PENGEMBANGAN FITUR AUTENTIKASI TANPA PASSWORD PADA SISTEM SSO UNDIKSHA DENGAN TEKNOLOGI FIDO2 PASSKEY

OLEH

I PUTU TEDI SOGUN

NIM 1715051073

PROGRAM STUDI PENDIDIKAN TEKNIK INFORMATIKA

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN KEJURUAN

UNIVERSITAS PENDIDIKAN GANESHA

SINGARAJA

2023

DAFTAR ISI

DAFTAR ISI II
DAFTAR TABEL III
DAFTAR GAMBAR IV
ABSTRAK V
BAB I PENDAHULUAN 1
1.1 LATAR BELAKANG 1
1.2 RUMUSAN MASALAH 5
1.3 TUJUAN PENELITIAN 5
1.4 BATASAN MASALAH PENELITIAN 5
1.5 MANFAAT HASIL PENELITIAN 6
BAB II KAJIAN TEORI 7
2.1 KAJIAN PUSTAKA 7
2.2 LANDASAN TEORI 10
2.2.1 Autentikasi 10
2.2.2 FIDO 11
2.2.3 FIDO2 12
2.2.4 FIDO2 Passkey 13
2.2.5 Elliptic Curve Digital Signature Algorithm (ECDSA) 16
2.2.6 RSA Digital Signature Algorithm 17
2.2.7 SHA256 18
BAB III METODOLOGI PENELITIAN 19
3.1 JENIS PENELITIAN 19
3.2 TAHAPAN PENELITIAN 19
3.2.1 Tahap Requirement Analysis 20
3.2.2 Tahap Design 24
3.2.3 Tahap Implementation 31
3.2.4 Tahap Verification 31
3.3 JADWAL PENELITIAN 35
DAFTAR PUSTAKA 37

DAFTAR TABEL

Tabel 3.1 Analisis Pengguna 22
Tabel 3.2 Kebutuhan Fungsional Sistem 23
Tabel 3.3 Kebutuhan Non-fungsional Sistem 24
Tabel 3.4 Interval Interpretasi Skor 34

DAFTAR GAMBAR

Gambar 2.1 Ringkas Proses Registrasi dengan metode FIDO2 Passkey 14
Gambar 2.2 Proses Registrasi dengan metode FIDO2 Passkey secara Mendetail 15
Gambar 2.3 Ringkas Proses Login dengan metode FIDO2 Passkey 15
Gambar 2.4 Proses Login dengan metode FIDO2 Passkey secara Mendetail 16

Gambar 3.1 Siklus SDLC Model Waterfall 20
Gambar 3.2 Flowchart Registrasi Sistem 25
Gambar 3.3 Flowchart Login ke Sistem 26
Gambar 3.4 Rancangan Basis Data 27
Gambar 3.5 Homepage SSO Undiksha 28
Gambar 3.6 Penggunaan Biometrik atau Pin 28
Gambar 3.7 Pesan Sukses Registrasi FIDO2 Passkey 29
Gambar 3.8 Halaman Login SSO Undiksha dengan FIDO2 Passkey 29
Gambar 3.9 Proses Login menggunakan FIDO2 Passkey 30
Gambar 3.10 Login Berhasil dengan metode FIDO2 Passkey 30

ABSTRAK

SSO Undiksha merupakan layanan autentikasi pengguna berbasis website untuk dapat mengakses layanan-layanan sistem informasi yang ada di Universitas Pendidikan Ganesha. Sistem autentikasi ini masih menggunakan metode password. Penggunaan password sebagai metode keamanan autentikasi ke dalam sebuah sistem menjadi penyebab utama kebobolan data karena kebanyakan pengguna menggunakan password yang lemah. Dari segi pengalaman pengguna password juga kurang nyaman digunakan karena password yang kuat adalah password yang sulit untuk diingat. Hal tersebut menjadikan perlu adanya pengembangan fitur autentikasi tanpa password pada sistem SSO Undiksha menggunakan teknologi terbaru FIDO2 Passkey. Dengan implementasi FIDO2 Passkey, diharapkan dapat meningkatkan keamanan dan kenyamanan dalam proses autentikasi pengguna serta meminimalkan masalah yang terjadi pada mekanisme autentikasi dengan password. Kajian teori yang dilakukan meliputi pemahaman tentang metode-metode autentikasi yang digunakan pada saat ini, standar FIDO2 Passkey dan analisis perbandingan kinerja antara metode autentikasi yang digunakan saat ini dengan FIDO2 Passkey. Hasil dari penelitian ini diharapkan dapat memberikan manfaat dalam pengembangan sistem autentikasi pada layanan sistem SSO yang ada di Universitas Pendidikan Ganesha.

Kata Kunci: FIDO2, Passkey, Webauthn, SSO Undiksha

BAB I PENDAHULUAN

1.1 LATAR BELAKANG

Autentikasi adalah sebuah proses validasi atau pembuktian identitas terhadap pengguna yang ingin mengakses suatu file, aplikasi, atau sistem tertentu. Proses autentikasi menyediakan kontrol akses ke sistem dengan mencocokkan apakah kredensial(data/identitas) pengguna sesuai kredensial pada basis data pengguna yang berwenang (server data). Apabila kredensial pengguna sesuai dengan yang terekam di kredensial sistem, maka pengguna tersebut diizinkan untuk mengakses sistem. Ada beberapa jenis autentikasi yang paling umum digunakan antara lain autentikasi biometrik yaitu jenis autentikasi yang memverifikasi individu berdasarkan karakteristik biologis unik mereka. Karakter unik individu yang bisa dijadikan sebagai faktor autentikasi antara lain sidik jari, iris pada bola mata, bentuk wajah dan lain sebagainya. Keunggulan dari penggunaan autentikasi biometrik adalah proses autentikasi yang cepat dan mudah dilakukan, ini menciptakan kenyamanan bagi pengguna dalam melakukan proses autentikasi. Kemudian ada jenis autentikasi menggunakan perangkat keras. Jenis perangkat keras yang biasa digunakan dalam autentikasi ini adalah kartu identitas yang memanfaatkan sinyal rfid. Ada juga menggunakan USB Key seperti Yubikey dalam proses autentikasi. Tetapi autentikasi yang paling umum digunakan adalah autentikasi menggunakan metode password.

Menurut (Feri Sulianta, 2009) password dalam bahasa Indonesia yang berarti kata sandi adalah deretan karakter yang dimasukan untuk mendapatkan akses terhadap file, aplikasi atau sistem komputer. Password umum digunakan sebagai mekanisme autentikasi di Internet. Namun, autentikasi menggunakan password memiliki banyak celah keamanan. Password yang dibuat dengan asal-asalan seperti menggunakan tanggal lahir yang sangat rentan untuk diretas. Salah satu penyebab kebobolan data di Internet disebabkan oleh lemahnya password yang digunakan oleh pengguna. Hal ini dikarenakan manusia memiliki keterbatasan untuk mengingat, sesuatu yang unik dan panjang seperti password. Ketika terjadi

data kebocoran atau kebobolan di dalam sistem server dan peretas berhasil mencuri basis data pengguna yang berisi *hash-password* maka dia bisa menebak password dari pengguna menggunakan teknik *brute-force attack* atau mencoba beberapa kombinasi password, sampai menemukan informasi password yang benar. Teknik ini memiliki persentase yang tinggi jika password yang digunakan pengguna lemah dan tidak unik (Bonneau, J., Herley, C., Oorschout, P. C. V., & Stajano, F., 2015).

Menurut data publikasi monitoring BSSN pada tahun 2022, password masih menjadi penyebab utama kebocoran data. Dalam publikasi ini pula ada beberapa hal yang bisa dilakukan untuk mengurangi terjadinya risiko kebocoran data karena penggunaan password, salah satu di antaranya adalah menggunakan password yang kuat (Laporan Hasil Monitoring Keamanan Siber Tahun 2022, 2022). Penggunaan password juga sangat rentan terhadap tindakan *phising* khususnya bagi pengguna yang kurang teliti dalam masuk ke sebuah sistem. Dari segi pengalaman pengguna, penggunaan password juga kurang nyaman untuk digunakan karena rata-rata panjang password yang kuat saat ini minimal 10 karakter yang terdiri dari kombinasi dari huruf, nomor dan simbol. Password yang kuat adalah password yang sulit untuk diingat (Katha Chanda, 2016).

SSO (Single Sign-On) Undiksha merupakan layanan autentikasi sekali login berbasis website untuk dapat mengakses berbagai layanan sistem informasi yang ada di Universitas Pendidikan Ganesha (E-Ganesha). Layanan SSO Undiksha digunakan oleh Pihak Dosen dan Mahasiswa dalam proses perkuliahan di Universitas Pendidikan Ganesha secara daring. Adanya layanan ini memudahkan pengguna karena hanya dengan melakukan autentikasi sekali pada halaman *login* SSO Undiksha, pengguna bisa mengakses berbagai layanan seperti E-learning, SIAK dan lainnya tanpa harus melakukan proses autentikasi berulang-ulang. Namun layanan ini masih menggunakan mekanisme autentikasi dengan password.

Penggunaan password sebagai metode autentikasi telah menyebabkan berbagai masalah keamanan dan kenyamanan bagi pengguna. Wawancara dengan Kepala UPT TIK dan Ketua Divisi Infrastruktur dan Keamanan UPT TIK mengungkapkan bahwa kelemahan dalam penggunaan password pada sistem SSO UNDIKSHA meliputi kelalaian pengguna dalam mengelola password, penggunaan password lemah yang mudah ditebak, dan kebiasaan berbagi password dengan

orang lain. Contoh kejadian kelalaian ini terjadi pada salah satu Dosen Universitas Pendidikan Ganesha yang membagikan passwordnya dengan Mahasiswa, mengakibatkan akses yang tidak diizinkan dan perubahan data di sistem Siak. Kejadian serupa juga terjadi pada Pegawai Universitas Pendidikan Ganesha, dimana data kepegawainnya diubah oleh entitas tanpa izin yang berhasil masuk menggunakan kredensial akun pengguna.

Berdasarkan data kejadian tersebut, dapat disimpulkan bahwa password menjadi masalah utama yang memungkinkan keberhasilan penyerang menyusupi sebuah sistem. Meskipun saat ini kasus phishing belum pernah terjadi pada sistem SSO UNDIKSHA, namun karena maraknya serangan phishing yang disebabkan oleh kelalaian pengguna dan kurangnya pengetahuan tentang metode penyerangan ini, penting untuk memitigasi risiko di masa mendatang. Oleh karena itu, penggunaan metode autentikasi password harus segera diganti dengan metode autentikasi yang lebih aman untuk meminimalisir kejadian akses tanpa izin dan penyerangan phishing. Alternatif metode autentikasi selain password yang dapat digunakan adalah One-Time Password (OTP), Google Authenticator, dan FIDO2 Passkey. Metode autentikasi OTP mengirimkan kode yang berubah setiap kali pengguna melakukan login atau autentikasi. Namun, metode ini rentan terhadap serangan phishing (Sivaprasad, R., & Sivasubramanian, S., 2020) dan memerlukan biaya implementasi yang mahal, terutama karena penggunaan SMS Gateway untuk mengirimkan kode OTP. Metode Google Authenticator, yang digunakan sebagai faktor kedua dalam autentikasi, dapat meminimalisir kejadian berbagi password dan meningkatkan kekuatan password pengguna. Namun, Google Authenticator tidak dapat sepenuhnya memitigasi risiko terjadinya serangan phishing.

Metode autentikasi yang bisa digunakan lainnya adalah FIDO2 Passkey lebih aman dari OTP maupun Google Authenticator karena tidak rentan terhadap serangan *phishing* atau *man-in-the-middle*, dan *SIM swapping*, dan tidak memerlukan pengiriman kode rahasia yang dapat dicuri atau ditiru oleh penyerang. Selain keamanannya, pengimplementasian FIDO2 Passkey juga lebih hemat biaya dibandingkan dengan metode OTP. Hal ini karena penggunaan FIDO2 Passkey tidak memerlukan biaya tambahan seperti pada metode OTP yang menggunakan *SMS Gateway* untuk mengirimkan kode rahasia ke ponsel pengguna, FIDO Alliance

(2021). Kesimpulannya, FIDO2 Passkey menjadi metode autentikasi terbaik untuk dipilih dibandingkan dengan OTP karena lebih aman dan efektif dalam memverifikasi identitas pengguna. FIDO2 Passkey menggunakan teknologi kriptografi yang kuat, sehingga kridensial hampir tidak mungkin bisa ditebak walaupun menggunakan super komputer, arsitektur dan pengimplementasian FIDO2 juga memastikan bahwa kridensial hanya bisa diakses oleh sistem yang sah sehingga menyebabkan metode penyerangan phising sangat tidak mungkin untuk dilakukan.

