LAPORAN HASIL PELAKSANAAN MAGANG

IMPLEMENTASI PROTOTYPE KEAMANAN *TWO-FACTOR AUTHENTICATION (2FA)* PADA SISTEM INFORMASI AKADEMIK (STUDI KASUS: UIN SULTAN MAULANA HASANUDDIN BANTEN)

Disusun untuk memenuhi salah satu syarat pelaksanaan Magang
pada Program Studi Informatika

Disusun oleh:
Nama : Bayu Endru Subiyakto
NIM : 231730029

PROGRAM STUDI INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI
SULTAN MAULANA HASANUDDIN BANTEN

2026

HALAMAN PENGESAHAN

Laporan hasil pelaksanaan Magang ini telah disusun oleh:

Nama	:	Bayu Endru Subiyakto
Nim	:	231730029
Program Studi	:	Informatika
Judul Magang	:	Implementasi Prototype Keamanan *Two-Factor Authentication (2FA)* Pada Sistem Informasi Akademik (Studi Kasus:UIN Sultan Maulana Hasanuddin Banten
Tempat Magang	:	Badan Riset Inovasi Nasional – KST BJ. Habibie Serpong
Waktu Pelaksanaan	:	18 Februari 2026 sampai 17 Juli 2026

Laporan ini telah diperiksa dan disahkan sebagai laporan hasil pelaksanaan Magang.

Tangerang, 26 Juni 2026

Dosen Pembimbing Magang,	Pembimbing Lapangan,
	TT ELEKTRONIK
Ahmad Tabrani, M.T.I	Christine Cecylia Munthe S.Kom., M.T.I
NIP.198509172018011002	NIP.199311302019022001

Mengetahui,
Ketua Program Studi Informatika

Ahmad Tabrani, M.T.I
NIP.198509172018011002

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT karena atas rahmat dan karunia-Nya, penulis dapat menyelesaikan laporan hasil pelaksanaan Magang yang berjudul "Implementasi Prototype Keamanan *Two-Factor Authentication (2FA)* pada Sistem Informasi Akademik (Studi Kasus: UIN Sultan Maulana Hasanuddin Banten)" dengan baik.

Laporan ini disusun sebagai salah satu bentuk pertanggungjawaban atas kegiatan Magang yang telah dilaksanakan di Badan Riset Inovasi Nasional – KST BJ. Habibie Serpong. Melalui kegiatan ini, penulis memperoleh pengalaman, pengetahuan, serta pemahaman secara langsung mengenai dunia kerja, khususnya dalam bidang perancangan keamanan sistem yang berorientasi pada pengguna *(usable security)* pada lingkup *Human-Computer Interaction and Visualisation*.

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan bantuan, bimbingan, dan dukungan selama pelaksanaan Magang hingga penyusunan laporan ini, terutama kepada:

1. Ahmad Tabrani, M.T.I. selaku Ketua Program Studi Informatika yang telah memberikan izin dan dukungan dalam pelaksanaan PKL/Magang.
2. Ahmad Tabrani, M.T.I selaku dosen pembimbing PKL/Magang yang telah memberikan bimbingan dan arahan selama pelaksanaan kegiatan.
3. Christine Cecylia Munthe S.Kom., M.T.I selaku pembimbing lapangan yang telah memberikan bimbingan teknis selama kegiatan berlangsung.
4. Badan Riset dan Inovasi Nasional (BRIN), khususnya Kawasan Sains dan Teknologi (KST) B.J. Habibie Serpong, yang telah memberikan kesempatan kepada penulis untuk melaksanakan kegiatan magang serta memperoleh pengalaman dan pengetahuan yang berharga.
5. Dan juga kepada semua pihak yang tidak dapat penulis sebutkan satu-persatu, pada lembaran ini, penulis banyak mengucapkan terima kasih yang sebesar-besarnya. Jazakumullah khairan katsiran.

Penulis menyadari bahwa laporan ini masih memiliki kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan agar laporan ini dapat menjadi lebih baik.

Semoga laporan ini dapat memberikan manfaat bagi pembaca dan pihak-pihak yang membutuhkan.

Tangerang, 26 Juni 2026

Bayu Endru Subiyakto

DAFTAR ISI

RINGKASAN

Magang dilaksanakan di Badan Riset dan Inovasi Nasional (BRIN), KST B.J. Habibie Serpong, pada Kelompok Riset *Human-Computer Interaction and Visualization (KR HCIV)* dibawah Pusat Riset Sains Data dan Informasi (PRSDI). Kegiatan magang ini berfokus pada perancangan dan implementasi prototype keamanan *Two-Factor Authentication (2FA)* pada Sistem Informasi Akademik (SIAKAD), dengan studi kasus SIAKAD UIN Sultan Maulana Hasanuddin Banten.

Permasalahan yang ditemukan adalah mekanisme autentikasi SIAKAD UIN Banten yang masih sederhana, yaitu hanya menggunakan kombinasi NIM dan PIN tanpa adanya lapisan verifikasi tambahan. Kondisi ini membuat akun mahasiswa rentan terhadap pengambilalihan akun *(account takeover)* apabila kredensial bocor atau dapat ditebak, mengingat data akademik seperti nilai, KRS, dan data pribadi mahasiswa tersimpan di dalamnya.

Untuk menjawab permasalahan tersebut, penulis merancang prototype antarmuka 2FA menggunakan Figma yang mengimplementasikan tiga mekanisme verifikasi tambahan, yaitu Email *OTP (One-Time* Password yang dikirim ke email terdaftar), *Google Authenticator* (kode TOTP berbasis aplikasi), dan notifikasi deteksi perangkat *baru (new device detection)* yang meminta verifikasi serta pemilihan durasi sesi setiap kali login terdeteksi dari perangkat berbeda. Perancangan dilakukan secara iteratif melalui tahapan kajian literatur, penyusunan proposal, pembuatan wireframe, dan pengembangan prototype bersama pembimbing.

Setiap lapisan keamanan pada prototype tetap mengikuti prinsip *Human-Computer Interaction*, yaitu *visibility of system status* (status pengiriman kode dan hitung mundur waktu berlaku terlihat jelas), error prevention and recovery (validasi kode *OTP* dan opsi kirim ulang), serta *user control and freedom* (pengguna dapat memilih metode verifikasi dan durasi kepercayaan perangkat). Hasil ini menunjukkan bahwa penambahan lapisan keamanan *2FA* pada SIAKAD dapat dirancang tanpa mengorbankan kenyamanan dan kemudahan penggunaan bagi mahasiswa.

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Kegiatan magang memberikan mahasiswa pengalaman langsung di dunia kerja, sehingga ilmu yang diperoleh selama perkuliahan dapat diterapkan secara nyata. Melalui magang, mahasiswa dapat melihat kondisi kerja yang sesungguhnya, khususnya pada bidang riset dan pengembangan teknologi keamanan informasi.

Penulis melaksanakan magang di Badan Riset dan Inovasi Nasional (BRIN), tepatnya di Kawasan Sains dan Teknologi (KST) B.J. Habibie, Serpong. BRIN merupakan lembaga yang mengelola riset dan inovasi di banyak bidang ilmu pengetahuan dan teknologi [11]. Penulis bergabung dengan Kelompok Riset *Human-Computer Interaction and Visualization* (*KR HCIV)* – Pusat Riset Sains Data dan Informasi, yang mengkaji bagaimana manusia berinteraksi dengan sistem komputer, termasuk pada aspek keamanan sistem informasi.

Sistem Informasi Akademik (SIAKAD) menyimpan data yang sangat penting bagi mahasiswa, seperti penilaian mahasiswa, status pembayaran, dan data pribadi. Akan tetapi, beberapa SIAKAD di perguruan tinggi termasuk UIN SMH Banten masih mengandalkan autentikasi satu faktor *(single-factor authentication),* yaitu kombinasi NIM dan PIN/password saja. Mekanisme ini dinilai rentan, karena password yang pendek dan mudah ditebak menjadi salah satu penyebab utama insiden pengambilalihan akun *(account takeover)* [18]. Apabila kredensial pengguna bocor melalui phishing atau kebocoran data dari layanan lain, penyerang dapat dengan mudah masuk ke akun SIAKAD tanpa adanya lapisan verifikasi tambahan.

Two-Factor Authentication (2FA) merupakan salah satu solusi yang banyak digunakan untuk mengatasi kelemahan autentikasi satu faktor. *2FA* mensyaratkan dua bentuk verifikasi yang berbeda kategori, yaitu sesuatu yang diketahui pengguna (password) dan sesuatu yang dimiliki pengguna (kode *OTP* pada email atau aplikasi authenticator), sehingga akun tetap relatif aman walaupun password telah diketahui pihak lain [22][23]. Namun demikian, penerapan *2FA* yang dirancang tanpa memperhatikan kenyamanan pengguna berisiko menimbulkan resistensi, kebingungan, atau bahkan upaya menghindari mekanisme keamanan tersebut [7][17]. Oleh karena itu, prinsip *Human-Computer Interaction (HCI)* menjadi penting untuk dipertimbangkan agar penambahan *2FA* tetap mudah dipahami dan tidak membebani pengguna [1][2].

Penulis melakukan pengamatan pada SIAKAD UIN SMH Banten dan menemukan bahwa proses login pada sistem tersebut masih hanya menggunakan NIM dan Kode Akses/PIN tanpa adanya lapisan verifikasi tambahan. Kondisi ini menunjukkan kesenjangan antara kebutuhan keamanan data akademik yang makin penting dengan mekanisme autentikasi yang masih sederhana. Berdasarkan kondisi tersebut, penulis merancang dan mengimplementasikan prototype antarmuka keamanan *2FA* untuk SIAKAD UIN SMH Banten, dengan tiga mekanisme verifikasi, yaitu Email OTP, *Google Authenticator*, dan notifikasi deteksi perangkat baru (new device detection), yang seluruhnya dirancang dengan tetap memperhatikan *prinsip visibility of system status*, *error prevention and recovery*, dan *user control and freedom* [1][2][20].

