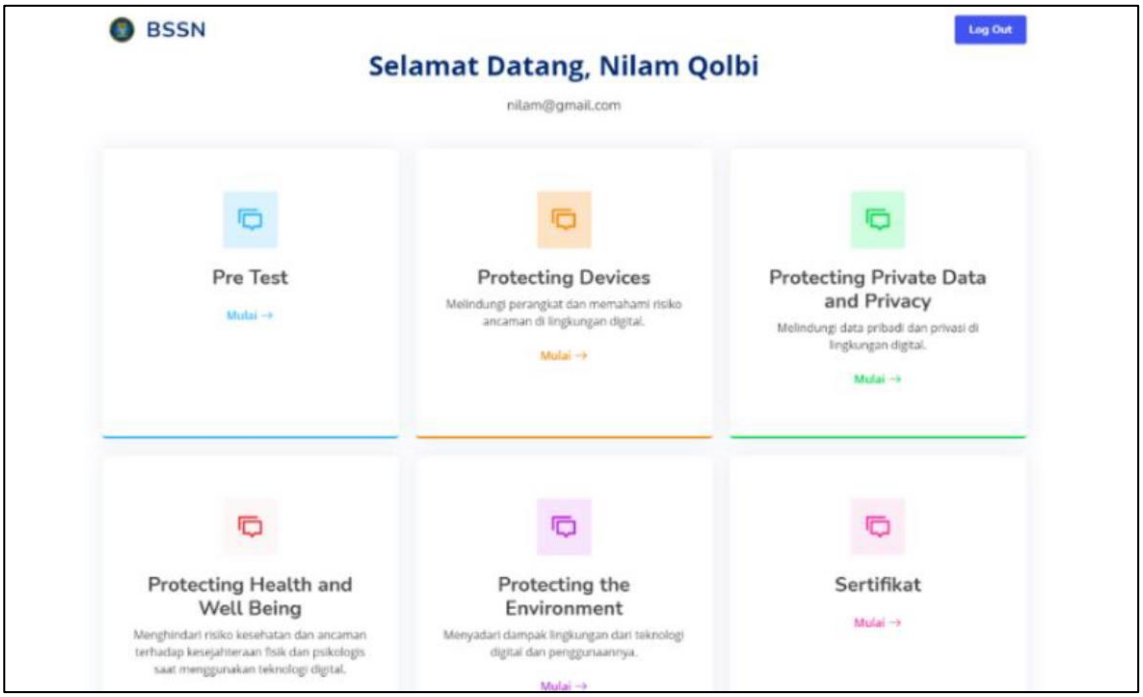
yang dapat dilakukan hanya ketika admin *login* ke dalam aplikasi. Sedangkan Pengguna dapat melakukan registrasi dan *login* serta beberapa fungsi lain yang dapat diakses setelah melaksanakan fungsi sebelumnya.

Tabel 4. Kebutuhan non-fungsional aplikasi KLiKS

NF-ID	Kebutuhan non-fungsional
KN01	Aplikasi dapat berjalan dengan baik minimal pada 3 *web browser* populer
KN02	Aplikasi menyediakan fungsi keamanan menggunakan *password* hash
KN03	Aplikasi menyediakan keamanan dengan mengenkripsi informasi di dalam *database*