FIDO2 Passkey menggunakan teknologi dari FIDO Alliance (Fast IDentity Online) yang menyediakan standar untuk autentikasi yang aman, mudah digunakan, dan tidak tergantung pada perangkat keras atau perangkat lunak tertentu. FIDO2 Passkey menggunakan teknologi *Public Key Cryptography* (PKC) yang memungkinkan pengguna untuk menggunakan perangkat yang dimiliki sebagai faktor autentikasi, seperti *fingerprint, facial recognition* atau PIN. Dengan menggunakan FIDO2 Passkey, diharapkan dapat meningkatkan keamanan dan kenyamanan dalam proses autentikasi pengguna serta meminimalkan masalah yang terjadi pada saat lupa password.

Penelitian ini akan mencakup rancangan dan pembuatan prototipe sistem autentikasi FIDO2 Passkey yang kompitabel dengan sistem autentikasi pada SSO Undiksha saat ini, serta pengujian dan evaluasi terhadap kenyamanan pengguna terhadap fitur autentikasi tanpa password dengan FIDO2 Passkey yang dikembangkan. Penelitian FIDO2 Passkey pada SSO Undiksha diharapkan dapat menjadi referensi atau acuan yang berguna dalam pemilihan dan pengembangan metode autentikasi baru di Sistem SSO Undiksha nantinya, serta dapat diadaptasikan oleh institusi lain yang memiliki sistem autentikasi yang serupa. Secara keseluruhan, skripsi ini akan memberikan kontribusi dalam bidang keamanan informasi dengan mengembangkan fitur autentikasi tanpa password yang lebih aman dan nyaman bagi pengguna. Dengan demikian, skripsi ini diharapkan dapat memberikan manfaat yang signifikan bagi Universitas Pendidikan Ganesha dan institusi lain yang memiliki sistem autentikasi yang serupa.

Berdasarkan latar belakang di atas yang telah dipaparkan, peneliti tertarik untuk melakukan penelitian dengan judul yaitu “Pengembangan Fitur Autentikasi

Tanpa Password Pada Sistem SSO Undiksha Dengan Teknologi Fido2 Passkey". Dengan dikembangkan fitur ini diharapkan proses autentikasi pada layanan SSO Undiksha menjadi lebih aman dan nyaman digunakan.

1.2 RUMUSAN MASALAH

1. Bagaimana rancangan Fitur Autentikasi tanpa Password dengan teknologi FIDO2 Passkey pada SSO UNDIKSHA berbasis website.
2. Bagaimana Implementasi Fitur Autentikasi tanpa Password dengan teknologi FIDO2 Passkey pada SSO UNDIKSHA berbasis website.
3. Bagaimana Pengujian dan Evaluasi terhadap Fitur Autentikasi tanpa Password dengan teknologi FIDO2 Passkey pada SSO UNDIKSHA berbasis website.

1.3 TUJUAN PENELITIAN

1. Merancang Fitur Autentikasi tanpa Password dengan teknologi FIDO2 Passkey pada SSO UNDIKSHA berbasis website.
2. Implementasi Fitur Autentikasi tanpa Password dengan teknologi FIDO2 Passkey pada SSO UNDIKSHA berbasis website.
3. Pengujian dan Evaluasi terhadap Fitur Autentikasi tanpa password dengan teknologi FIDO2 Passkey pada SSO UNDIKSHA berbasis website.

1.4 BATASAN MASALAH PENELITIAN

1. Penelitian hanya membahas rancangan dan implementasi proses registrasi dan login pada SSO Undiksha versi website yang secara eksklusif hanya bisa diakses melalui aplikasi web browser
2. Penelitian ini tidak membahas secara mendetail tentang aspek kriptografi dari FIDO2 Passkey
3. Output dari fase rancangan dan implementasi berupa prototipe halaman registrasi dan login SSO Undiksha menggunakan fitur Autentikasi tanpa Password dengan teknologi FIDO2 Passkey yang siap untuk diuji dan di evaluasi

1.5 MANFAAT HASIL PENELITIAN

1. **Manfaat Teoritis**

   Penelitian ini kedepannya diharapkan dapat menjadi referensi, acuan ataupun sumber bacaan terkait dengan pengembangan teknologi autentikasi tanpa password dengan FIDO2 Passkey

2. **Manfaat Praktis**

   a. Manfaat bagi Universitas Pendidikan Ganesha. Pengembangan fitur autentikasi tanpa password untuk masuk ke sistem SSO Undiksha dengan teknologi FIDO2 Passkey bisa dijadikan referensi atau acuan dalam pengembangan sistem autentikasi baru nantinya pada sistem SSO Undiksha

   b. Manfaat bagi Peneliti.

      1. Dapat mengembangkan dan mengimplementasikan teknologi terbaru yaitu autentikasi tanpa password dengan menerapkan teknologi FIDO2 Passkey pada sebuah sistem
      2. Sebagai Wadah untuk merealisasikan teori-teori yang sebelumnya telah didapat di bangku perkuliahan

BAB II KAJIAN TEORI

2.1 KAJIAN PUSTAKA

Dalam pemilihan topik penelitian ini, penulis terinspirasi dan mereferensi dari beberapa penelitian yang telah dilakukan sebelumnya yang berkaitan dengan Kelemahan autentikasi menggunakan password, penerapan autentikasi dengan FIDO2 Passkey. Berikut ini beberapa penelitian terdahulu yang menjadi referensi penelitian ini.

Penelitian terkait tentang analisis kekuatan dan kerentanan dari password dilakukan oleh Katha Chanda (2016) dengan judul “Password Security: An Analysis of Password Strengths and Vulnerabilities”. Dalam penelitian ini dijelaskan bawah Saat pengguna menyetel password, mereka cenderung mengatur password umum. Kalau bukan nama keluarga dekat anggota atau tempat tinggal, sering kali berupa 'kata sandi', ‘password123’, atau ‘abcdef4567’ dan lain-lain. Jika password yang diatur dengan sesuatu yang sangat umum maka penyerang dapat menjalankan dictionary attack menggunakan kamus daftar kata umum atau buku frase dan ada kemungkinan serangan itu berhasil. Untuk menciptakan password yang kuat dibutuhkan kombinasi antara panjang karakter password dan jumlah set karakter seperti kombinasi dari huruf kecil dan huruf besar, angka dan simbol yang digunakan dalam password. Password yang kuat adalah password yang panjang, unik dan susah untuk diingat.

FIDO Alliance (2022). "FIDO Authentication A Passwordless Vision". Pada artikel ini, FIDO Alliance memberikan penjelasan mengenai FIDO2 yang merupakan standar baru untuk autentikasi yang kuat. FIDO2 menawarkan keamanan yang lebih baik dibandingkan metode autentikasi yang digunakan saat ini seperti *username* dan password. Selain itu, FIDO2 juga digambarkan sebagai teknologi yang mudah digunakan dan tidak tergantung pada perangkat keras atau perangkat lunak tertentu.

IBM (2019). "FIDO2: The future of passwordless authentication" Pada artikel ini, IBM menyatakan bahwa FIDO2 adalah standar baru untuk autentikasi tanpa password yang aman dan mudah digunakan. FIDO2 menawarkan keamanan

yang lebih baik dengan menggunakan teknologi PKC yang memungkinkan pengguna untuk menggunakan perangkat yang dimiliki sebagai faktor autentikasi. Selain itu, FIDO2 juga diharapkan dapat mengurangi masalah yang terjadi pada saat lupa password.

Penelitian yang membahas tentang autentikasi passwordless dengan berbasis FIDO2 dilakukan oleh Fatima Alqubaisi, Ahmad Samer Wazan dan Liza Ahmad (2020). Penelitian ini memiliki judul "Should We Rush to Implement Password-less Single Factor FIDO2 based Authentication?". Tren di dunia web adalah berupaya secepat mungkin untuk menjauh dari autentikasi menggunakan password dan beralih ke autentikasi passwordless yang lebih kuat dan lebih aman. Menjawab tren ini, peneliti melakukan penelitian yang berupaya untuk mencari jawaban apakah kita harus bergegas mengganti sistem autentikasi yang sebelumnya berbasis password menjadi *passwordless*. Penelitian ini membandingkan model ancaman (*threat models*) dari mekanisme autentikasi dengan password dan autentikasi passwordless berbasis FIDO2. Di akhir penelitian, peneliti memberikan kesimpulan dengan jelas bahwa autentikasi (*Single Factor)* berbasis FIDO2 lebih aman dari autentikasi (*Single Factor*) berbasis password. Penelitian juga menyebutkan bahwa sebagian besar model ancaman(*threat models*) pada autentikasi berbasis password dapat ditutupi dengan autentikasi *passwordless* berbasis FIDO2.

Penelitian yang dilakukan oleh Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes dan Sven Bugiel (2020) dengan judul "Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication" dengan jelas memiliki kekhawatiran akan penerimaan pengguna sistem dengan perubahan metode autentikasi dari menggunakan password menjadi passwordless. Perubahan paradigma tentang cara autentikasi yang sebelumnya merupakan sebuah faktor pengetahuan menjadi faktor kepemilikan. Dari penelitian ini menunjukan bahwa pengguna menganggap autentikasi dengan standar FIDO2 sebagai lebih bermanfaat dan lebih dapat diterima daripada autentikasi berbasis password tradisional, tetapi juga ada kekhawatiran yang menghalangi keinginan pengguna untuk meninggalkan password. kekhawatiran ini berakar pada kesenjangan antara perspektif pribadi

pengguna ke teknologi autentikasi baru ini dan pandangan global dari desainer FIDO2 yang mungkin belum cukup menyertakan pandangan pengguna.

Penelitian yang dilakukan oleh Leon Wursching, Florentin Putz, Steffen Haesler dan Matthias Hollick (2023) dengan judul "FIDO2 the Rescue? Platform vs. Roaming Authentication on Smartphones" membandingkan metode authenticator yang digunakan pada fido2 yaitu antara Platform dan Roaming Authentication. Penelitian ini bertujuan untuk menentukan kelebihan dan kelemahan FIDO2 penggunaan dalam skenario mobile. Sebagian besar peserta bersedia mengadopsi autentikasi dengan metode FIDO2 selama studi pengguna tatap muka, tetapi analisis lebih lanjut menunjukkan bahwa peserta memberi prioritas yang berbeda terhadap kegunaan, keamanan, dan ketersediaan. Pada penelitian ini disimpulkan bahwa hambatan adopsi terakhir dari autentikasi menggunakan FIDO2 adalah pada bagian ketersediaan(availability) yaitu pendelegasian akun dan penggunaan akun pada multi client masih sulit untuk dilakukan.

Kajian pustaka ini membahas tentang autentikasi menggunakan FIDO2 sebagai alternatif yang lebih aman dan efisien daripada autentikasi berbasis password tradisional. Penelitian sebelumnya menyoroti kelemahan dari penggunaan password, di mana pengguna sering mengatur password yang lemah dan mudah ditebak, meningkatkan risiko serangan seperti dictionary attack. Untuk mengatasi masalah ini, FIDO2 diperkenalkan sebagai standar baru untuk autentikasi yang kuat dan passwordless. Penelitian-penelitian tersebut menyatakan bahwa FIDO2 menawarkan keamanan yang lebih baik dengan menggunakan teknologi Public Key Cryptography (PKC), memungkinkan pengguna untuk menggunakan perangkat yang dimilikinya sebagai faktor autentikasi. FIDO2 juga dianggap mudah digunakan dan tidak bergantung pada perangkat keras atau perangkat lunak tertentu. Meskipun demikian, ada beberapa kekhawatiran dan hambatan adopsi terkait perubahan paradigma dari autentikasi berbasis password menjadi passwordless. Beberapa pengguna masih ragu untuk meninggalkan penggunaan password karena kebiasaan dan kesenjangan antara perspektif pribadi pengguna dan pandangan desainer FIDO2. Selain itu, dalam skenario mobile, masalah ketersediaan (availability) dan pendelegasian akun pada multi client masih

menjadi kendala dalam adopsi FIDO2. Secara keseluruhan, kajian pustaka ini menyimpulkan bahwa FIDO2 memiliki potensi besar sebagai solusi autentikasi yang lebih aman dan diterima

2.2 LANDASAN TEORI

2.2.1 Autentikasi

Dalam penelitian oleh oleh Butler Lampson, Martín Abadi, Michael Burrows, dan Edward Wobber (1992) berjudul "Authentication in Distributed Systems: Theory and Practice", autentikasi didefinisikan sebagai proses yang digunakan untuk membuktikan identitas pengguna, proses, atau sistem dalam konteks sistem terdistribusi. Autentikasi bertujuan untuk memastikan bahwa entitas yang mengakses sumber daya atau layanan dalam sistem memiliki izin yang tepat dan benar-benar merupakan entitas yang mengakuinya. Dengan demikian, autentikasi berfungsi sebagai langkah penting dalam menjaga keamanan dan integritas sebuah sistem. Apabila kredensial pengguna sesuai dengan yang terekam di kredensial sistem, maka pengguna tersebut diizinkan untuk mengakses sistem.