Berdasarkan uraian tersebut, penulis menyusun laporan magang dengan judul "Implementasi Prototype Keamanan *Two-Factor Authentication (2FA)* pada Sistem Informasi Akademik (Studi Kasus: UIN Sultan Maulana Hasanuddin Banten)". Laporan ini menjelaskan proses perancangan prototype, kendala yang dihadapi selama magang, serta pelajaran yang diperoleh penulis selama berada di lingkungan riset BRIN KST B.J. Habibie Serpong.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam laporan magang ini adalah sebagai berikut:

- Apa saja permasalahan yang ditemukan terkait mekanisme keamanan autentikasi pada Sistem Informasi Akademik UIN SMH Banten?
- Bagaimana upaya penyelesaian yang dilakukan untuk merancang dan mengimplementasikan prototype keamanan *Two-Factor Authentication (2FA)* pada SIAKAD yang tetap memperhatikan prinsip Human-Computer Interaction selama pelaksanaan magang?

1.3 Tujuan Magang

1.3.1 Tujuan umum

Tujuan umum pelaksanaan magang adalah untuk memberikan pengalaman kerja secara langsung kepada mahasiswa di lingkungan riset, sehingga mahasiswa dapat memahami penerapan ilmu pengetahuan yang dipelajari selama perkuliahan dalam kegiatan riset dan pengembangan teknologi keamanan informasi yang sesungguhnya.

1.3.2 Tujuan khusus

- Mengetahui proses kerja dan lingkungan riset di Badan Riset dan Inovasi Nasional (BRIN), khususnya pada kelompok riset *Human-Computer Interaction.*
- Mengidentifikasi permasalahan terkait mekanisme keamanan autentikasi pada sistem informasi akademik, khususnya pada studi kasus SIAKAD UIN SMH Banten.
- Menganalisis mekanisme *Two-Factor Authentication (2FA)* yang sesuai untuk diterapkan pada SIAKAD tanpa membebani pengguna.
- Merancang dan mengimplementasikan prototype antarmuka keamanan *2FA* pada SIAKAD, meliputi Email *OTP*, *Google Authenticator*, dan deteksi perangkat baru.
- Menyusun laporan hasil pelaksanaan magang secara sistematis sebagai bentuk pertanggungjawaban atas kegiatan yang telah dilaksanakan selama magang di BRIN.

1.4 Manfaat Magang

1.4.1 Manfaat teoritis

Laporan magang ini diharapkan dapat menjadi referensi dan sumber informasi bagi mahasiswa maupun pihak lain yang ingin mempelajari penerapan *Two-Factor Authentication* pada sistem informasi akademik dengan pendekatan *Human-Computer Interaction*. Selain itu, laporan ini juga diharapkan dapat menambah wawasan mengenai bagaimana mekanisme keamanan berlapis dapat dirancang agar tetap mudah digunakan, sehingga dapat memberikan kontribusi terhadap pengembangan ilmu pengetahuan di bidang interaksi manusia dan komputer serta keamanan sistem informasi.

1.4.2 Manfaat praktis

Bagi Mahasiswa, kegiatan magang ini memberikan pengalaman nyata dalam dunia riset, khususnya dalam merancang prototype mekanisme *2FA* berbasis prinsip *HCI*. Penulis juga mendapatkan kesempatan untuk mendalami isu keamanan autentikasi sistem informasi

akademik secara langsung, sehingga dapat meningkatkan kemampuan analisis, perancangan desain, serta penulisan karya ilmiah.

Bagi Instansi, hasil rancangan dan prototype *2FA* yang dikembangkan selama magang ini diharapkan dapat menjadi salah satu referensi bagi BRIN, khususnya kelompok riset *Human-Computer Interaction*, dalam mengembangkan studi lanjutan terkait integrasi mekanisme autentikasi berlapis dengan *usability* pada sistem informasi, khususnya di lingkungan akademik.

Bagi Kampus, laporan ini dapat menjadi referensi bagi kampus mengenai pentingnya penambahan mekanisme *2FA* pada SIAKAD yang digunakan, khususnya dari sudut pandang pengalaman pengguna. Selain itu, hasil magang ini juga dapat menjadi bahan pertimbangan bagi kampus dalam menyesuaikan kurikulum agar lebih relevan dengan kebutuhan riset di bidang keamanan sistem dan interaksi manusia-komputer.

BAB II
KAJIAN PUSTAKA

2.1 Kajian Pustaka

2.1.1 Pengertian Human-Computer Interaction

Human-Computer Interaction (HCI) mempelajari bagaimana manusia berinteraksi dengan sistem komputer, dengan tujuan menghasilkan sistem yang dipakai secara efektif, efisien, dan nyaman oleh pengguna [1][20]. Nielsen mengajukan sepuluh prinsip *usability heuristic* yang menjadi dasar penilaian dan perancangan antarmuka pengguna [1][2]. Di antara sepuluh prinsip tersebut, tiga yang paling relevan dengan perancangan mekanisme keamanan adalah *visibility of system* status, error *prevention and recovery*, dan *user control and freedom.*

Visibility of system status berarti sistem harus selalu memberikan informasi yang jelas mengenai apa yang sedang terjadi, misalnya status pengiriman kode *OTP* atau sisa waktu kode tersebut berlaku. Error prevention and *recovery* berarti sistem mencegah kesalahan pengguna sebelum terjadi, serta memberikan jalan keluar yang mudah apabila kesalahan tetap terjadi, misalnya validasi format kode *OTP* dan opsi kirim ulang kode. *User control and freedom* berarti sistem memberi kebebasan kepada pengguna untuk mengatur tindakan mereka sendiri, misalnya memilih metode verifikasi yang diinginkan atau menentukan durasi kepercayaan terhadap suatu perangkat [1][2].

Sistem informasi akademik perlu menerapkan prinsip *HCI* karena pengguna SIAKAD berasal dari latar belakang dan tingkat literasi teknologi yang berbeda-beda. Perbedaan ini mengharuskan perancang antarmuka menjaga tampilan tetap sederhana dan mudah dipahami, meskipun ditambahkan fitur keamanan baru seperti *2FA* [4][13].

2.1.2 Konsep Keamanan Sistem dan Two-Factor Authentication (2FA)

Keamanan sistem informasi bertujuan melindungi data dan informasi dari ancaman seperti akses tidak sah, kebocoran data, dan serangan siber [6]. Salah satu mekanisme keamanan yang paling umum digunakan untuk mencegah akses tidak sah adalah Multi-*Factor Authentication (MFA)*, dengan *Two-Factor Authentication (2FA)* sebagai bentuk yang paling banyak diterapkan [22][23]. 2FA mensyaratkan kombinasi dua faktor verifikasi yang berbeda kategori, yaitu sesuatu yang diketahui pengguna (*knowledge factor*, misalnya password atau PIN) dan sesuatu yang dimiliki pengguna *(possession factor*, misalnya kode *OTP* pada email atau kode dari aplikasi *authenticator)* [22].

Terdapat beberapa metode implementasi *2FA* yang umum digunakan, di antaranya *One-Time Password (OTP)* berbasis email atau SMS, dan *Time-based One-Time Password (TOTP)* yang dihasilkan oleh aplikasi authenticator seperti *Google Authenticator* [22][23]. *TOTP* dinilai lebih aman dibandingkan *OTP* berbasis *SMS* karena tidak rentan terhadap serangan *SIM swapping*, sementara *OTP* berbasis email lebih mudah diakses oleh pengguna yang belum familiar dengan aplikasi authenticator [22]. Selain *OTP* dan *TOTP,* mekanisme deteksi perangkat baru *(new device detection)* juga banyak diterapkan sebagai lapisan tambahan, di mana sistem akan meminta verifikasi ulang dan menampilkan informasi perangkat (browser, sistem operasi, lokasi, dan alamat IP) setiap kali login terdeteksi dari perangkat yang belum dikenali [7][8].

Studi mengenai kebiasaan penggunaan password pada skala besar menunjukkan bahwa pengguna cenderung memilih password yang pendek dan mudah ditebak, sehingga mekanisme autentikasi yang hanya mengandalkan password atau PIN dinilai rentan terhadap ancaman keamanan seperti credential stuffing dan brute force [18]. Penambahan *2FA* secara signifikan mengurangi risiko tersebut, karena penyerang memerlukan akses ke faktor kedua yang umumnya tidak dapat diperoleh hanya dari kebocoran password [22][23].

Di sisi lain, penerapan keamanan yang terlalu rumit tanpa memperhatikan pengalaman pengguna dapat menyebabkan resistensi, di mana pengguna merasa terbebani

atau bahkan mencari cara untuk menghindari mekanisme keamanan tersebut [7][17]. Konsep *usable security* muncul untuk menjembatani kebutuhan keamanan dengan kemudahan penggunaan, sehingga pengguna tetap dapat menjalankan mekanisme keamanan tanpa mengalami kesulitan berarti [6][14]. Tingkat kemudahan pakai suatu sistem umumnya diukur menggunakan instrumen seperti *System Usability Scale (SUS)*, yang telah banyak digunakan dalam penelitian HCI [5].