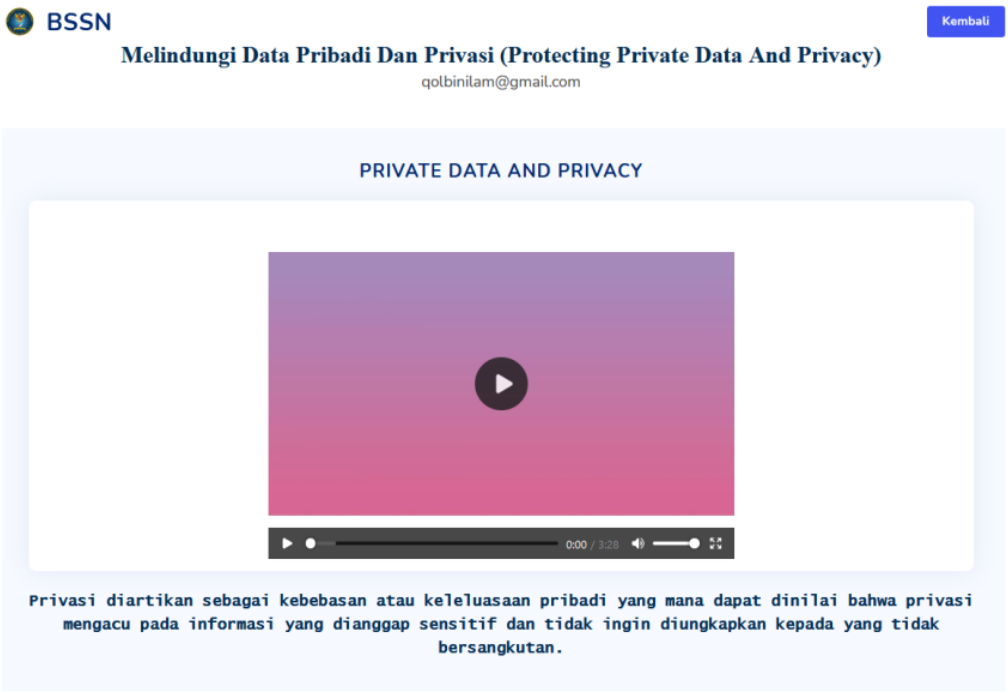
Implementasi dan Pengujian

Tahap implementasi dilakukan dengan pengembangan prototipe media edukasi keamanan siber sesuai dengan rancangan yang telah dimodelkan pada tahap desain dengan menggunakan bahasa pemrograman PHP.



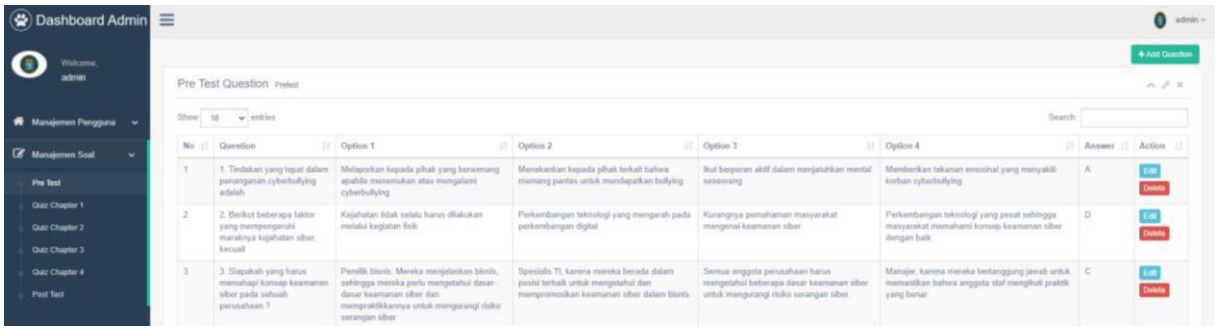
Gambar 3. Halaman utama aplikasi KLiKS

Gambar 3 merupakan halaman utama aplikasi yang menampilkan semua menu aplikasi yang dapat diakses oleh pengguna meliputi *pre-test*, materi, dan akses sertifikat. Halaman ini dapat diakses oleh pengguna hanya jika pengguna telah terdaftar pada aplikasi dan telah ter-autentikasi. Apabila pengguna menekan salah satu menu materi, maka halaman materi akan tampil seperti ditunjukkan pada Gambar 4.



Gambar 4. Halaman salah satu materi

Aplikasi KLiKS terdiri dari dua aktor, salah satunya adalah aktor yang berperan sebagai admin. Admin memiliki hak untuk mengelola akun dan mengelola soal *pre-test* dan *post-test/quiz*. Gambar 5 menunjukkan halaman manajemen soal yang hanya dapat diakses oleh admin.



Gambar 5. Halaman manajemen soal

Setelah sistem selesai diimplementasikan, selanjutnya dilakukan pengujian menggunakan *User Acceptance Testing* (UAT) untuk memberikan penilaian terhadap aplikasi. UAT dilakukan oleh Kelompok PKIP dengan menggunakan *form* daring yang berisi 9 (sembilan) pertanyaan. Penilaian aplikasi dilakukan dengan skala Likert yang menggunakan data interval pada rentang 1 sampai 5. Skala 5 menunjukkan Sangat Setuju (SS), skala 4 Setuju (S), skala 3 Biasa(B), skala 2 Tidak Setuju (TS), dan skala 1 Sangat Tidak Setuju (STS). *Form* penilaian yang diberikan mendapatkan tanggapan 6 responden, dengan persentase untuk masing-masing pertanyaan dihitung berdasarkan persamaan 1.