Metode autentikasi yang paling umum digunakan saat ini adalah autentikasi berbasis kata sandi (*password-based authentication*). Metode ini mengharuskan pengguna untuk memasukkan kata sandi yang telah ditetapkan sebelumnya saat mencoba mengakses sistem atau layanan. Meskipun autentikasi berbasis kata sandi telah menjadi standar dalam industri selama beberapa dekade, metode ini memiliki beberapa kelemahan, seperti rentan terhadap serangan *brute-force*, kelemahan dalam memilih kata sandi yang lemah oleh pengguna, dan ancaman *phishing*. Oleh karena itu, metode autentikasi yang lebih kuat dan aman, seperti autentikasi dua faktor (2FA) dan autentikasi *multi-faktor* (MFA), mulai mendapat perhatian dan implementasi yang lebih luas. Autentikasi dua faktor menggabungkan dua metode autentikasi yang berbeda, seperti kata sandi dan kode OTP yang dikirim melalui SMS atau aplikasi *autentikator*. Autentikasi *multi-faktor* melibatkan penggunaan tiga atau lebih metode yang berbeda untuk mengkonfirmasi identitas pengguna (Bonneau, Herley, van Oorschot, & Stajano, 2012).

2.2.2 FIDO

Fast IDentity Online atau (FIDO) adalah standar terbuka yang dikembangkan oleh FIDO Alliance untuk menciptakan standar autentikasi tanpa password pada sistem berbasis web. Untuk mencapai standar ini digunakan teknologi *kriptografi asimetris*, *public key kriptografi* dan *digital signature*. FIDO Alliance sebagai pengembang standar autentikasi FIDO mengedepankan tiga aspek utama yaitu 1) Keamanan, 2) Kenyamanan, 3) Privasi, 4) Skalabilitas.

Tujuan utama adalah untuk membuat layanan berbasis web ataupun aplikasi baik untuk korporasi atau umum, untuk mendukung metode autentikasi yang aman, versi awal Fido memiliki 3 standar utama yaitu FIDO U2F, UAF dan FIDO2. (FIDO Alliance, 2022).

1. **FIDO Universal Second Factor** (FIDO U2F) menyediakan sarana standar untuk menghubungkan autentikator perangkat keras faktor kedua. Standar ini terutama digunakan oleh browser Web untuk memungkinkan aplikasi Web berinteraksi dengan autentikator perangkat keras pengguna. Standar U2F digunakan sebagai Autentikasi tambahan atau *second factor authentication*. Dengan dirilisnya FIDO2, U2F telah diubah namanya menjadi CTAP1

2. **FIDO Universal Authentication Framework (FIDO UAF)** mendefinisikan kerangka kerja bagi pengguna untuk mendaftarkan perangkat mereka (yaitu laptop, desktop, mobile) ke layanan online dan memilih salah satu mekanisme Autentikasi lokal yang tersedia di perangkat untuk mengautentikasi penggunanya. Layanan online dapat memilih mekanisme autentikasi yang tersedia secara lokal yang akan diterimanya. Misalnya, pengguna dapat mendaftarkan perangkat seluler mereka dan memilih sensor sidik jari yang tertanam sebagai sarana autentikasi lokal yang digunakan untuk mengautentikasi mereka ke layanan online.

2.2.3 FIDO2

FIDO2 adalah standar autentikasi terbaru hasil kerja sama antara Fido Alliance dan *World Wide Web Consortium* (W3C). Standar ini terdiri dari 2 komponen protokol yaitu *Webauthn* dan Ctap2 (FIDO Alliance, 2022)..

a. WebAuthn

WebAuthn adalah Api berbasis browser yang memungkinkan aplikasi web untuk menyederhanakan dan mengamankan autentikasi pengguna dengan menggunakan perangkat terdaftar (ponsel, laptop, dll) sebagai autentikasi faktor utama. *WebAuthn* memastikan hanya *host* terdaftar yang bisa mengakses kredensial sehingga melindungi pengguna dari serangan *phishing*.

b. CTAP2

CTAP1 adalah nama baru untuk FIDO U2F. Ini mendefinisikan cara membangun komunikasi antara browser dan sistem operasi yang mendukung FIDO2 dan perangkat FIDO U2F, untuk mengaktifkan pengalaman autentikasi faktor kedua. CTAP2 mendefinisikan cara membangun komunikasi antara browser dan sistem operasi yang mendukung FIDO2 dan *autentikator* eksternal (Kunci Keamanan FIDO, perangkat seluler) untuk mengaktifkan pengalaman autentikasi tanpa kata sandi (faktor utama), faktor kedua, atau multi-faktor.

Dalam mekanisme autentikasi menggunakan standar FIDO2 entitas yang terlibat dapat dibagi menjadi 3 yaitu

a. Server (Relaying Party)

Server umumnya berupa aplikasi web online. Pada saat proses registrasi, entitas server akan meregenerasi dan mengirimkan *data random challenge* ke aplikasi client yang meminta dan menerima *public* key yang akan digenerasikan oleh entitas authenticator dan dikirim kembali ke server. Pada saat proses autentikasi, browser akan membuat challenge dan dikirim ke aplikasi client dan di respon kembali ke server dengan *data random challenge* yang sudah di sign dengan *private key* yang dimiliki client. Server

dapat melanjutkan ke tahap selanjutnya seperti mengatur *cookie* atau *session* untuk aplikasi client.

b. Client (Webauthn)

FIDO client akan bertindak sebagai jembatan antara authenticator dengan server. Dengan menggunakan library Fido2ApiClient API yang telah dikembangkan untuk Android, Aplikasi native Android dapat berkomunikasi dengan entitas authenticator. Aplikasi Client akan meminta *data random challenge* dari entitas server kemudian akan mengirimkannya ke *authenticator* untuk meminta proses pembuatan *key pairs* untuk proses registrasi maupun meminta proses sign-the-*challenge* untuk proses autentikasi.

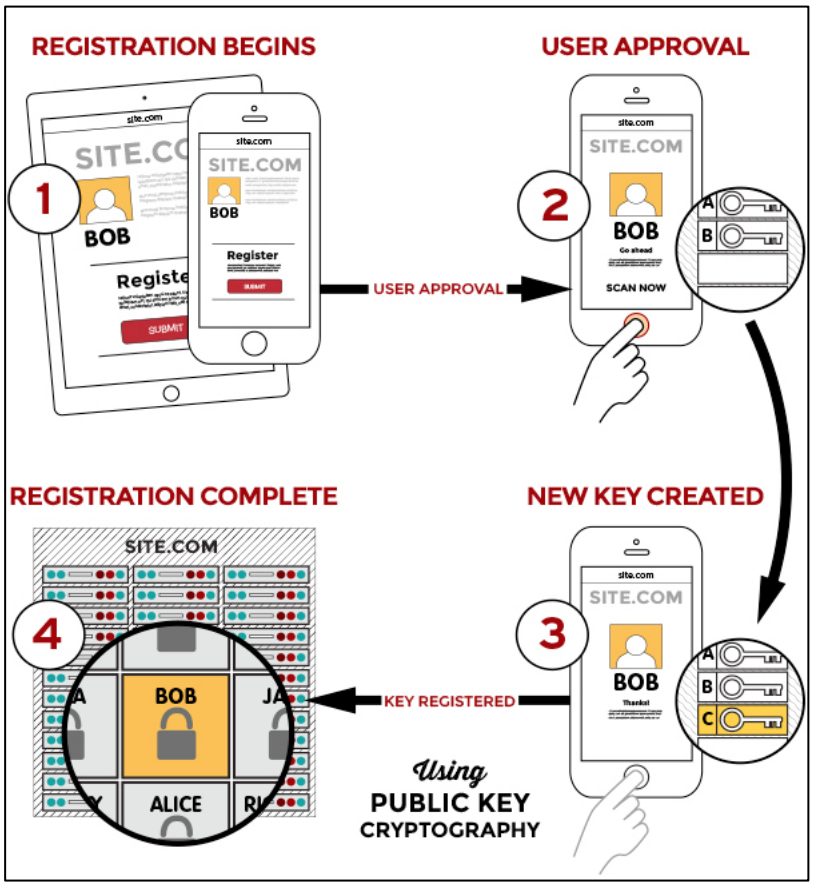
c. Authenticator

FIDO2 Authenticator bisa digunakan untuk external maupun internal *authenticator*. External *authenticator* bisa menggunakan USB Key seperti YubiKey yang dirancang secara khusus untuk autentikasi, external authenticator juga bisa menggunakan fitur roaming dengan QR Code dari device lain untuk proses autentikasi. Untuk Internal authenticator bisa menggunakan Platform authenticator yang tertanam secara native pada perangkat. Entitas Authenticator ini akan membuat *key pairs* dan *key handles* pada saat proses registrasi dan akan melakukan *sign-the-challenge* dengan *private key* pada saat proses autentikasi. Semua data tersebut akan dikirim ke client yang kemudian akan diteruskan ke server.

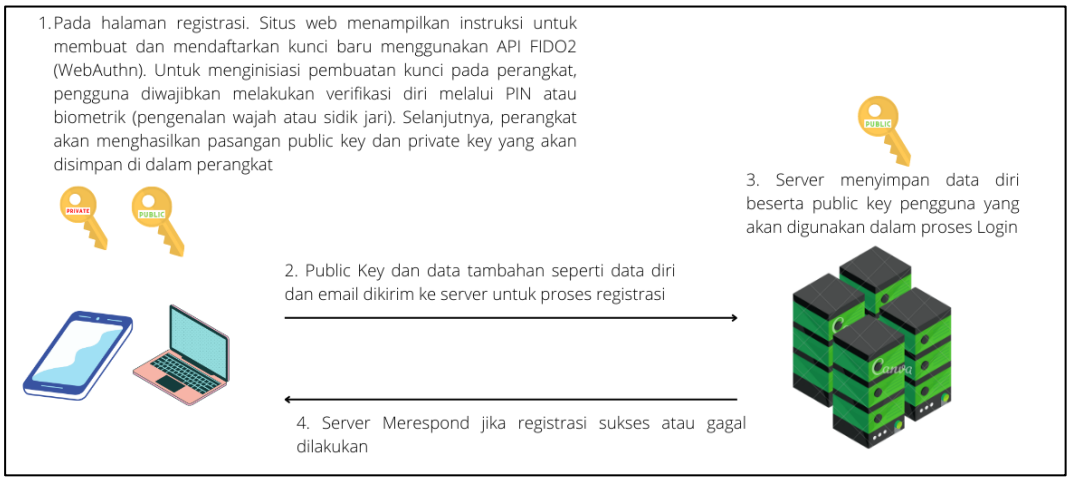
2.2.4 FIDO2 Passkey

FIDO2 Passkey lebih memfokuskan penggunaannya pada Platform Authenticator, yaitu teknologi yang menyimpan kunci enkripsi pada perangkat keras dan menyediakan metode otentikasi yang aman, cepat, dan mudah digunakan oleh pengguna. Dibandingkan dengan FIDO2 klasik atau kredensial perangkat tunggal, FIDO2 Passkey memberikan kemampuan bagi kredensial FIDO untuk dapat berpindah di antara beberapa perangkat yang dimiliki oleh pengguna. Dengan demikian, FIDO2 Passkey mengatasi kekurangan dari FIDO2 klasik yang hanya dapat digunakan pada satu perangkat saja, serta memberikan solusi atas masalah