2.1.3 Penelitian atau Referensi Terkait

Berikut adalah beberapa penelitian dan referensi yang relevan dengan topik laporan magang ini. Pertama, penelitian mengenai survei *Multi-Factor Authentication* menunjukkan bahwa terdapat berbagai metode *2FA* dengan tingkat keamanan dan kemudahan penggunaan yang berbeda-beda, mulai dari *OTP* berbasis SMS/email hingga *TOTP* dan metode berbasis biometrik [22][23]. Penelitian ini menjadi dasar bagi penulis dalam menentukan kombinasi metode *2FA* yang sesuai untuk diterapkan pada SIAKAD.

Kedua, audit keamanan sistem informasi akademik pada umumnya memakai standar seperti ISO 27002 dan berfokus pada *vulnerability assessment* secara teknis, namun belum banyak meneliti bagaimana pengguna merasakan interaksi dengan mekanisme keamanan tersebut [9]. Kajian mengenai sistem autentikasi selama lebih dari satu dekade juga menunjukkan bahwa desain mekanisme login yang tidak memperhatikan pengguna cenderung ditinggalkan atau disiasati oleh pengguna itu sendiri [16].

Ketiga, penelitian usability pada sistem akademik biasanya menilai kemudahan navigasi dan efektivitas antarmuka secara umum, namun belum banyak membahas keamanan modern seperti *2FA* secara mendalam [4][15]. Penelitian human-centric security and privacy menekankan pentingnya merancang mekanisme keamanan yang berpusat pada manusia, agar adopsi mekanisme keamanan oleh pengguna dapat lebih tinggi [24].

Dari beberapa kelompok penelitian tersebut, penulis menemukan celah penelitian, yaitu belum banyak studi yang secara khusus memadukan perancangan *2FA* dengan prinsip HCI dalam satu prototipe antarmuka pada studi kasus SIAKAD di perguruan tinggi Indonesia. Celah penelitian inilah yang menjadi dasar bagi pekerjaan magang penulis.

2.2 Kerangka Pikir Teoritis

Kerangka pikir laporan ini dibangun atas dasar teori *Human-Computer Interaction* yang dipadukan dengan konsep *Two-Factor Authentication*. Kerangka pikir ini berawal dari kondisi nyata di lapangan, yaitu proses login SIAKAD UIN SMH Banten yang masih hanya menggunakan NIM dan Kode Akses/PIN tanpa adanya lapisan verifikasi tambahan, sehingga sistem berpotensi rentan terhadap pengambilalihan akun apabila kredensial pengguna bocor [8][18].

Kondisi tersebut dikaitkan dengan dua landasan teori utama. Pertama, teori *Human-Computer Interaction* menekankan prinsip *visibility of system* status, *error prevention and recovery,* dan *user control and freedom* dalam perancangan antarmuka [1][2]. Kedua, konsep *Two-Factor Authentication* menekankan pentingnya kombinasi dua faktor verifikasi yang berbeda kategori untuk meningkatkan keamanan akun [22][23]. Kedua landasan ini menjadi dasar bagi penulis dalam merancang solusi yang mengatasi kesenjangan antara kebutuhan keamanan dan kenyamanan pengguna pada SIAKAD.

Berdasarkan kerangka pikir tersebut, penulis merancang prototype antarmuka keamanan SIAKAD yang terdiri atas tiga mekanisme *2FA*, yaitu Email OTP, *Google Authenticator*, dan notifikasi deteksi perangkat baru. Data dikumpulkan melalui studi literatur mengenai prinsip *HCI* dan *2FA* [5][22], diskusi dengan pembimbing riset di BRIN, serta pengamatan langsung terhadap proses login SIAKAD UIN SMH Banten. Data tersebut kemudian dianalisis secara deskriptif untuk menghasilkan prototipe antarmuka *2FA* yang tetap aman sekaligus nyaman digunakan oleh mahasiswa [12].

BAB III
METODE MAGANG

3.1 Lokasi Magang

Magang dilaksanakan di Badan Riset dan Inovasi Nasional (BRIN), tepatnya di Kawasan Sains dan Teknologi (KST) B.J. Habibie, Serpong, Tangerang Selatan, Banten. BRIN merupakan lembaga pemerintah non-kementerian yang bertugas menyelenggarakan riset dan inovasi di berbagai bidang ilmu pengetahuan dan teknologi di Indonesia.

Penulis ditempatkan pada Pusat Riset Sains Data dan Informasi (PRSDI), khususnya pada Kelompok Riset *Human-Computer Interaction and Visualization (KR HCIV).* Kelompok riset ini berfokus pada kajian interaksi manusia dengan sistem komputer, termasuk perancangan antarmuka, *evaluasi usability*, serta keamanan sistem yang berpusat

pada pengguna. Selain mengikuti kegiatan pada KR HCIV, penulis juga turut serta dalam pertemuan pekanan bersama kelompok riset lain di bawah PRSDI, seperti KR NLP, KR DG, KR IR, dan KR KDE sebagai bagian dari kegiatan diskusi lintas kelompok riset. Pelaksanaan magang berlangsung selama kurang lebih empat bulan, dimulai dari bulan Februari hingga bulan Juli tahun 2026.

3.2 Desain Pelaksanaan Magang

Magang ini menggunakan pendekatan deskriptif dengan rancangan kegiatan yang berbasis riset dan perancangan desain (*design-based research)* [12]. Pendekatan ini dipilih karena kegiatan magang tidak hanya mengamati kondisi yang ada, tetapi juga menyusun rancangan dan membuat prototype nyata sebagai solusi atas masalah yang ditemukan [19].

Selama magang, penulis menjalani tiap tahapan kegiatan, mulai dari membaca literatur mengenai prinsip *Human-Computer Interaction* dan konsep *Two-Factor Authentication* [1][5][22], menyiapkan proposal penelitian, membuat *wireframe* dan prototipe antarmuka *2FA* dengan *Figma*, hingga memperbaiki desain berdasarkan masukan pembimbing. Penulis juga mengikuti bimbingan mingguan bersama dosen pembimbing kampus, menyajikan presentasi perkembangan penelitian, serta menyiapkan *weekly report* untuk melaporkan progres kegiatan secara berkala. Pendekatan ini dipilih karena sesuai untuk penelitian *HCI* yang memakai proses iteratif, mencakup perancangan desain, evaluasi, dan revisi [1][2][19].

3.3 Penentuan Objek Magang

Fokus magang ini adalah merancang dan mengimplementasikan prototipe antarmuka keamanan *Two-Factor Authentication (2FA)* untuk Sistem Informasi Akademik (SIAKAD), dengan studi kasus SIAKAD UIN SMH Banten. Studi kasus ini dipilih karena SIAKAD UIN SMH Banten masih menggunakan autentikasi satu faktor, yaitu NIM dan Kode Akses/PIN, tanpa adanya lapisan verifikasi tambahan, sehingga cocok dijadikan studi kasus untuk penelitian implementasi 2FA berbasis prinsip *HCI* [8][18].

Desain objek magang ini berfokus pada empat komponen utama prototype. Komponen pertama adalah halaman login yang meminta NIM dan Kode Akses/PIN, dilengkapi opsi untuk langsung login menggunakan Google Authenticator. Komponen kedua adalah verifikasi dua langkah *(2FA)* yang menyediakan dua metode, yaitu Email *OTP* berupa kode

enam digit yang dikirim ke email terdaftar dengan batas waktu dua menit, dan *Google Authenticator* berupa kode *TOTP* enam digit yang berubah otomatis setiap 30 detik. Komponen ketiga adalah notifikasi deteksi perangkat baru, yang menampilkan informasi browser, sistem operasi, lokasi, alamat IP, dan waktu login, serta meminta pengguna memilih durasi kepercayaan terhadap perangkat tersebut (1 jam atau 24 jam). Komponen keempat adalah mekanisme keamanan tambahan berupa kemampuan menolak perangkat yang tidak dikenali. Setiap komponen dirancang dengan tetap menerapkan prinsip *visibility of system status, error prevention and recovery*, dan *user control and freedom* [1][2][20], sehingga peningkatan keamanan tetap memperhatikan kenyamanan mahasiswa sebagai pengguna utama SIAKAD [5][14].

3.4 Metode Pengumpulan Data

Berikut adalah metode pengumpulan data yang digunakan selama pelaksanaan magang.

Observasi

Penulis mengamati langsung proses login dan mekanisme keamanan pada SIAKAD UIN SMH Banten, mulai dari tahap input NIM dan Kode Akses/PIN hingga ditemukannya fakta bahwa belum ada lapisan verifikasi tambahan pada sistem tersebut [8][18]. Penulis juga mengamati kegiatan riset di BRIN, terutama pada Kelompok Riset Human-Computer Interaction and Visualization, untuk memahami cara kerja dan budaya riset yang berlaku.

Wawancara

Wawancara dilakukan secara rutin melalui diskusi dan bimbingan dengan dosen pembimbing kampus serta pembimbing lapangan di BRIN. Penulis menerima arahan mengenai metode dan pendekatan penelitian, masukan untuk proposal yang disusun, serta evaluasi terhadap rancangan prototype *2FA* yang dikembangkan selama proses perancangan [12].

Dokumentasi

Penulis melakukan dokumentasi dengan mengumpulkan data berupa hasil kajian literatur, dokumen proposal penelitian, desain *wireframe* dan prototype *2FA* di *Figma*, *weekly report* kegiatan magang, serta foto-foto kegiatan di lingkungan BRIN, termasuk apel pagi, forum diskusi ilmiah, dan pertemuan pekanan kelompok riset [11].

Penelitian ini memilih ketiga metode tersebut karena bersifat deskriptif dan berbasis perancangan desain. Data utama dikumpulkan melalui pengamatan langsung, diskusi dengan pembimbing, dan dokumentasi proses perancangan, bukan melalui pengumpulan data kuantitatif [12].