Tabel 5. Tanggapan *User Acceptance Test*

Responden	P1	P2	P3	P4	P5	P6	P7	P8	P9
R1	5	4	4	5	4	5	4	4	4
R2	4	3	4	4	3	4	4	4	4
R3	4	4	4	5	5	4	4	4	5
R4	4	4	4	3	3	4	4	4	4

R5	5	4	5	4	4	4	4	4	5
R6	4	3	4	3	4	4	4	4	4
Total: 219	26	22	25	24	23	25	24	24	26
Persentase	87%	73%	83%	80%	77%	83%	80%	80%	87%

Tabel 5 menyatakan bahwa total skor penilaian aplikasi oleh Kelompok PKIP adalah 219, selanjutnya dengan menggunakan persamaan 2, dihitung nilai aplikasi secara keseluruhan dengan membagi total skor yang didapat dengan total pertanyaan dikali total responden dan skor tertinggi.

$$Perhitungan\ Nilai\ Aplikasi\ Keseluruhan = \frac{219}{9 \times 6 \times 5} \times 100\% = 81{,}11\%$$

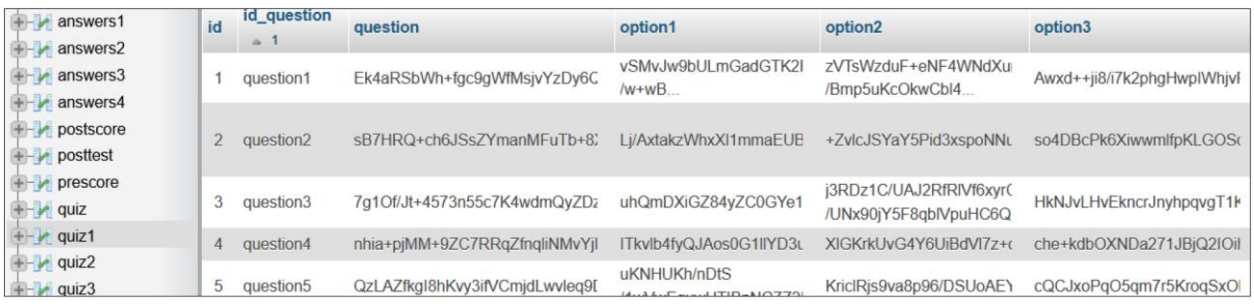
Dari perhitungan menggunakan persamaan 2, didapatkan nilai aplikasi secara keseluruhan adalah 81,11%. Nilai aplikasi secara keseluruhan adalah nilai dari *user acceptance testing* yang menunjukkan bahwa hasil penilaian baik dan sesuai dengan kebutuhan pengguna.

Selain pengujian dengan UAT, pengujian non-fungsional juga dilakukan terhadap aplikasi. Pengujian non-fungsional bertujuan untuk memastikan aplikasi telah memenuhi kebutuhan non-fungsional yang ditetapkan.

Tabel 6. Hasil pengujian non-fungsional

NF-ID	**ID**	***Test Case***	***Expected Result***	***Actual Result***	**Pass/Fail**
KN01	TC01	Aplikasi dapat berjalan baik pada web browser Google Chrome	Berjalan baik	Berjalan baik	Pass
	TC02	Aplikasi dapat berjalan baik pada web browser Mozilla Firefox	Berjalan baik	Berjalan baik	Pass
	TC03	Aplikasi dapat berjalan baik pada web browser Microsoft Edge	Berjalan baik	Berjalan baik	Pass
KN02	TC04	Aplikasi menyediakan fungsi keamanan menggunakan *password hash*	Tersedia	Tersedia	Pass
KN03	TC05	Aplikasi melakukan enkripsi informasi di dalam *database*	Tersedia	Tersedia	Pass

Berdasarkan Tabel 6, diperoleh hasil bahwa aplikasi telah memenuhi kebutuhan non-fungsional antara lain, aplikasi dapat diakses dengan baik melalui 3 web browser yang berbeda, aplikasi menerapkan *password hash* sebagai bentuk keamanan pada *database*, dan aplikasi menyediakan keamanan dengan melakukan enkripsi pada *database*. Enkripsi *database* menggunakan pustaka enkripsi pada *framework* Codeigniter dengan menggunakan *handler* OpenSSL yang mengenkripsi menggunakan algoritma AES-256. Informasi yang dienkripsi berupa soal dan jawaban pada aplikasi, apabila data dilihat dari dalam *database*, ditampilkan dalam bentuk terenkripsi, namun ketika ditampilkan pada halaman *website*, data tersebut dalam bentuk ter-dekripsi. Hasil pengujian ditampilkan pada Gambar 6.



Gambar 6. Record pada database terenkripsi

5. KESIMPULAN DAN SARAN-SARAN

Kesimpulan

Berdasarkan pembahasan pada bab-bab sebelumnya maka dapat diambil kesimpulan sebagai berikut:

1) Instrumen pembelajaran dalam aplikasi disusun dengan menerapkan metode Taksonomi Bloom yang diturunkan dalam bentuk indikator dan pertanyaan. Indikator dan pertanyaan telah diuji validitas dan reliabilitasnya sehingga dinyatakan valid dan reliabel dengan koefisien reliabilitas sebesar 0,788.
2) Pengujian aplikasi menggunakan *User Acceptance Testing* dan *Non-functional Testing*. Hasil dari *User Acceptance Testing* dinyatakan aplikasi yang dikembangkan telah sesuai dengan kebutuhan Kelompok PKIP dengan persentase 81,11%. Hasil *Non-functional testing* menyatakan bahwa aplikasi telah memenuhi kebutuhan non-fungsional yang ditetapkan.