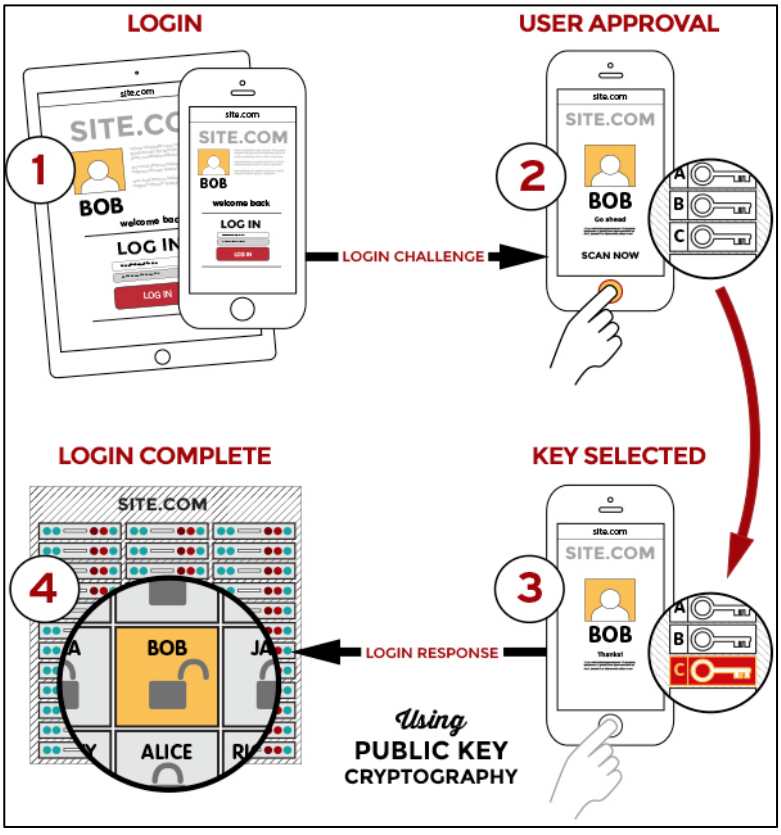
pemulihan dan pendaftaran ulang berkali-kali. Selain itu, FIDO2 Passkey memungkinkan sinkronisasi kunci enkripsi antara berbagai perangkat yang dimiliki oleh pengguna, sehingga pengguna tidak perlu memulai proses pendaftaran ulang dari awal setiap kali menggunakan perangkat yang berbeda. (FIDO Alliance, 2022).



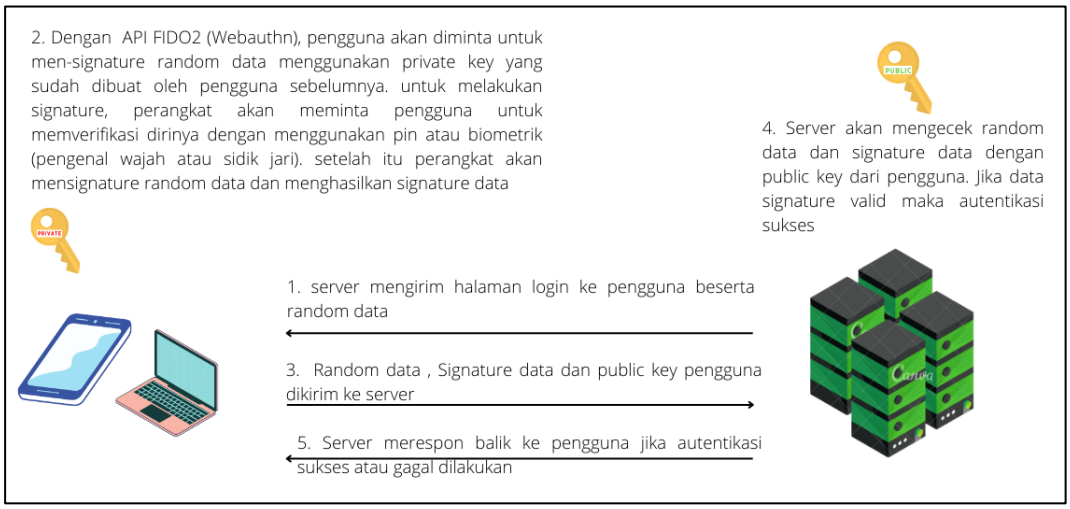
Gambar 2.1 Ringkas Proses Registrasi dengan metode FIDO2 Passkey



Gambar 2.2 Proses Registrasi dengan metode FIDO2 Passkey secara Mendetail



Gambar 2.3 Ringkas Proses Login dengan metode FIDO2 Passkey



Gambar 2.4 Proses Login dengan metode FIDO2 Passkey secara Mendetail

2.2.5 Elliptic Curve Digital Signature Algorithm (ECDSA)

Elliptic Curve Cryptography (ECC) adalah salah satu pendekatan dalam kriptografi kunci publik yang menawarkan keamanan yang lebih tinggi dengan ukuran kunci yang lebih kecil dibandingkan dengan metode tradisional seperti RSA. ECC didasarkan pada matematika kurva eliptik di atas bidang Galois, yang merupakan bidang yang terdiri dari elemen hingga (Barker, 2015). Keunggulan utama ECC adalah efisiensi penggunaan kunci: ukuran kunci yang lebih kecil memungkinkan kecepatan komputasi yang lebih cepat dan penggunaan memori yang lebih rendah, sambil tetap memberikan tingkat keamanan yang setara dengan kriptografi kunci publik yang lebih tradisional (Bos, Costello, & Naehrig, 2015).

Elliptic Curve Digital Signature Algorithm (ECDSA) adalah salah satu algoritma yang diterapkan dalam pembuatan tanda tangan digital yang menggunakan analogi kurva elips. ECDSA merupakan penggabungan algoritma Elliptic Curve Cryptography (ECC) dengan Digital Signature Algorithm (DSA). Tidak seperti logaritma diskrit biasa dan masalah faktorisasi integer, masalah logaritma diskrit kurva elips tidak mengenal algoritma perkalian sub-eksponensial. Karenanya, kekuatan per bit kunci algoritma yang menggunakan kurva elips lebih kuat secara substansial daripada algoritma biasa.

Penggabungan ECC dan ECDSA menjadi metode enkripsi kunci di FIDO2 Passkey memanfaatkan keamanan dan efisiensi dari ECC serta kekuatan tanda tangan digital dari ECDSA. Dalam FIDO2 Passkey, ECC digunakan untuk menghasilkan dan mengelola kunci publik dan kunci privat untuk autentikasi yang lebih aman dan efisien. ECDSA digunakan untuk membentuk tanda tangan digital yang digunakan dalam proses autentikasi FIDO2 Passkey untuk memverifikasi identitas pengguna secara andal dan aman.

2.2.6 RSA Digital Signature Algorithm

Rivest-Shamir-Adleman (RSA) merupakan salah satu algoritma kriptografi kunci publik yang paling awal dan terkenal yang digunakan dalam banyak aplikasi keamanan digital (Rivest, Shamir, & Adleman, 1978). RSA menggunakan matematika teori bilangan, terutama sifat-sifat bilangan prima dan perkalian modular, untuk menyediakan enkripsi, dekripsi, dan digital signature. Keamanan RSA terutama didasarkan pada kesulitan faktorisasi bilangan besar menjadi faktor prima, yang merupakan masalah komputasi yang sulit (Boneh, 1999).

RSA Digital Signature Algorithm adalah sebuah metode yang digunakan dalam kriptografi kunci publik untuk menyediakan tanda tangan digital berbasis algoritma RSA (Rivest, Shamir, & Adleman, 1978). Dalam RSA Digital Signature Algorithm, pengirim menggunakan kunci privat mereka untuk membuat tanda tangan digital pada pesan atau dokumen, dan penerima menggunakan kunci publik pengirim untuk memverifikasi keaslian tanda tangan tersebut (Boneh, 1999).

Penggabungan RSA dan RSA DSA menjadi metode enkripsi kunci di FIDO2 Passkey. Dalam FIDO2 Passkey, RSA digunakan untuk menghasilkan dan mengelola kunci publik dan kunci privat untuk autentikasi. RSA DSA digunakan untuk membentuk tanda tangan digital yang digunakan dalam proses autentikasi FIDO2 Passkey untuk memverifikasi identitas pengguna.

2.2.7 SHA256

SHA (Secure Hashing Algorithm) merupakan fungsi kriptografi yang dirancang khusus oleh penyedia otoritas keamanan internet untuk menjaga keamanan data. SHA ini bekerja dengan cara melakukan transformasi data menggunakan fungsi *Hash*. *Hash* merupakan algoritma yang terdiri dari operasi bitwise (ini berkaitan dengan fungsi besaran bit enkripsi), penambahan modular dan fungsi kompresi. Fungsi *Hash* akan menghasilkan fungsi acak yang tidak terlihat seperti aslinya. Fungsi *Hash* merupakan fungsi satu arah yang tidak dapat diubah menjadi nilai *Hash* masing-masing data tergantung tingkat bit enkripsi yang akan digunakan.

Salah satu fungsi *Hash* yang tersedia adalah SHA 256. SHA-256 adalah fungsi *Hash* dengan kapasitas terbaru dengan panjang 32-bit kata. Fungsi *Hash* ini dalam proses matematisnya menggunakan penjumlahan karakter yang berbeda dan ditambah dengan konstanta substansi (Panjaitan, 2020)

SHA256 berperan penting dalam menjamin keamanan dan integritas proses autentikasi FIDO2 Passkey. Fungsi hash ini digunakan untuk menghasilkan nilai hash dari kunci publik, tanda tangan digital, challenge, dan response dalam proses registrasi dan autentikasi. Dengan menggunakan SHA256, autentikasi FIDO2 dapat mengamankan data dan memastikan bahwa tanda tangan digital yang dihasilkan adalah autentik dan tidak dapat dipalsukan

BAB III METODOLOGI PENELITIAN

3.1 JENIS PENELITIAN

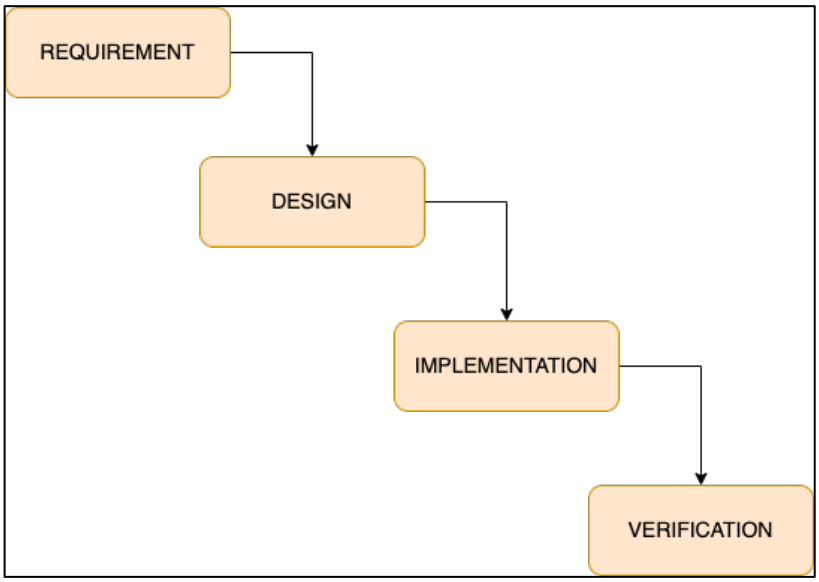
Penelitian yang dilakukan adalah berjenis *Research & Development* (R&D). R&D adalah metode penelitian yang melalui proses pengembangan dan pembuatan produk baru atau inovasi untuk menghasilkan produk tertentu dan menguji keefektifannya. Pada penelitian ini bertujuan untuk mengembangkan sebuah sebuah fitur autentikasi tanpa *password* pada sistem SSO Undiksha dengan menggunakan teknologi FIDO2 Passkey

3.2 TAHAPAN PENELITIAN

Tahapan penelitian ini mengadopsi tahapan dari metode *Software Development Life Cycle* (SLDC) model *Waterfall*. SDLC model *Waterfall* merupakan metode pengembangan sistem atau *software* yang mengikuti pendekatan yang berurutan dan sistematis secara linear dalam pengembangan perangkat lunak. Prinsipnya adalah menyelesaikan fase terlebih dahulu sebelum beranjak ke fase berikutnya. Tahapan model *waterfall* antara lain adalah *requirement analysis*, *design*, *implementation*, *verification*, dan *maintenance* (Wahid, 2020).