3.5 Instrumen Magang

Selama pelaksanaan magang, beberapa alat dan bahan yang digunakan antara lain:

- Laptop, digunakan sebagai alat utama dalam melakukan studi literatur, menyusun proposal penelitian, serta merancang *wireframe* dan prototype antarmuka *2FA.*
- Figma, digunakan sebagai aplikasi utama dalam merancang wireframe dan prototype keamanan SIAKAD, mulai dari tampilan login, deteksi perangkat baru, hingga verifikasi dua langkah berupa Email *OTP* dan *Google Authenticator.*
- Buku dan jurnal referensi, digunakan sebagai bahan kajian literatur terkait prinsip Human-Computer Interaction, *Two-Factor Authentication, usable security*, serta metode *evaluasi usability seperti Cognitive Walkthrough dan System Usability Scale* [3][4][5][14][20].
- Buku catatan, digunakan untuk mencatat hasil diskusi dan arahan dari pembimbing selama bimbingan mingguan maupun forum diskusi kelompok riset.
- Aplikasi pesan dan email, digunakan sebagai media komunikasi dengan pembimbing kampus maupun pembimbing di BRIN terkait perkembangan penelitian.

3.6 Teknik Analisis Data

Analisis data dalam magang ini menggunakan pendekatan deskriptif kualitatif. Data hasil observasi terhadap mekanisme login SIAKAD UIN SMH Banten, hasil kajian literatur mengenai prinsip *HCI* dan metode *2FA*, serta masukan dari pembimbing selama bimbingan mingguan dikumpulkan dan dianalisis secara naratif untuk merumuskan kebutuhan rancangan prototype [12][13].

Tahapan analisis dimulai dengan mengidentifikasi kelemahan mekanisme autentikasi SIAKAD yang ada saat ini, kemudian membandingkannya dengan metode *2FA* yang tersedia di literatur, seperti Email *OTP, TOTP* berbasis aplikasi *authenticator*, dan deteksi perangkat baru [22][23]. Hasil perbandingan tersebut digunakan untuk menentukan

kombinasi metode *2FA* yang paling sesuai untuk diterapkan pada SIAKAD, dengan tetap memperhatikan prinsip *HCI* agar rancangan tidak membebani pengguna [1][2]. Setiap rancangan kemudian didiskusikan dan direvisi secara iteratif bersama pembimbing hingga menghasilkan prototype akhir yang dianggap sesuai dengan kebutuhan penelitian [19].

BAB IV
HASIL DAN PEMBAHASAN

4.1 Gambaran Umum Lokasi Magang

Badan Riset dan Inovasi Nasional (BRIN), khususnya di Kawasan Sains dan Teknologi (KST) B.J. Habibie Serpong, merupakan lembaga riset yang menaungi berbagai pusat riset di bidang sains dan teknologi. Penulis ditempatkan pada Pusat Riset Sains Data dan Informasi (PRSDI), tepatnya pada Kelompok Riset *Human-Computer Interaction and Visualization (KR HCIV).* Kelompok riset ini secara rutin mengadakan pertemuan pekanan untuk membahas perkembangan riset masing-masing anggota, termasuk riset yang dilakukan oleh peserta magang.

Selama magang, penulis mengikuti rangkaian kegiatan rutin seperti apel pagi, forum diskusi ilmiah lintas kelompok riset, dan bimbingan mingguan bersama pembimbing lapangan. Lingkungan kerja di BRIN bersifat kolaboratif, di mana peserta magang didorong untuk aktif berdiskusi dan menyampaikan perkembangan penelitian dalam forum kelompok riset.

4.2 Analisis Permasalahan Autentikasi pada SIAKAD

Pengamatan terhadap SIAKAD UIN Sultan Maulana Hasanuddin Banten menunjukkan bahwa proses login hanya mensyaratkan dua data, yaitu NIM dan Kode Akses/PIN, tanpa adanya lapisan verifikasi tambahan apa pun. Kondisi ini sejalan dengan temuan bahwa banyak SIAKAD di perguruan tinggi Indonesia masih bergantung pada autentikasi satu faktor, sehingga rentan terhadap pengambilalihan akun apabila kredensial pengguna bocor melalui phishing atau kebocoran data layanan lain [18].

Berdasarkan kajian pustaka pada Bab II, terdapat tiga risiko utama yang dapat timbul dari mekanisme autentikasi satu faktor pada SIAKAD, yaitu: (1) akun dapat diakses pihak lain apabila Kode Akses/PIN diketahui atau ditebak, mengingat banyak pengguna memakai kombinasi angka yang sederhana dan mudah ditebak [18]; (2) tidak ada mekanisme yang

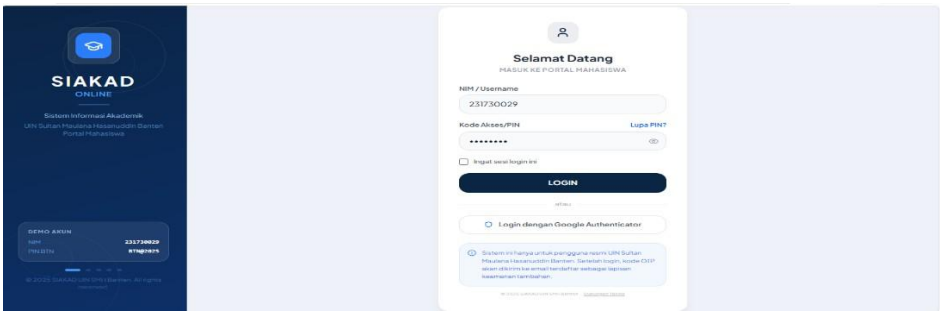
memberi tahu pemilik akun apabila terjadi login dari perangkat atau lokasi yang tidak biasa [7][8]; dan (3) tidak ada lapisan verifikasi kedua yang dapat menghambat penyerang meskipun PIN telah diketahui [22][23]. Ketiga risiko tersebut menjadi dasar bagi penulis dalam merancang prototype 2FA yang akan dijelaskan pada subbab berikutnya.

4.3 Perancangan Prototype Keamanan 2FA

Berdasarkan analisis permasalahan tersebut, penulis merancang prototype antarmuka keamanan *2FA* untuk SIAKAD menggunakan Figma. Perancangan dilakukan secara iteratif, dimulai dari *wireframe* sederhana, kemudian dikembangkan menjadi prototype interaktif dengan tetap menerapkan prinsip *Human-Computer Interaction* yang dijelaskan pada Bab II, yaitu *visibility of system status*, *error prevention and recovery*, dan user control and freedom [1][2][20]. Terdapat empat tampilan utama yang dihasilkan dari proses perancangan ini, yaitu halaman login, verifikasi *Google Authenticator*, verifikasi Email *OTP*, dan notifikasi deteksi perangkat baru.

4.3.1 Halaman Login SIAKAD

Halaman login dirancang sesederhana mungkin agar tidak membingungkan pengguna, sekaligus tetap mengarahkan pengguna pada opsi keamanan tambahan. Pengguna memasukkan NIM/Username dan Kode Akses/PIN seperti pada mekanisme yang sudah ada, namun ditambahkan opsi "Login dengan *Google Authenticator*" sebagai alternatif metode masuk yang lebih cepat bagi pengguna yang telah mengaktifkan *TOTP*. Penambahan informasi keamanan pada bagian bawah formulir, yang menjelaskan bahwa kode *OTP* akan dikirim ke email terdaftar sebagai lapisan keamanan tambahan, merupakan penerapan prinsip visibility of system status, sehingga pengguna mengetahui sejak awal bahwa proses login akan melalui verifikasi tambahan.



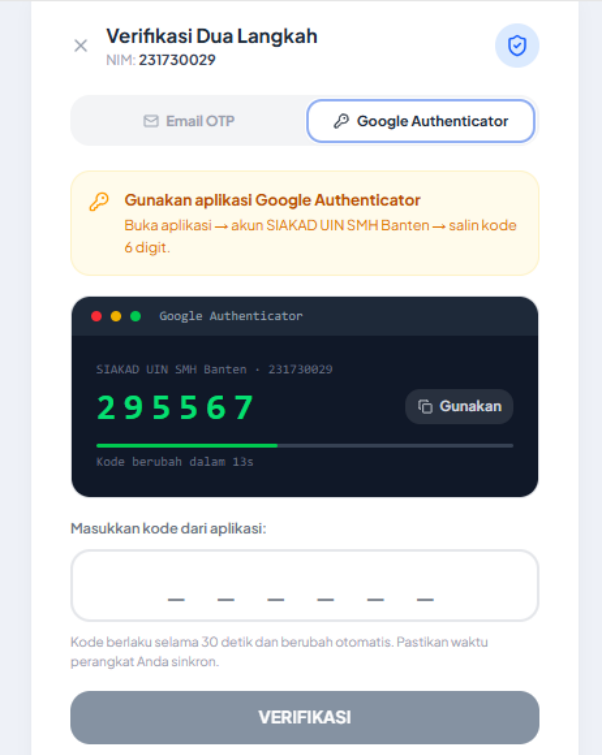
Gambar 4.1 Prototype Halaman Login SIAKAD UIN SMH Banten

Sumber: Hasil perancangan penulis menggunakan Figma (2026)

4.3.2 Verifikasi Dua Langkah Menggunakan Google Authenticator

Metode verifikasi pertama yang dirancang adalah penggunaan aplikasi *Google Authenticator*. Setelah pengguna berhasil memasukkan NIM dan Kode Akses/PIN, sistem menampilkan halaman verifikasi dua langkah dengan dua pilihan tab, yaitu Email *OTP* dan *Google Authenticator*. Pada tab *Google Authenticator*, terdapat petunjuk singkat mengenai cara memperoleh kode (membuka aplikasi, memilih akun SIAKAD UIN SMH Banten, lalu menyalin kode enam digit yang ditampilkan), serta simulasi tampilan aplikasi authenticator yang menunjukkan kode *TOTP* beserta indikator waktu berupa progress bar yang menghitung mundur sebelum kode berubah.