Saran

Penelitian ini hanya berfokus pada penerapan pedoman dari UNESCO (*A Global Framework of Reference on Digital Literacy Skills for Indicator* 4.4.2), penelitian berikutnya dapat dilakukan dengan menerapkan pedoman dari pihak lain seperti NIST Cybersecurity Framework, General Data Protection Regulation (GDPR), atau SANS Security Awareness Training.

6. DAFTAR PUSTAKA

1. BSSN. 2024. *Lanskap Keamanan Siber Indonesia 2023*.
2. Z. Alkhalil, C. Hewage, L. Nawaf, & I. Khan. 2021. Phishing Attacks: A Recent Comprehensive Study & a New Anatomy. *Front. Comput. Sci.*, vol. 3, no. March, page 1–23.
3. K. Lee, S. Sjöberg, and A. Narayanan. 2022. Password policies of most top websites fail to follow best practices. In *Proceedings of the 18th Symposium on Usable Privacy and Security, SOUPS*, no. Soups, page 561–580.
4. N. Samarasinghe, A. Adhikari, M. Mannan, & A. Youssef. 2022. Et tu, Brute? Privacy Analysis of Government Websites and Mobile Apps. Association for Computing Machinery, vol. 1, no. 1.
5. A. Fattah, W. Wagimin, & N. Nurlia. 2023. Enhancing Cybersecurity Awareness among University Students: A Study on the Relationship between Knowledge, Attitude, Behavior, and Training. *JSI J. Sist. Inf.*, vol. 15, no. 1.
6. T. Tan, H. Sama, T. Wibowo, G. Wijaya, & O. E. Aboagye. 2024. Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam Cybersecurity Awareness among University Students in Batam City. *J. Teknol. dan Inf.*, vol. 14, no. September, page 163–173.
7. V. Marcelliana, dkk. 2023. Penerapan Perlindungan Konsumen Terhadap Nasabah PT. Bank Syariah Indonesia Dalam Kasus Kebocoran Data Nasabah. *Depos. J. Publ. Ilmu Huk.*, vol. 1, no. 2, page 180–194.
8. D. Susanti & E. Elmiyati. 2020. Perancangan Website Media Informasi dan Pemesanan pada PT. Trita Musi Prasada dengan Metode RAD. *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 20, no. 1, page 35–46.
9. L. Astuti, Y. Wihardi, & D. Rochintaniawat. 2020. The Development of Web-Based Learning using Interactive Media for Science Learning on Levers in Human Body Topic. *J. Sci. Learn.*, vol. 3, no. 2, page 89–98, 2020
10. S. Maqsood & S. Chiasson. 2021. Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens. in *ACM Conference in Interaction Design and Children*, vol. 24, no. 4.
11. UNESCO Institute for Statistics. 2018. A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2. *UNESCO Inst. Stat.*, no. 51, page 146.
12. T. Wu, K. Y. Tien, W. C. Hsu, & F. H. Wen. Assessing the Effects of Gamification on Enhancing Information Security Awareness Knowledge. *Appl. Sci.*, vol. 11, no. 19.
13. K. P. Nuci, R. Tahir, A. I. Wang, & A. S. Imran. 2021. Game-Based Digital Quiz as a Tool for Improving Students Engagement and Learning in Online Lectures. *IEEE Access*, vol. 9, page 91220–91234.
14. D. Agnia Hardianty, I. Yustiana, & S. Somantri. 2022. Rancang Bangun Aplikasi E-Learning Berbasis Progressive Web Apps Untuk Menunjang Pembelajaran Online dengan Metode Prototyping. *J. Sains Komput. Inform.*, vol. 6, no. 2, page 754–756.
15. A. R. Setiawan. 2019. Penyusunan Program Pembelajaran Biologi Berorientasi Literasi Saintifik. in *Seminar Nasional Sains dan Enterpreneurship VI Tahun 2019*, no. 23, pp. 1–8.
16. L. Maisari, R. Darusyamsu, D. M, & S. Fuadiyah. 2020. Validitas Instrumen Penilaian Kemampuan

Berpikir Tingkat Tinggi tentang Materi Tumbuhan untuk Peserta Didik SMA/MA Kelas X. *Pedagog. Hayati*, vol. 4, no. 1, page 47–54