1. *Requirement Analysis* (Perencanaan), merupakan proses mengumpulkan, menganalisis, dan mengklarifikasi kebutuhan dari pengguna atau klien. Hasil dari fase ini adalah solusi atau spesifikasi yang menjelaskan kebutuhan sistem yang akan dikembangkan.
2. *Design* (Desain), adalah fase menentukan arsitektur, komponen, dan detail teknis dari sistem yang akan dikembangkan. Hasil dari fase ini adalah desain sistem yang menjelaskan bagaimana sistem akan terlihat dan bekerja.
3. *Implementation* (Implementasi), merupakan fase pengimplementasian hasil rancangan dari fase sebelumnya dengan cara menulis kode sistem sesuai dengan desain yang telah dibuat.

4. *Verification* (Verifikasi/Pengujian), merupakan tahap melakukan pengujian sistem untuk memastikan bahwa sistem bekerja sesuai dengan spesifikasi yang ditentukan.



Gambar 3.1 Siklus SDLC Model Waterfall

3.2.1 Tahap Requirement Analysis

Tahap *requirement analysis* atau perencanaan adalah awal dalam model SDLC *Waterfall* yang digunakan untuk mengumpulkan, menganalisis, dan mengklarifikasi kebutuhan dari pengguna atau klien. Tujuan dari fase ini adalah untuk menentukan apa yang diinginkan oleh pengguna dari sistem yang akan dikembangkan, dan bagaimana sistem tersebut akan memenuhi kebutuhan tersebut. Tahap perencanaan dimulai dengan mengumpulkan data dan informasi terkait permasalahan yang diteliti, dalam hal ini peneliti dapat mengetahui kebutuhan sistem dari pengguna yang harus dipenuhi. Selanjutnya peneliti melakukan Analisis kebutuhan dengan wawancara terhadap narasumber terkait dan observasi secara langsung dan mempelajari teori yang berkaitan dengan ruang lingkup penelitian.

Tahap perencanaan terbagi menjadi dua fase, yakni fase analisis masalah dan solusi dan analisis kebutuhan sistem. Analisis masalah dan solusi dilakukan dengan wawancara ke pihak UPT TIK Undiksha mengenai sistem SSO Undiksha untuk mengetahui masalah dan mencari solusi dari permasalahan tersebut.

Sedangkan analisis kebutuhan sistem adalah analisis terhadap spesifikasi dari sistem yang akan dibuat untuk mengatasi masalah yang ditemukan.

3.2.1.1 Analisis Masalah dan Solusi

Berdasarkan analisis dari permasalahan yang telah ditemukan pada sistem autentikasi SSO Undiksha dan pada penggunaan Password secara umumnya, masih terdapat masalah sebagai berikut.

1. Kelalian pengguna membagikan password ke orang lain. Kekurangan dari metode autentikasi berbasis password adalah pengguna cenderung mudah membagikan password mereka kepada orang lain yang mengakibatkan akun diakses secara tidak sah oleh orang lain.
2. Akun rawan terkena *phising* dan peretasan akun, autentikasi menggunakan password dan username sangat mudah untuk terkena *phising* sehingga perlu adanya metode yang lebih kuat untuk menghindari kemungkinan terjadi peretasan dari *phising*.
3. Kurang *nyaman*, autentikasi dengan metode password dan username kurang nyaman karena untuk membuat password yang kuat pengguna perlu membuat password yang unik dan panjang, password kuat adalah password yang susah untuk diingat

Berdasarkan analisis masalah di atas, maka solusi yang dapat diusulkan adalah sebuah sistem autentikasi tanpa password menggunakan FIDO2 Passkey. Sistem yang dikembangkan ini diharapkan dapat menangani permasalahan yang telah disebutkan sebelumnya. Berikut adalah solusi yang ditawarkan dari sistem yang akan dikembangkan.

1. FIDO2 Passkey memanfaatkan kriptografi asimetris sebagai landasan mekanisme autentikasi, di mana kunci disimpan dalam perangkat yang tidak dapat diakses atau disalin secara langsung. Kunci ini hanya dapat digunakan untuk proses autentikasi. Dengan demikian, pengguna tidak dapat secara sembarangan membagikan kunci mereka kepada pihak lain, sehingga meningkatkan keamanan sistem.

2. Teknologi FIDO2 Passkey dapat mengatasi masalah peretasan akun dengan *phising* karena menggunakan metode autentikasi ini memaksa browser hanya menerima permintaan autentikasi dari alamat domain yang sama dengan yang *user* gunakan untuk mendaftar. Jika alamat domain website meminta kunci berbeda maka browser akan menolak untuk melakukan autentikasi, hal ini sangat membantu untuk mengurangi *phising* bagi pengguna yang tidak begitu paham dan mengerti mengenai pencegahan *phising*
3. FIDO2 Passkey memungkinkan pengguna tidak lagi harus mengingat dan mengelola kata sandi untuk masuk ke sistem SSO Undiksha. Sebagai gantinya, dapat menggunakan metode autentikasi lain yang lebih mudah seperti Biometrik atau PIN sehingga lebih *user friendly*

3.2.1.2 Analisis Kebutuhan Sistem

Dalam mengembangkan sistem autentikasi FIDO2 pada SSO Undiksha untuk mengatasi masalah yang telah dijelaskan sebelumnya didapatkan spesifikasi dalam kebutuhan sistem. Analisis kebutuhan sistem dibagi menjadi tiga bagian, yakni analisis pengguna, analisis fungsional, dan analisis non-fungsional.

1. Analisis Pengguna

   Analisis pengguna dilakukan untuk mengidentifikasi calon pengguna atau orang yang akan menggunakan sistem. Berikut adalah aktor atau pengguna yang terlibat dan memiliki akses untuk menggunakan sistem autentikasi FIDO2 SSO Undiksha seperti yang terlihat pada Tabel 3.1.

Tabel 3.1 Analisis Pengguna

Pengguna	**Keterangan**
Dosen	Dosen Undiksha adalah pengguna yang memiliki keperluan untuk mengakses siak, e-learning dan sistem dosen lainnya menggunakan SSO sebagai sistem autentikasi

Pegawai	Pegawai Undiksha adalah pengguna yang memiliki keperluan untuk mengakses data kepegawaian dan sistem lainnya yang menggunakan SSO Undiksha sebagai sistem autentikasi
Mahasiswa	Mahasiswa Undiksha adalah pengguna yang memiliki keperluan akses untuk siak, *e-learning*, dan *service* lainnya pada SSO Undiksha.

2. Analisis Fungsional

Analisis fungsional dilakukan mengidentifikasi kebutuhan yang berisi proses-proses apa saja yang nantinya dapat dilakukan oleh sistem. Proses dirinci pada setiap hak akses pengguna, secara lengkap terlihat pada tabel 3.2.

Tabel 3.2 Kebutuhan Fungsional Sistem

Kode	**Pengguna**	**Keterangan**
F-1	Dosen, Pegawai dan Mahasiswa Undiksha	Sistem mampu memberikan akses untuk melakukan opsi Registrasi menggunakan sistem autentikasi FIDO2 Passkey. Dimana Pengguna akan di suruh untuk menggunakan Biometrik atau PIN Ketika proses registrasi
F-2	Dosen, Pegawai dan Mahasiswa Undiksha	Sistem mampu memberikan akses untuk melakukan opsi Masuk ke Sistem(Login) menggunakan metode FIDO2 Passkey pada Perangkat yang sebelumnya digunakan untuk registrasi. Pengguna akan disuruh untuk memverifikasi Login ke sistem dengan memverifikasi biometric atau memasukkan PIN pada perangkat mereka

F-3	Dosen, Pegawai dan Mahasiswa Undiksha	Sistem mampu memberikan akses untuk melakukan opsi Masuk ke Sistem(Login) menggunakan metode FIDO2 Passkey pada Perangkat yang sebelumnya tidak pernah digunakan untuk registrasi memanfaatkan metode *Roaming*. Pengguna akan disuruh untuk memverifikasi Login ke sistem dengan Memindai Kode QR pada browser dengan perangkat yang sebelumnya sudah pernah diregistrasi dengan FIDO2 Passkey

3. Analisis Non-fungsional

Analisis non-fungsional dilakukan untuk mengidentifikasi kebutuhan sistem yang tidak spesifik pada suatu *user* seperti tampilan, kinerja, atau karakteristik sistem secara keseluruhan.

Tabel 3.3 Kebutuhan Non-fungsional Sistem

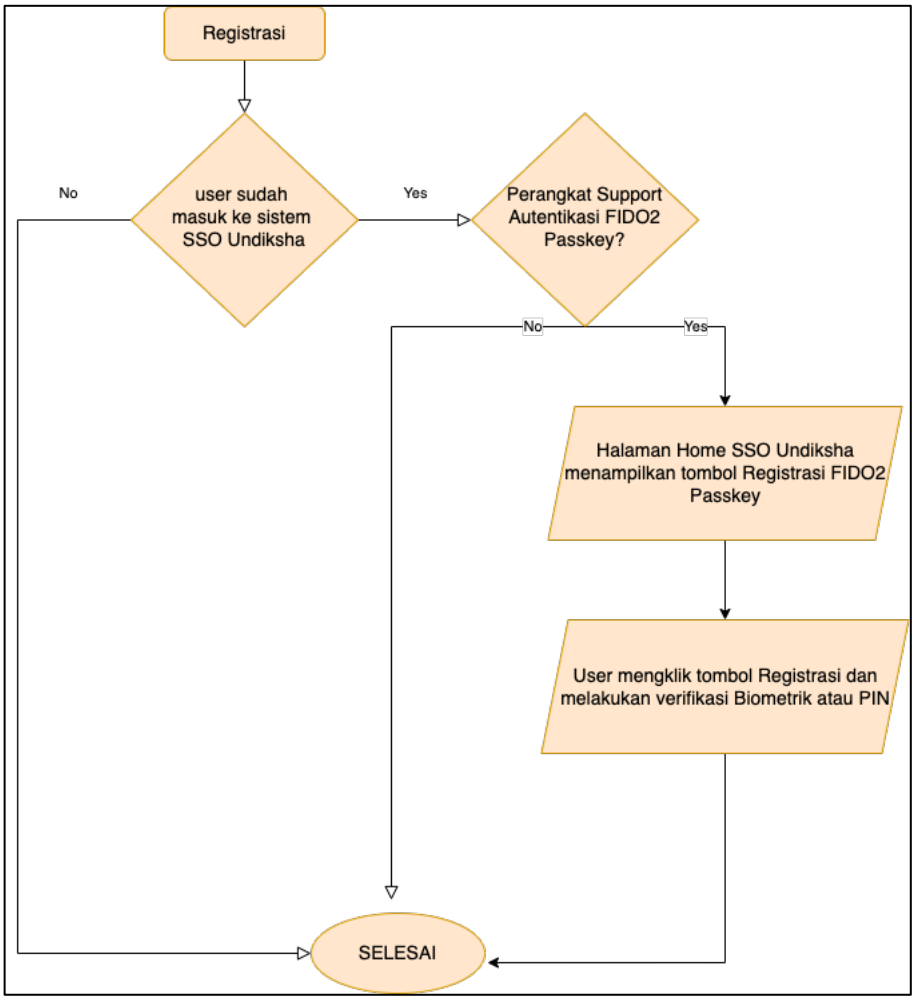
Kode	**Keterangan**
NF-1	Sistem memiliki *user interface* yang mudah digunakan.
NF-2	Sistem bersifat *responsive* dan dapat digunakan pada platform *desktop*, *tab*, dan *mobile*.