Rancangan ini menerapkan prinsip *visibility of system* status melalui indikator waktu yang jelas ("Kode berubah dalam 13s"), sehingga pengguna mengetahui sisa waktu sebelum harus menyalin kode yang baru. Tombol "Gunakan" pada pojok kanan kode juga mempermudah pengguna untuk langsung menyalin kode ke kolom input tanpa perlu mengetik manual, sejalan dengan prinsip error prevention, karena mengetik manual berisiko menimbulkan kesalahan input.



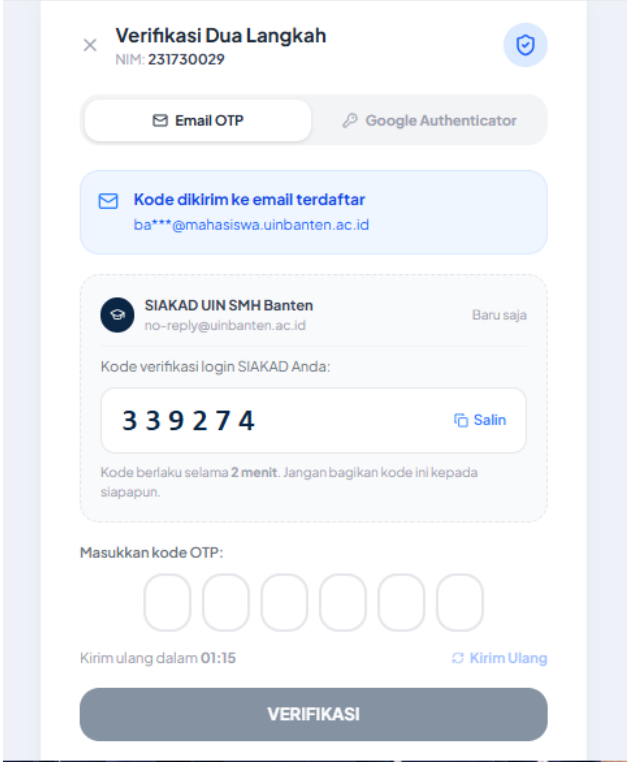
Gambar 4.2 Prototype Verifikasi Dua Langkah Menggunakan Google Authenticator

Sumber: Hasil perancangan penulis menggunakan Figma (2026)

4.3.3 Verifikasi Dua Langkah Menggunakan Email OTP

Metode verifikasi kedua adalah Email *OTP*, yang ditujukan bagi pengguna yang belum mengaktifkan aplikasi authenticator. Pada tab ini, sistem menampilkan informasi bahwa kode verifikasi telah dikirim ke alamat email terdaftar, dengan sebagian alamat email disamarkan demi menjaga privasi pengguna. Tampilan ini juga menyertakan simulasi notifikasi email yang menunjukkan kode *OTP* enam digit beserta keterangan masa berlaku kode selama dua menit, lengkap dengan peringatan agar kode tidak dibagikan kepada siapa pun.

Di bagian bawah, terdapat enam kotak input terpisah untuk memasukkan kode *OTP*, penghitung mundur waktu kirim ulang (“Kirim ulang dalam 01:15”), serta tautan “Kirim Ulang” yang aktif kembali setelah hitungan mundur berakhir. Rancangan ini menerapkan prinsip *error prevention and recovery*, karena pengguna diberikan jalan keluar yang jelas apabila kode tidak diterima atau telah kedaluwarsa, tanpa harus mengulang seluruh proses login dari awal.



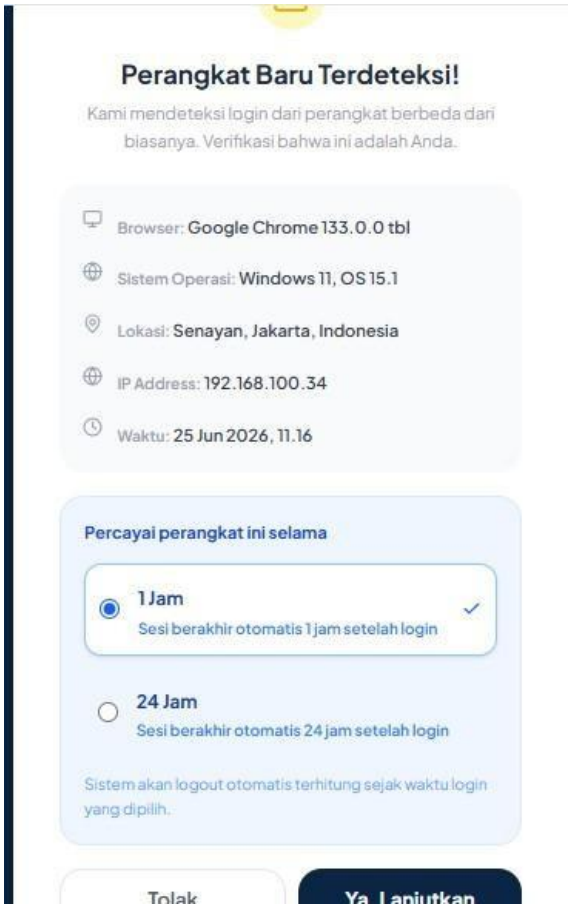
Gambar 4.3 Prototype Verifikasi Dua Langkah Menggunakan Email *OTP*

Sumber: Hasil perancangan penulis menggunakan Figma (2026)

4.3.4 Notifikasi Deteksi Perangkat Baru

Komponen keamanan tambahan yang dirancang adalah notifikasi deteksi perangkat baru *(new device detection)*, yang akan muncul setiap kali sistem mendeteksi proses login dari perangkat yang berbeda dari biasanya. Notifikasi ini menampilkan rincian informasi perangkat secara transparan, meliputi jenis browser, sistem operasi, lokasi, alamat IP, dan waktu login, sehingga pengguna dapat menilai sendiri apakah aktivitas login tersebut benar dilakukan oleh dirinya atau tidak.

Pengguna kemudian diminta menentukan tingkat kepercayaan terhadap perangkat tersebut, dengan dua pilihan durasi, yaitu satu jam atau dua puluh empat jam, sebelum sesi login otomatis berakhir dan meminta verifikasi ulang. Pada bagian bawah, tersedia dua tombol aksi, yaitu "Tolak" bagi pengguna yang tidak mengenali aktivitas login tersebut, dan "Ya, Lanjutkan" bagi pengguna yang mengonfirmasi bahwa perangkat tersebut benar miliknya. Rancangan ini secara langsung menerapkan prinsip *user control and freedom*, karena pengguna diberi kendali penuh untuk menerima atau menolak akses dari perangkat baru, sekaligus mengatur sendiri durasi kepercayaan sesuai kebutuhan dan tingkat kenyamanannya.



Gambar 4.4 Prototype Notifikasi Deteksi Perangkat Baru

Sumber: Hasil perancangan penulis menggunakan Figma (2026)

4.4 Pembahasan Hasil Rancangan

Keempat tampilan prototype yang dirancang menunjukkan bahwa penambahan mekanisme *2FA* pada SIAKAD dapat dilakukan tanpa harus mengorbankan kemudahan penggunaan. Penyediaan dua pilihan metode verifikasi, yaitu Email OTP dan *Google Authenticator*, memberikan fleksibilitas bagi pengguna dengan tingkat literasi teknologi yang berbeda-beda, sejalan dengan prinsip *user control and freedom* yang dijelaskan pada kajian pustaka [1][2]. Pengguna yang sudah familiar dengan aplikasi authenticator dapat memilih metode *TOTP* yang lebih cepat, sementara pengguna yang belum terbiasa dapat tetap mengandalkan metode Email OTP yang lebih familiar [22].

Penerapan indikator waktu, baik pada kode *TOTP* maupun Email OTP, serta notifikasi deteksi perangkat baru yang menampilkan rincian informasi perangkat secara transparan, merupakan bentuk konkret penerapan prinsip visibility of system status. Prinsip ini penting agar pengguna tidak merasa kebingungan atau khawatir berlebihan terhadap

proses verifikasi yang berlangsung, sebagaimana ditekankan dalam studi mengenai usable security [6][14].

Dari sisi keamanan, kombinasi tiga mekanisme tersebut secara signifikan mengurangi risiko pengambilalihan akun yang hanya mengandalkan Kode Akses/PIN semata, karena penyerang yang berhasil memperoleh PIN tetap harus melewati lapisan verifikasi kedua berupa kode *OTP* atau *TOTP*, atau terdeteksi melalui notifikasi perangkat baru [18][22][23]. Dengan demikian, rancangan prototype ini menjawab permasalahan yang dirumuskan pada Bab I, yaitu kebutuhan akan mekanisme keamanan berlapis pada SIAKAD yang tetap memperhatikan *prinsip Human-Computer* Interaction, sehingga peningkatan keamanan tidak menjadi beban tambahan bagi mahasiswa sebagai pengguna utama sistem.

Penulis menyadari bahwa rancangan ini masih berbentuk prototype antarmuka *(high-fidelity mockup)* yang belum diimplementasikan sebagai sistem yang berfungsi penuh (fully functional system) dan belum melalui pengujian *usability* secara kuantitatif, seperti pengukuran menggunakan *System Usability Scale (SUS)* [5] atau metode *evaluasi Cognitive Walkthrough* [3][4]. Pengujian tersebut menjadi salah satu rekomendasi penting bagi pengembangan lanjutan, sebagaimana akan dijelaskan pada Bab V.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pelaksanaan magang dan pembahasan yang telah diuraikan pada bab sebelumnya, dapat disimpulkan beberapa hal sebagai berikut.

1. Pelaksanaan magang di Badan Riset dan Inovasi Nasional (BRIN), khususnya pada Kelompok Riset *Human-Computer Interaction and Visualization* di KST B.J. Habibie Serpong, berjalan dengan baik melalui rangkaian kegiatan studi literatur, bimbingan mingguan, forum diskusi ilmiah, dan penyusunan prototype penelitian.
2. Penulis berhasil merancang dan mengimplementasikan prototype antarmuka keamanan *Two-Factor Authentication (2FA)* untuk SIAKAD menggunakan Figma, yang terdiri atas tiga mekanisme verifikasi, yaitu Email OTP, *Google Authenticator (TOTP)*, dan notifikasi deteksi perangkat baru. Setiap mekanisme dirancang dengan menerapkan prinsip *Human-Computer Interaction*, yaitu *visibility of system* status, *error prevention and recovery*, dan *user control and freedom*,sehingga penambahan

lapisan keamanan tetap memperhatikan kenyamanan dan kemudahan penggunaan bagi mahasiswa.

5.2 Saran

5.2.1 Saran bagi Instansi

BRIN, khususnya Kelompok Riset *Human-Computer Interaction and Visualization*, disarankan untuk terus mendukung penelitian lanjutan mengenai integrasi keamanan berlapis dengan prinsip *usability* pada sistem informasi, mengingat topik ini masih memiliki banyak peluang riset, khususnya pada konteks sistem informasi akademik di perguruan tinggi Indonesia.

5.2.2 Saran bagi Kampus

UIN Sultan Maulana Hasanuddin Banten disarankan untuk mempertimbangkan penambahan mekanisme *Two-Factor Authentication* pada SIAKAD yang digunakan, mengingat data akademik dan data pribadi mahasiswa yang tersimpan di dalamnya bersifat penting dan rentan apabila hanya dilindungi oleh autentikasi satu faktor. Kampus juga disarankan untuk melibatkan kajian pengalaman pengguna dalam setiap pengembangan fitur keamanan baru, agar peningkatan keamanan tidak menimbulkan kesulitan bagi mahasiswa.

5.2.3 Saran bagi Penelitian Selanjutnya

Penelitian selanjutnya disarankan untuk mengembangkan prototype ini menjadi sistem yang benar-benar berfungsi (fully functional prototype atau minimum viable product), serta melakukan pengujian *usability* secara kuantitatif menggunakan instrumen seperti *System Usability Scale (SUS)* atau metode evaluasi *Cognitive Walkthrough*, agar efektivitas rancangan *2FA* dapat diukur secara objektif. Selain itu, penelitian lanjutan juga dapat mengeksplorasi metode autentikasi tambahan lain, seperti verifikasi biometrik, sebagai pengembangan dari prototype yang telah dihasilkan dalam laporan ini.

DAFTAR PUSTAKA

[1] J. Nielsen, "10 Usability Heuristics for User Interface Design," Nielsen Norman Group, 1994.

[2] J. Nielsen and R. Molich, "Heuristic evaluation of user interfaces," in Proc. ACM CHI Conf. Human Factors in Computing Systems, 1990, pp. 249–256.

[3] C. Wharton, J. Rieman, C. Lewis, and P. Polson, "The cognitive walkthrough method: A practitioner's guide," in Usability Inspection Methods, J. Nielsen and R. L. Mack, Eds. New York: John Wiley & Sons, 1994, pp. 105–140.

[4] T. Tullis and B. Albert, Measuring the User Experience: Collecting, Analyzing, and Presenting Usability Metrics, 2nd ed. Waltham, MA: Morgan Kaufmann, 2013.

[5] J. Brooke, "SUS: A quick and dirty usability scale," in Usability Evaluation in Industry, P. W. Jordan, B. Thomas, B. A. Weerdmeester, and A. L. McClelland, Eds. London: Taylor & Francis, 1996, pp. 189–194.

[6] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed. Indianapolis, IN: Wiley, 2020.

[7] A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," in Proc. 8th USENIX Security Symp., 1999.

[8] C. Herley, "So long, and no thanks for the externalities: The rational rejection of security advice by users," in Proc. Workshop on New Security Paradigms (NSPW), 2009, pp. 133–144.

[9] ISO/IEC 27002:2022, Information Security, Cybersecurity and Privacy Protection — Information Security Controls. Geneva: International Organization for Standardization, 2022.

[10] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi, Panduan Penyelenggaraan Sistem Informasi Akademik Perguruan Tinggi. Jakarta: Kemendikbudristek, 2023.

[11] Badan Riset dan Inovasi Nasional, Profil Kawasan Sains dan Teknologi B.J. Habibie. Tangerang Selatan: BRIN, 2024.

[12] J. W. Creswell and J. D. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 6th ed. Thousand Oaks, CA: SAGE Publications, 2023.

[13] B. Shneiderman, C. Plaisant, M. Cohen, S. Jacobs, N. Elmqvist, and N. Diakopoulos, Designing the User Interface: Strategies for Effective Human-Computer Interaction, 6th ed. Boston: Pearson, 2018.

[14] L. F. Cranor and S. Garfinkel, Eds., Security and Usability: Designing Secure Systems that People Can Use. Sebastopol, CA: O'Reilly Media, 2005.

[15] J. Sauro and J. R. Lewis, Quantifying the User Experience: Practical Statistics for User Research, 2nd ed. Cambridge, MA: Morgan Kaufmann, 2016.

[16] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in Proc. IEEE Symp. Security and Privacy, 2012, pp. 553–567.

[17] A. Adams and M. A. Sasse, "Users are not the enemy," Commun. ACM, vol. 42, no. 12, pp. 40–46, Dec. 1999.

[18] D. Florencio and C. Herley, "A large-scale study of web password habits," in Proc. 16th Int. Conf. World Wide Web (WWW), 2007, pp. 657–666.

[19] A. Collins, D. Joseph, and K. Bielaczyc, "Design research: Theoretical and methodological issues," Journal of the Learning Sciences, vol. 13, no. 1, pp. 15–42, 2004.

[20] D. Norman, The Design of Everyday Things, Revised and Expanded ed. New York: Basic Books, 2013.

[21] National Institute of Standards and Technology, "Digital identity guidelines: Authentication and lifecycle management," NIST Special Publication 800-63B, 2023.

[22] M. Dasgupta, A. K. Nag, and D. Bhattacharyya, "A survey of multi-factor authentication mechanisms in modern web applications," Journal of Information Security and Applications, vol. 73, 2023.

[23] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," in Proc. IEEE/ACS Int. Conf. Computer Systems and Applications (AICCSA), 2009, pp. 641–644.

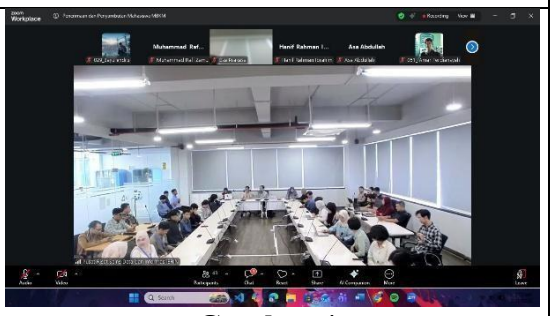
[24] S. Das, A. Kim, B. Jelen, J. Streiff, L. J. Camp, and L. Huber, "Towards implementing inclusive authentication technologies for older adults," in Proc. SOUPS Workshop on Inclusive Privacy and Security (WIPS), 2019.

LAMPIRAN

Gambar 1 .

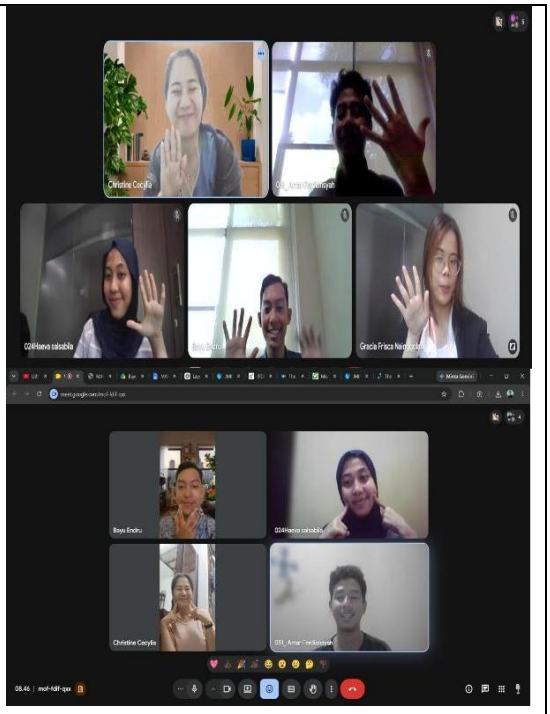
Gambar 2.

Gambar 3.



Gambar 4.

Gambar 5.