3.2.2 Tahap Design

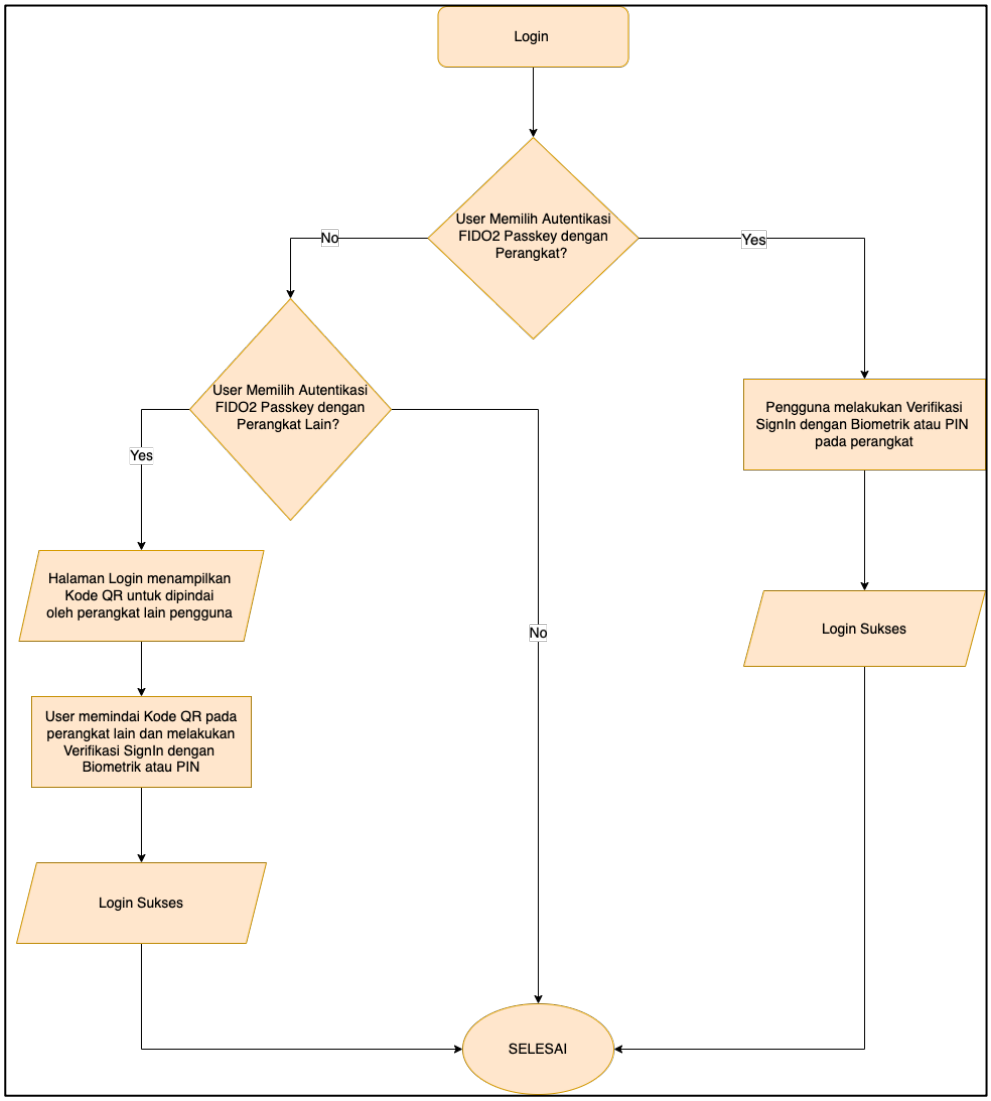
Tahap selanjutnya adalah desain, di mana peneliti menentukan arsitektur, komponen, dan detail teknis dari sistem yang akan dikembangkan. Tujuan dari fase ini adalah untuk menentukan bagaimana sistem akan terlihat dan bekerja sebelum dimulai proses implementasi. Fase ini menjelaskan tahap rancangan diagram alir sistem, rancangan basis data, dan rancangan tampilan antar pengguna. Rancangan bagaimana fitur autentikasi akan dikembangkan dijelaskan secara terperinci pada tahapan ini.

3.2.2.1 Rancangan Diagram Alir (*Flowchart*) Sistem

Flowchart atau diagram alir digunakan untuk mewakili algoritma, alur kerja, atau proses dalam sistem. Ini terdiri dari serangkaian bentuk yang dihubungkan dengan garis atau panah, dan setiap bentuk mewakili langkah dalam proses. *Flowchart* dari sistem terlihat pada Gambar 3.2.



Gambar 3.2 Flowchart Registrasi Sistem

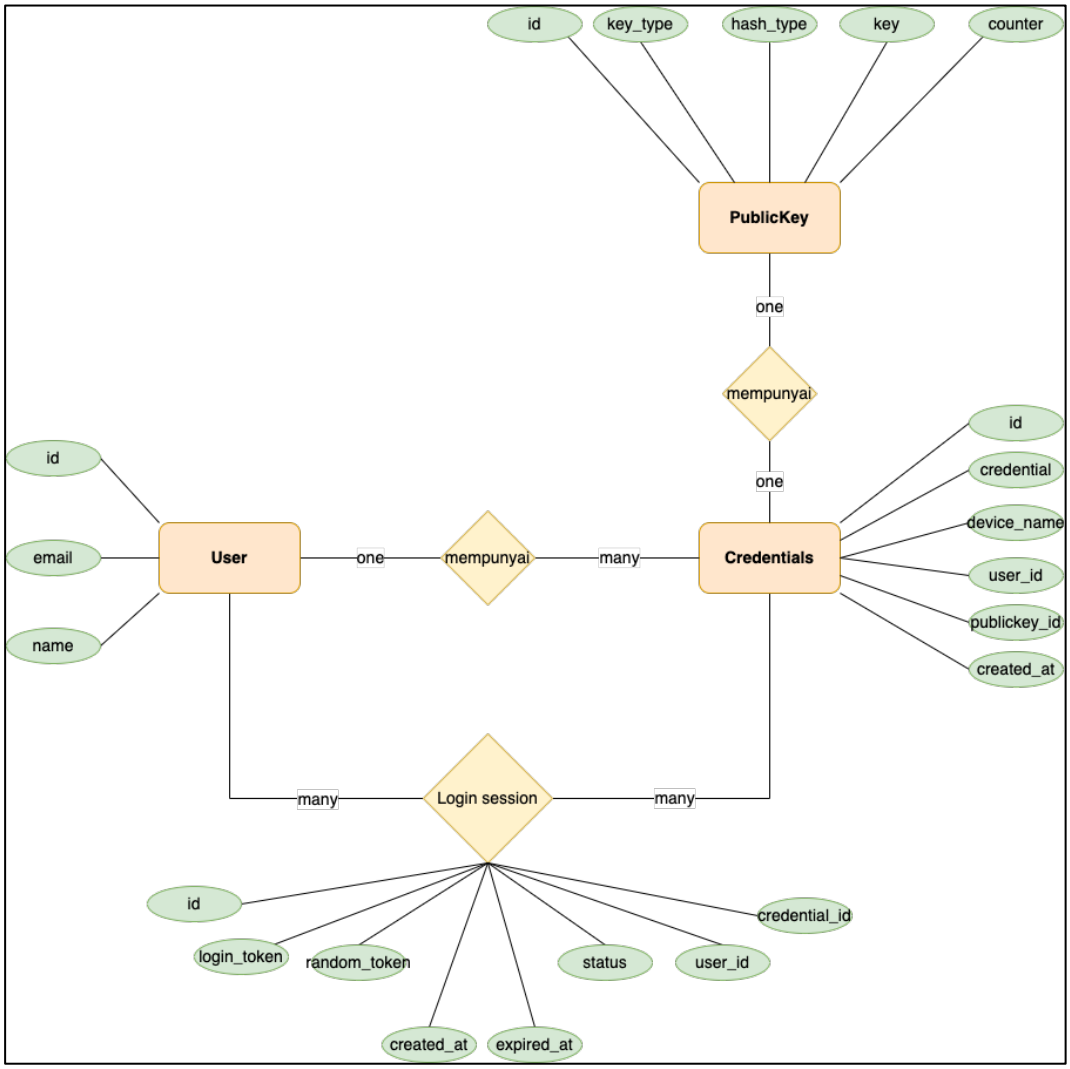


Gambar 3.3 Flowchart Login ke Sistem

3.2.2.2 Rancangan Basis Data Sistem

Rancangan basis data digunakan untuk proses pembuatan rencana terstruktur tentang bagaimana basis data akan diatur dan digunakan. Ini melibatkan penentuan data yang akan disimpan dalam basis data, serta hubungan antara bagian data yang berbeda. Proses desain juga termasuk menentukan cara yang paling efisien untuk relasi antar tabel data.

Tujuan dari perancangan basis data adalah untuk membuat basis data yang efisien, mudah digunakan, dan mampu memenuhi kebutuhan sistem. Rancangan basis data terlihat pada Gambar 3.4

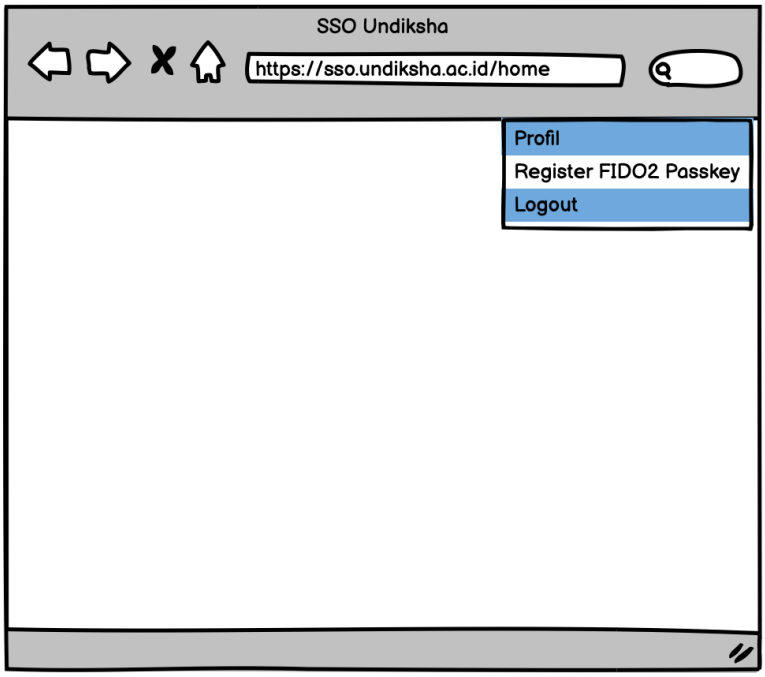


Gambar 3.4 Rancangan Basis Data

3.2.2.3 Rancangan User Interface Sistem

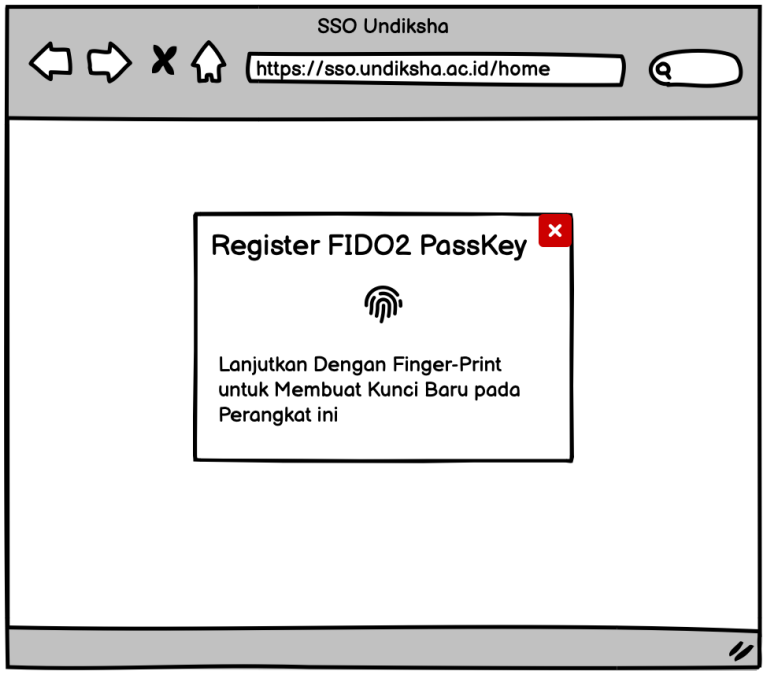
Rancangan *User Interface* dilakukan untuk memberikan gambaran tampilan aplikasi pada sistem yang akan dikembangkan. Rancangan aplikasi ini adalah sebagai berikut.