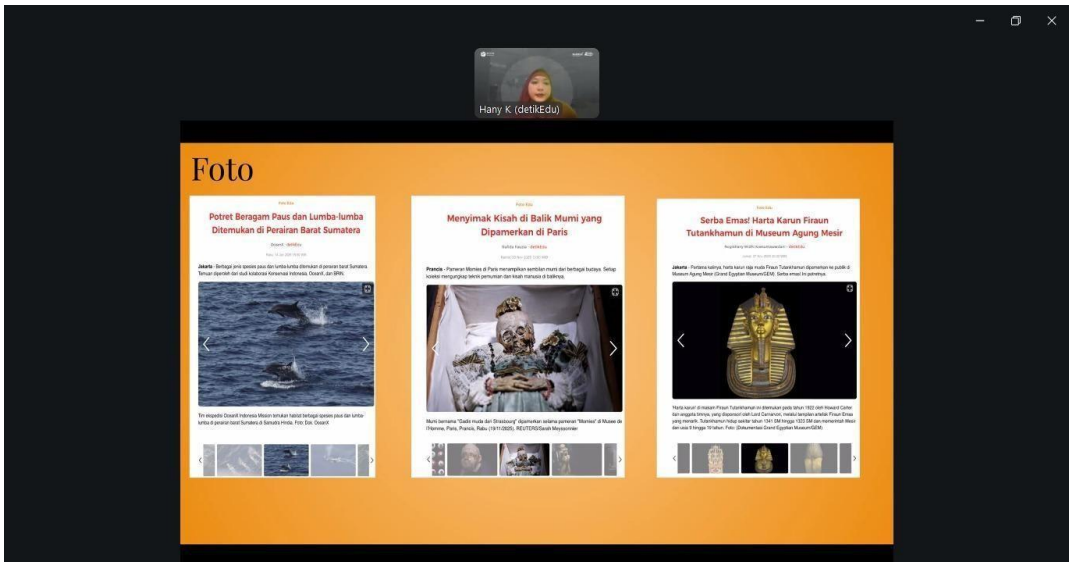
Gambar 6 .

Gambar 7.

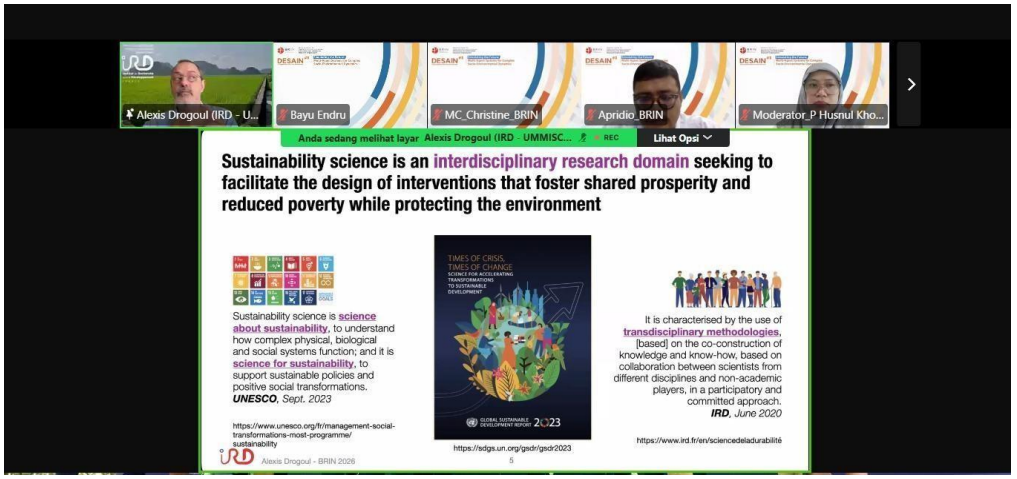
Gambar 8.

Gambar 9 .

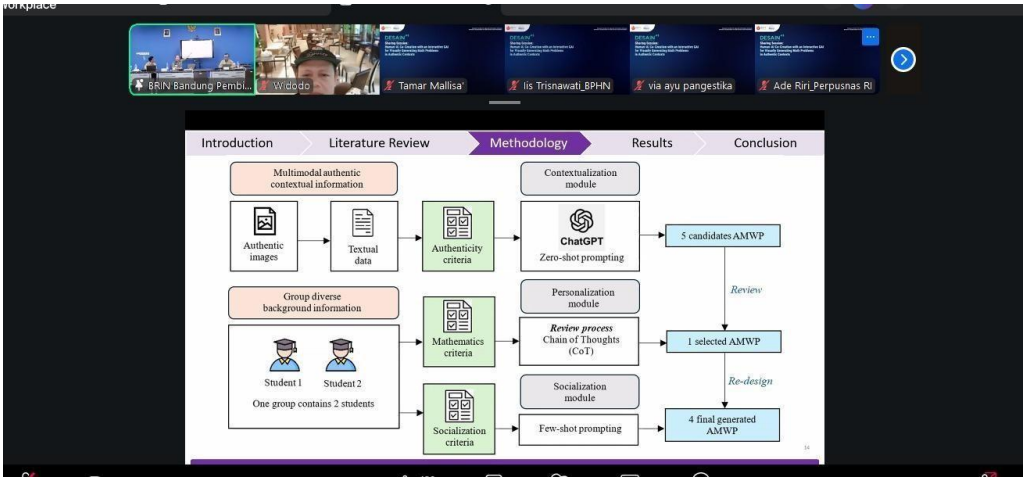
Gambar 10.

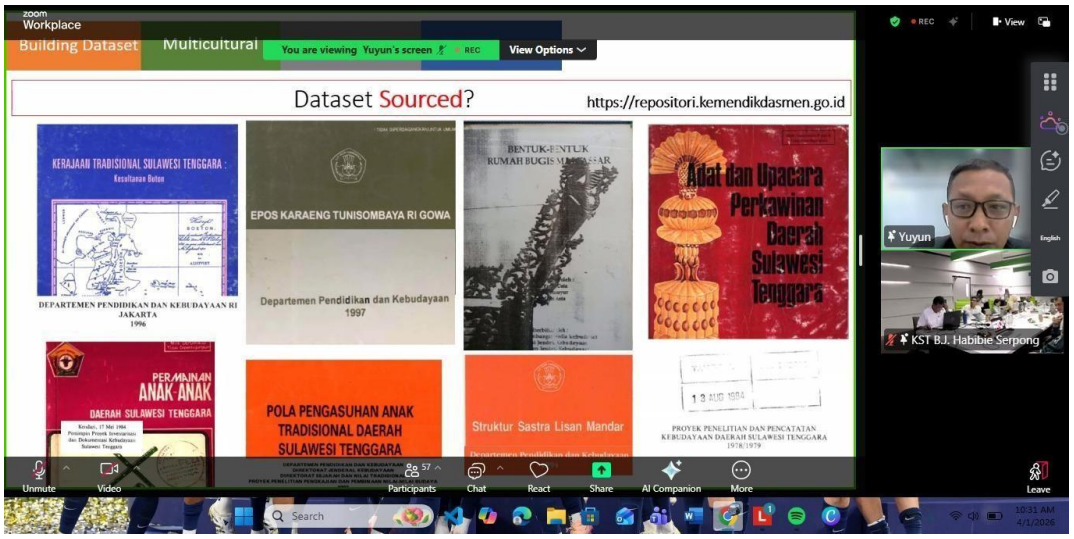

Hany K (detikEdu)
Foto
Potret Beragam Paus dan Lumba-lumba Ditemukan di Perairan Barat Sumatera
Menyimak Kisah di Balik Mumi yang Dipamerkan di Paris
Serba Emas! Harta Karun Firaun Tutankhamun di Museum Agung Mesir


zoom Workplace
Meeting
Andrari Grahitandaru's screen
REC
Andrari Grahitandaru
Budi N
Harnum Annisa
Esa Prakasa
Muhamad Jafar Elly
Rachiyatul Fajri
BRIN
"e-Voting bukan sekadar digitalisasi pemungutan suara, tetapi transformasi tata kelola demokrasi desa menuju proses yang lebih transparan, akuntabel, aman, dan dipercaya masyarakat."
DASAR HUKUM
•Putusan Mahkamah Konstitusi (MK) :Penggunaan e-voting pertama kali dinyatakan konstitusional dan legal berdasarkan Putusan MK Nomor 147/PUU-VII/2009, dan ditegaskan kembali dalam Putusan MK Nomor 137/PUU-XXII/2024yang meminta pembentuk undang-undang mempertimbangkan penggunaan peralatan pemilihan secara elektronik demi mewujudkan efektivitas dan efisiensi.
•Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)Keabsahan sistem elektronik yang digunakan dalam e-voting diatur dalam UU Nomor 19 Tahun 2016 tentang Perubahan Atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Amanatnya tertuang pada Pasal 5 ayat (1) dan (2) yang mengakui informasi dan/atau dokumen elektronik sebagai alat bukti hukum yang sah.
•Undang-Undang Pemilihan Kepala Daerah (Pilkada) : Metode pemungutan suara elektronik diakomodasi melalui revisi undang-undang pemilihan, di mana UU Nomor 1 Tahun 2015 (sebagai perubahan dari UU No. 32 Tahun 2004)
Audio
Video
Participants
Chat
React
Share
More
Leave


Alexis Drogoul (IRD - U...
Bayu Endru
MC_Christine_BRIN
Apridio_BRIN
Moderator_P Husnul Kho...
Anda sedang melihat layar Alexis Drogoul (IRD UMMISC...
Lihat Opsi
Sustainability science is an interdisciplinary research domain seeking to facilitate the design of interventions that foster shared prosperity and reduced poverty while protecting the environment
Sustainability science is science about sustainability, to understand how complex physical, biological and social systems function; and it is science for sustainability, to support sustainable policies and positive social transformations.
UNESCO, Sept. 2023
https://www.unesco.org/fr/management-social-transformations-most-programme/sustainability
TIMES OF CRISIS, TIMES OF CHANGE
GLOBAL SUSTAINABLE DEVELOPMENT REPORT 2023
https://sdgs.un.org/gsdr/gsdr2023
It is characterised by the use of transdisciplinary methodologies, [based] on the co-construction of knowledge and know-how, based on collaboration between scientists from different disciplines and non-academic players, in a participatory and committed approach.
IRD, June 2020
https://www.ird.fr/en/sciencedeladurabilité
Alexis Drogoul - BRIN 2026
5

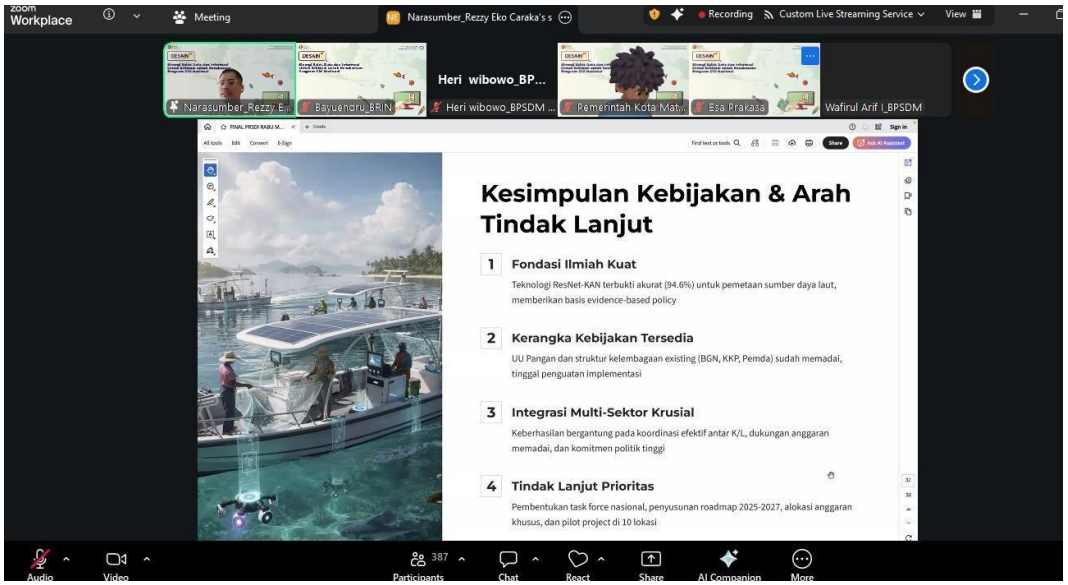

Christine Cecylia
024Haeva salsabila
Gracia Frisca Nainggolan
meet.google.com/nzw-ebaw-rhu
Christine Cecylia
Bayu Endru
051_ Amar Ferdiansyah
024Haeva salsabila
Gracia Frisca Nainggolan
10.16 | nzw-ebaw-rhu


BRIN Bandung Pembi...
Widodo
Tamar Mallisa'
Iis Trisnawati_BPHN
via ayu pangestika
Ade Riri_Perpusnas RI
Introduction
Literature Review
Methodology
Results
Conclusion
Multimodal authentic contextual information
Authentic images
Textual data
Authenticity criteria
Contextualization module
ChatGPT
Zero-shot prompting
5 candidates AMWP
Review
Group diverse background information
Student 1
Student 2
One group contains 2 students
Mathematics criteria
Personalization module
Review process
Chain of Thoughts (CoT)
1 selected AMWP
Re-design
Socialization criteria
Socialization module
Few-shot prompting
4 final generated AMWP

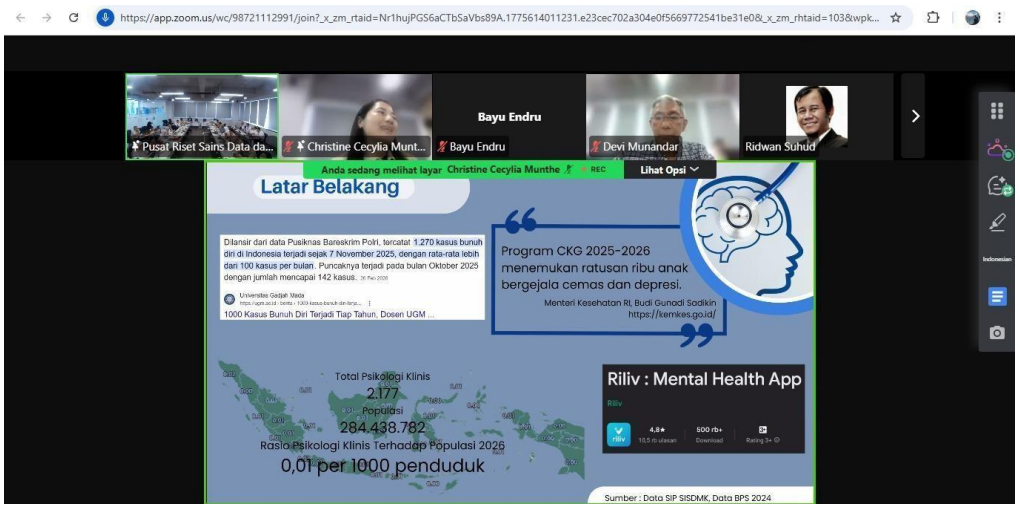

Workplace
Building Dataset
Multicultural
You are viewing Yuyun's screen
View Options
Dataset Sourced?
https://repositori.kemendikdasmen.go.id
KERAJAAN TRADISIONAL SULAWESI TENGGARA :
DEPARTEMEN PENDIDIKAN DAN KEBUDAYAAN RI
JAKARTA
1996
EPOS KARAENG TUNISOMBAYA RI GOWA
Departemen Pendidikan dan Kebudayaan
1997
Adat dan Upacara Perkawinan Daerah Sulawesi Tenggara
PERMAINAN ANAK-ANAK
DAERAH SULAWESI TENGGARA
POLA PENGASUHAN ANAK TRADISIONAL DAERAH SULAWESI TENGGARA
Struktur Sastra Lisan Mandar
PROYEK PENELITIAN DAN PENCATATAN KEBUDAYAAN DAERAH SULAWESI TENGGARA
1978/1979
Yuyun
KST B.J. Habibie Serpong
Unmute
Video
Participants
Chat
React
Share
AI Companion
More
Leave


Pentingnya Monitoring Pertanian
Ketergantungan global terhadap padi menuntut adanya sistem pemantauan yang kuat, terutama mengingat meningkatnya risiko yang dipicu oleh perubahan iklim seperti kekeringan, banjir, dan hama, serta ekspansi ekonomi dan demografi (Bachri et al., 2024)
Narasumber_Wawan Hendriawan Nur


Narasumber_Furqon
029_Bayu endru
Narasumber_M. Hasa...
Moderator_Dr. Heng...
Heri wibowo_BP...
Heri wibowo_BPSDM ...
Pemerintah Kota Mat...
AMANAT PEMERINTAHAN DIGITAL
BADAN GIZI NASIONAL
Arahan Presiden Prabowo Subianto terkait
Transformasi Pemerintahan
Responsivitas Birokrasi
Birokrasi lebih responsif dan tidak mempersulit masyarakat
Pemberantasan Korupsi & Kebocoran Anggaran
Penegakan hukum, terutama dalam mencegah korupsi di kalangan birokrasi. Pengawasan harus diperketat agar tidak terjadi penyimpangan dalam alokasi anggaran.
Percepatan Implementasi Kebijakan
Implementasi kebijakan yang telah dirumuskan dengan cepat dan efektif
Pengelolaan ASN
Memastikan disiplin dan produktivitas aparatur, serta melaksanakan peningkatan kompetensi
Penguatan Koordinasi Antar Lembaga
Memperkuat sinergitas dan koordinasi antar kementerian/lembaga
Pelayanan Berbasis Teknologi
Pemanfaatan teknologi untuk mempercepat penyebaran pendidikan dan akses ke layanan dasar.
Efektivitas Alokasi Anggaran
Alokasi anggaran digunakan secara efektif dan mendukung program prioritas, mengurangi kegiatan yang tidak berdampak langsung pada rakyat.
Reformasi Pelayanan Publik
Pembenahan pelayanan publik agar lebih efisien dan transparan sesuai kebutuhan masyarakat


Kesimpulan Kebijakan & Arah Tindak Lanjut
1 Fondasi Ilmiah Kuat
Teknologi ResNet-KAN terbukti akurat (94.6%) untuk pemetaan sumber daya laut, memberikan basis evidence-based policy
2 Kerangka Kebijakan Tersedia
UU Pangan dan struktur kelembagaan existing (BGN, KKP, Pemda) sudah memadai, tinggal penguatan implementasi
3 Integrasi Multi-Sektor Krusial
Keberhasilan bergantung pada koordinasi efektif antar K/L, dukungan anggaran memadai, dan komitmen politik tinggi
4 Tindak Lanjut Prioritas
Pembentukan task force nasional, penyusunan roadmap 2025-2027, alokasi anggaran khusus, dan pilot project di 10 lokasi


Siska Pebiana
029_Bayu endru
Teduh
Arafat
Ghobin Sinaga
Nimas Ayu Untariyati
BRIN
AI Safety Red Teaming Challenge Singapore
HARD CHALLENGE
Weekly Meeting PRSDI-February 18th 2025


Bayu Endru
Latar Belakang
Program CKG 2025-2026 menemukan ratusan ribu anak bergejala cemas dan depresi.
Menteri Kesehatan RI, Budi Gunadi Sadikin
https://kemkes.go.id/
Total Psikologi Klinis
2.177
Populasi
284.438.782
Rasio Psikologi Klinis Terhadap Populasi 2026
0,01 per 1000 penduduk
Riliv : Mental Health App
Sumber : Data SIP SISDMK, Data BPS 2024