1. Rancangan *Interface* Registrasi FIDO2 Passkey pada *Homepage* SSO Undiksha



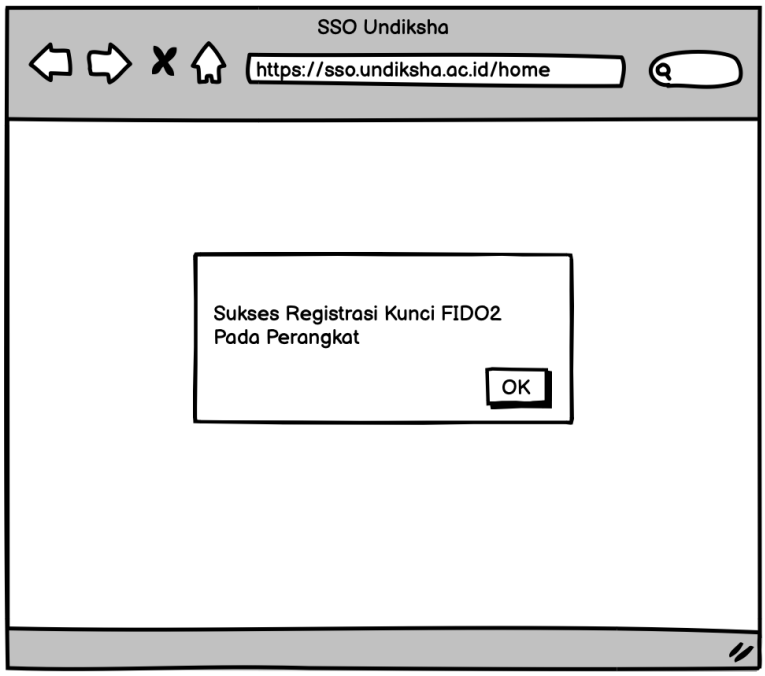
Gambar 3.5 Homepage SSO Undiksha

2. Rancangan *Interface* proses Registrasi FIDO2 Passkey menggunakan Biometrik atau Pin



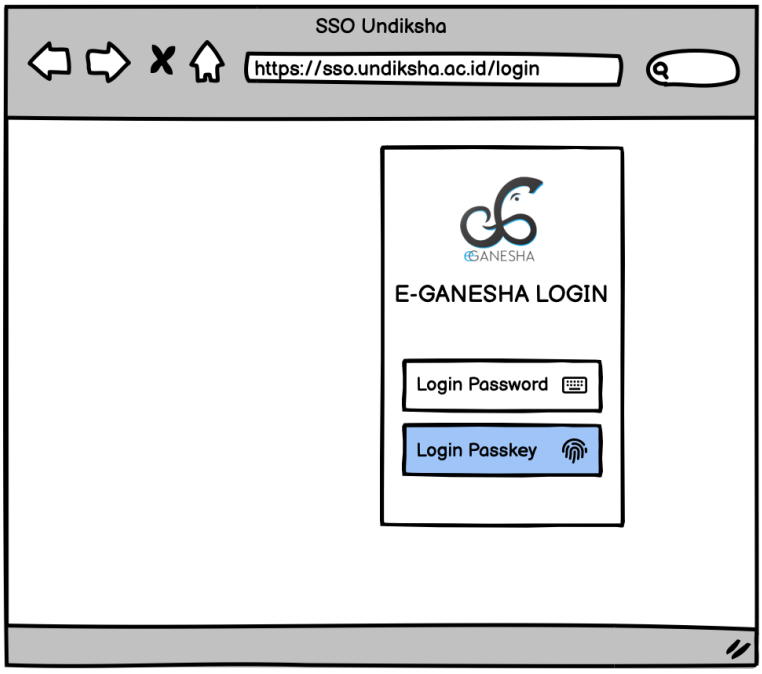
Gambar 3.6 Penggunaan Biometrik atau Pin

3. Rancangan *Interface* Pesan Sukses setelah berhasil melakukan Registrasi FIDO2 Passkey



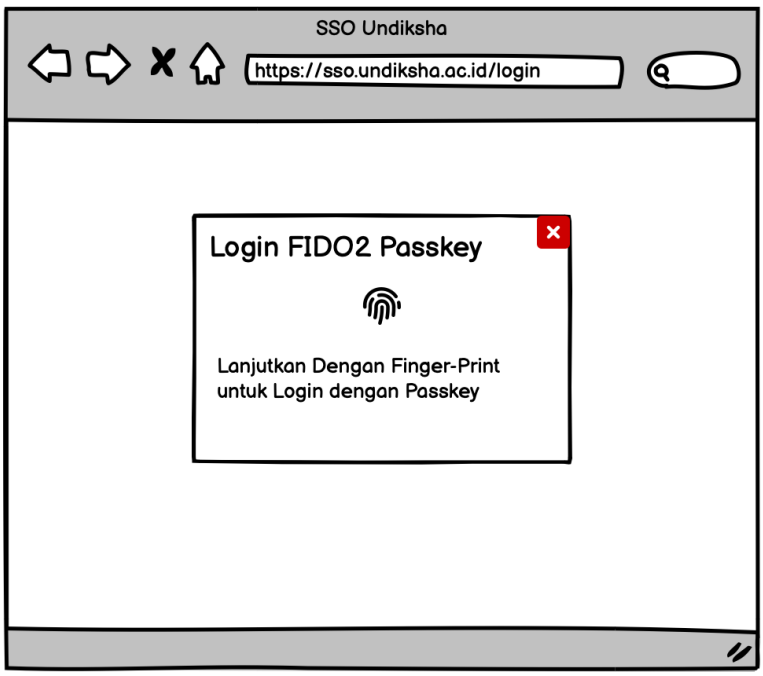
Gambar 3.7 Pesan Sukses Registrasi FIDO2 Passkey

4. Rancangan *Interface* Halaman Login SSO Undiksha dengan tambahan metode Login dengan FIDO2 Passkey



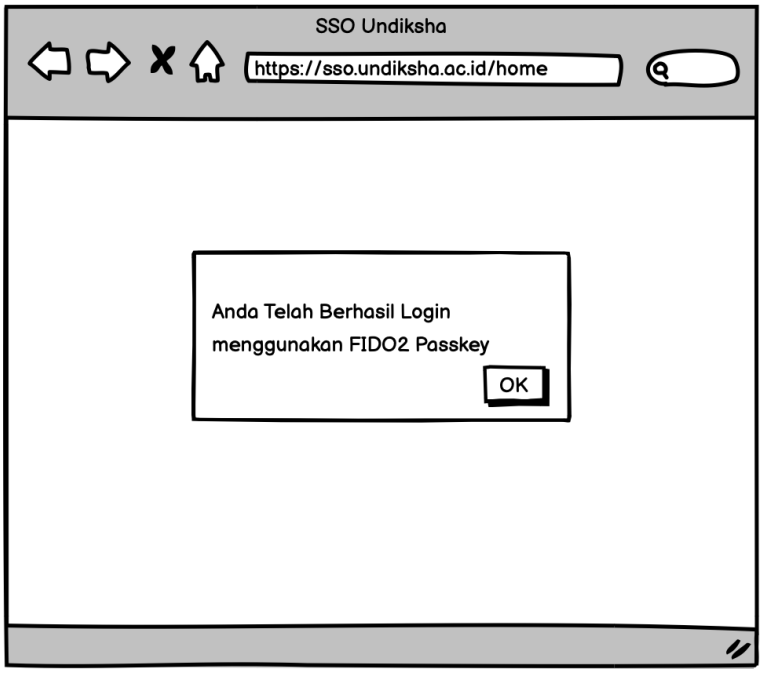
Gambar 3.8 Halaman Login SSO Undiksha dengan FIDO2 Passkey

5. Rancangan *Interface* Proses Login menggunakan metode Login dengan FIDO2 Passkey



Gambar 3.9 Proses Login menggunakan FIDO2 Passkey

6. Rancangan *Interface* Proses Berhasil Login dengan metode FIDO2 Passkey



Gambar 3.10 Login Berhasil dengan metode FIDO2 Passkey

3.2.3 Tahap Implementation

Rancangan dari tahap desain kemudian akan diimplementasikan dalam tahap implementasi. Pada tahapan ini, rancangan seperti basis data akan diimplementasikan langsung ke dalam sistem manajemen basis data Mysql, dan rancangan tampilan antarmuka pengguna akan diprogram menjadi halaman web. Untuk sistem SSO Undiksha, tampilan antarmuka fitur autentikasi web akan dikembangkan menggunakan bahasa HTML, CSS, dan Javascript. Selanjutnya, metode autentikasi FIDO2 Passkey akan memanfaatkan Webauthn API pada browser untuk berkomunikasi dengan FIDO2 Platform Authenticator yang tertanam pada perangkat pengguna. Pada bagian server, bahasa pemrograman PHP akan digunakan untuk mengimplementasikan proses registrasi, login, dan enkripsi kunci dari pengguna sistem. Fase implementasi ini merupakan tahap nyata dalam mengimplementasikan fitur atau sistem yang telah dirancang atau dikembangkan

3.2.4 Tahap Verification

Tahap selanjutnya adalah melakukan pengujian terhadap fitur yang telah dibuat, untuk memastikan bahwa fitur bekerja sesuai dengan spesifikasi yang ditentukan. Tujuannya adalah untuk menemukan dan memperbaiki kesalahan atau *bug* dalam fitur dan mengetahui respon dari pengguna tentang fitur yang dikembangkan sebelum bisa dipertimbangkan untuk di implementasikan dan di rilis sebagai fitur baru di pada SSO Undiksha. Dilakukan 3 Jenis Pengujian yakni *black box testing*, *white box testing dan tes usability*.

3.2.4.1 *Black Box Testing*

Pengujian Black Box, juga dikenal sebagai pengujian fungsional atau pengujian spesifikasi, adalah metode pengujian yang menguji perangkat lunak tanpa mengetahui struktur internal atau kode programnya (Beizer, 1995). Pengujian ini berfokus pada input dan output yang dihasilkan oleh perangkat lunak, serta fungsi yang diharapkan untuk dilakukan oleh sistem. Pengujian Black Box memastikan bahwa sistem bekerja sesuai dengan spesifikasi dan memenuhi kebutuhan pengguna, tanpa memerlukan pengetahuan tentang bagaimana sistem tersebut diimplementasikan.

Pengujian *black box* untuk autentikasi FIDO2 akan melibatkan pengujian fungsionalitas proses autentikasi tanpa mengetahui cara kerja internal atau protokol FIDO2. Fokusnya adalah pada pengujian interaksi pengguna dengan sistem, seperti mendaftarkan akun, melakukan autentikasi, dan memverifikasi bahwa autentikasi berhasil.

Adapun rancangan pengujian fungsionalitas atau blackbox testing dapat dilihat pada lampiran 2.

Selanjutnya untuk mengetahui hasil uji fungsional atau blackbox testing yang dilakukan sebagai berikut.

$$blackbox\ (\%) = \frac{\sum data\ uji\ benar}{\sum total\ data\ uji}\ x\ 100$$

3.2.4.2 *White Box Testing*

Pengujian White Box, juga dikenal sebagai pengujian struktur atau pengujian kaca transparan, adalah metode pengujian yang melibatkan analisis dan pemeriksaan struktur internal dan kode program perangkat lunak (Myers, 1979). Berbeda dengan pengujian Black Box yang hanya mengamati input dan output, pengujian White Box berfokus pada aliran data antara input dan output dalam perangkat lunak. Metode ini memungkinkan pengujian lebih mendalam untuk memastikan kualitas kode dan untuk mengidentifikasi kesalahan atau kekurangan dalam struktur kode.

Proses pengujian dilakukan dengan Langkah-langkah sebagai berikut

1. Membuat Flow Graph
2. Menghitung Cyclomatic Complexity
3. Menunjukan Independent Path dari basis path testing

Adapun perangcangan pengujian konseptual atau whitebox testing dapat dilihat pada lampiran 4.

Selanjutnya untuk mengetahui hasil uji pengujian konseptual atau whitebox testing dapal dilakukan sebagai berikut.

$$whitebox\ (\%) = \frac{\sum data\ uji\ benar}{\sum total\ data\ uji}\ x\ 100$$

3.2.4.3 Tes Usability

Tes usability merupakan suatu metode evaluasi yang digunakan untuk mengevaluasi sejauh mana sebuah sistem atau produk dapat digunakan dengan efektif, efisien, dan memuaskan oleh pengguna. Pada penelitian ini, tes usability dilakukan untuk mengevaluasi fitur autentikasi tanpa password pada SSO Undiksha dengan teknologi FIDO2 Passkey. Metode yang akan digunakan adalah metode pengujian pengguna.

Metode pengujian pengguna dilakukan dengan merekrut sejumlah responden pengguna (minimal lima orang) yang mewakili demografi dan karakteristik pengguna sistem SSO Undiksha. Peneliti akan menggunakan masing-masing 5 sample pengguna untuk setiap demografi pengguna SSO Undiksha sebagai responden Sehingga total responden yang akan digunakan dalam pengujian ini adalah 15 responden yang diambil dari 5 Mahasiswa, 5 Pegawai dan 5 Dosen. Pengujian pengguna dilakukan dengan memberikan tugas-tugas yang mencakup aspek sistem autentikasi, proses registrasi dan login. Selama proses pengujian, pengamat mengamati bagaimana responden menyelesaikan tugas tersebut, mencatat kesulitan apa pun yang mereka hadapi, dan berapa waktu yang dibutuhkan untuk menyelesaikan tugas.

Penelitian ini menggunakan jumlah responden yang cukup minimal, yaitu lima orang untuk mewakili setiap demografi pengguna. Hal ini didukung oleh penjelasan dari Jakob Nielsen, seorang ahli usabilitas terkenal, yang menyatakan bahwa menggunakan lima responden dalam pengujian pengguna sudah cukup untuk menemukan masalah-masalah utama yang ada dalam sebuah sistem. Nielsen juga menambahkan bahwa pengujian pengguna dengan lebih dari lima responden tidak akan memberikan hasil yang signifikan dalam temuan usabilitas dan akan menambah biaya serta waktu pengujian (Nielsen, J., 2000). Dengan penggunaan masing-masing 5 sample pengguna yang mewakili demografi sistem diharapkan dapat membantu dalam mengoptimalkan usabilitas sistem autentikasi tanpa password pada SSO Undiksha

Adapun untuk mengetahui hasil masing-masing uji Pengujian pengguna yang dilakukan kepada 3 demografi pengguna yang berbeda yaitu Dosen, Pegawai, dan Mahasiswa yang dilakukan sebagai berikut.

$$F = \frac{total\ skor}{(skor\ tertinggi * n)}\ x\ 100$$

Keterangan:

F = hasil skor per demografi pengguna

n = Jumlah Responded per demografi pengguna

Metode yang digunakan adalah dengan mencari interval (rentang jarak) dan interpretasi persen untuk mengetahui penilaian dengan mencari Interval skor persen (I).

Rumus interval skor (I)

$$I = \frac{100}{jumlah\ skor(likert)}$$

maka

$$I = \frac{100}{4} = 25$$

Hasil I=25, yang artinya adalah masing-masing interval jarak dari yang terendah 0% hingga yang tertinggi 100% adalah 25. Maka dapat dibuatkan ke dalam tabel interval interpretasi skor berdasarkan interval pada table dibawah

Tabel 3.4 Interval Interpretasi Skor

Persentase	Kategori
0% - 24,9%	Sangat Buruk
25% - 49,9%	Kurang Baik
50% - 74,9%	Baik
75% - 100%	Sangat Baik

3.3 JADWAL PENELITIAN

No	Kegiatan	Waktu Kegiatan (Februari – Juli 2023)																							
		Mei				Juni				Juli				Agustus				September				Oktober			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Penyusunan Proposal	■	■	■	■	■	■																		
2	Seminar Proposal							■																	
3	Revisi Proposal								■	■	■	■	■	■											
4	Pembuatan Produk dan Penyelesaian Skripsi														■	■	■	■	■						
5	Ujian Skripsi																		■						

6	Revisi																					

DAFTAR PUSTAKA

Rivest, R. L., Shamir, A., & Adleman, L. (1978). *"A method for obtaining digital signatures and public-key cryptosystems". Communications of the ACM*, Volume 21, Nomor 2, (hlm.120-126). DOI: 10.1145/359340.359342

Myers, G. J. 1979. *The Art of Software Testing*. John Wiley & Sons, Inc.

Lampson, B., Abadi, M., Burrows, M., & Wobber, E. (1992). *"Authentication in Distributed Systems: Theory and Practice". ACM Transactions on Computer Systems*, Volume 10, Nomor 4, (hlm.265-310). DOI: 10.1145/138873.138874

Beizer, B. 1995. *Black-Box Testing: Techniques for Functional Testing of Software and Systems*. John Wiley & Sons, Inc.

Boneh, D. (1999). *"Twenty years of attacks on the RSA cryptosystem". Notices of the AMS,* Volume 46, Nomor 2, (hlm.203-213). http://www.ams.org/notices/199902/boneh.pdf

Nielsen, J. 2000. *"Why You Only Need to Test with 5 Users".* Tersedia pada https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/ (diakses pada 5 April 2023)

Triwinarko, Andy. (2005). *"Elliptic Curve Digital Signature Algorithm (ECDSA)". Departemen Teknik Informatika ITB*.

Sulianta, Feri. 2009. *Teknik Mengoptimalkan Password*. Jakarta: PT Elex Media Komputindo

Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). *"The Quest to Replace Passwords: A framework for Comparative Evaluation of Web*

Authentication Schemes". 2012 IEEE Symposium on Security and Privacy, (hlm.553-567). DOI: 10.1109/SP.2012.44

Bonneau, J., Herley, C., Oorschout, P. C. V., & Stajano, F. (2015). "*Passwords and the Evolution of Imperfect Authentication". Communications of the ACM*. Volume 58, Nomor 7, (hlm.78–87). DOI:10.1145/2699390

Barker, E. (2015). *"Recommendation for Key Management - Part 1: General". NIST Special Publication 800-57 Part 1 Revision 4.* DOI: 10.6028/NIST.SP.800-57pt1r4

Bos, J. W., Costello, C., & Naehrig, M. 2015. *"Exponentiating in Pairing Groups. Cryptology ePrint Archive, Report 2015/247".* Tersedia pada https://eprint.iacr.org/2015/247 (diakses pada 10 Januari 2023)

Bos, J. W., Costello, C., & Naehrig, M. 2015. *"Exponentiating in Pairing Groups. Cryptology ePrint Archive, Report 2015/247".* Tersedia pada https://eprint.iacr.org/2015/247 (diakses pada 10 Januari 2023)

Chanda, Katha. (2016). *"Password Security: An Analysis of Password Strengths and Vulnerabilities". I. J. Computer Network and Information Security*, Volume 7, (hlm.23-30). DOI: 10.5815/ijcnis.2016.07.04

IBM. 2019. *"FIDO2: The future of passwordless authentication".* Tersedia pada https://www.ibm.com/blogs/security/fido2-passwordless-authentication/ (diakses pada 5 Januari 2023)

Sivaprasad, R., & Sivasubramanian, S. (2020). *"A survey on OTP-based two-factor authentication schemes for securing IoT devices". International Journal of Communication Systems*, Volume 33, Nomor 3. DOI:10.1002/dac.4223

F. Alqubaisi, A. S. Wazan, L. Ahmad & D. W. Chadwick. (2020). *"Should We Rush to Implement Password-less Single Factor FIDO2 based Authentication?". 12th Annual Undergraduate Research Conference on Applied Computing (URC),* (hlm.1-6). DOI: 10.1109/URC49805.2020.9099190

S. Ghorbani Lyastani, M. Schilling, M. Neumayr, M. Backes and S. Bugiel. (2020). *"Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication". IEEE Symposium on Security and Privacy (SP),* (hlm.268-285). DOI: 10.1109/SP40000.2020.00047

Panjaitan, Zaimah, Erika Fahmi Ginting, and Yusnidah Yusnidah. (2020). *"Modifikasi SHA-256 Dengan Algoritma Hill Cipher Untuk Pengamanan Fungsi Hash Dari Upaya Decode Hash." Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika Dan Komputer),* Volume 19, Nomor 1, (hlm.53). DOI: 10.53513/jis.v19i1.225

Wahid, Aceng Abdul. (2020). *"Analisis Metode Waterfall Untuk Pengembangan Sistem Informasi". Jurnal Ilmu-Ilmu Informatika Dan Manajemen STMIK, November*, 1–5.

Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia. 2022. *" Sistem Pemerintahan Berbasis Elektronik (SPBE)".* Tersedia pada https://www.menpan.go.id/site/kelembagaan/sistem-pemerintahan-berbasis-elektronik-spbe-2 (diakses pada 10 Januari 2023)

Badan Siber dan Sandi Negara. 2022. *"Laporan Hasil Monitoring Keamanan Siber Tahun 2022"*. Tersedia pada https://cloud.bssn.go.id/s/GfpcGJNQqSZRgDE (diakses pada 10 April 2023)

FIDO Alliance. 2022. *"DO Authentication A Passwordless Vision (2022)"*. Tersedia pada https://fidoalliance.org/fido2/ (diakses pada 10 April 2023)

Würsching, L., Putz, F., Haesler, S., & Hollick, M. (2023). "*FIDO2 the Rescue? Platform vs. Roaming Authentication on Smartphones*". *In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems,* (hlm. 1-16). DOI: 10.1145/3544548.3580993

LAMPIRAN

Lampiran 1 Dokumentasi

Gambar. Observasi dan Wawancara Awal di Unit Pelaksana Teknis Teknologi, Informasi dan Komunikasi UPT-TIK UNDIKSHA dengan Bapak I Ketut Resika Arthana, S.T., M.Kom selaku Kepala UPT TIK UNDIKSHA

Gambar. Wawancara tentang Implementasi Sistem SSO UNDIKSHA di Unit Pelaksana Teknis Teknologi, Informasi dan Komunikasi UPT-TIK UNDIKSHA dengan Bapak Putu Marta Rino Ariana, S.Kom selaku Anggota Divisi Pusat Data dan Informasi UPT TIK UNDIKSHA

Lampiran 2 Hasil Wawancara

Wawancara dengan Bapak I Ketut Resika Arthana, S.T., M.Kom selaku Kepala UPT TIK UNDIKSHA pada Tanggal 6 maret 2023

Pertanyaan

1. Metode autentikasi apa yang saat ini digunakan pada sistem SSO Undiksha?
2. Apakah pernah terjadi kebocoran data pada SSO undiksha karena metode autentikasi yang digunakan saat ini?
3. Apakah pihak undiksha ada rencana untuk mengembangkan metode authentikasi lain kedepannya selain metode yang saat ini digunakan?
4. Saya berencana untuk melakukan penelitian tentang pengembangan metode autentikasi menggunakan standar fido2, bolehkah saya minta izin untuk menggunakan SSO Undiksha sebagai studi kasusnya ya pak?

Jawaban

1. Sistem SSO undiksha menggunakan Sistem CAS dengan metode email dan password
2. Untuk kebocoran data karena metode autentikasi email & password belum ada tetapi kelalian pengguna yang membagikan email dan passwordnya ke orang lain
3. Sistem SSO Undiksha sudah terintegrasi dengan Sistem OTP lewat email. Kamu bisa bandingkan nanti kelebihan sistem fido2 yang kamu jelaskan tadi dengan sistem autentikasi yang kami gunakan saat ini.
4. Kamu boleh riview dulu sistem autentikasi kami. Jika kamu mengembangkan autentikasi khususnya yang memanfaatkan biometrik memang kita butuhkan saat ini.

Lampiran 3 Rancangan Verifikasi Blackbox Testing

VERIFIKASI BLACKBOX TESTING PENGUJIAN FUNGSIONALITAS FITUR AUTENTIKASI TANPA PASSWORD PADA SISTEM SSO UNDIKSHA DENGAN TEKNOLOGI FIDO2 PASSKEY

Tujuan : Pengujian Fungsionalitas Fitur Autentikasi

Cara Pengisian : Tulisakan hasil pengujian sesuai hasil yang diperoleh perangkat lunak kemudian beri tanda centang (✓) pada kolom sesuai atau tidak sesuai

No	Uji Coba	Skenario	Penanganan	Hasil	
				Sesuai	Tidak
1	Proses registrasi perangkat baru pengguna	Perangkat user belum terdaftar. perangkat support fido2 dan platform authenticator	Menampilkan tombol pilihan pada menu untuk registreasi perangkat baru		
		Perangkat user belum terdaftar. perangkat tidak support fido2 atau platform authenticator	Tombol registrasi perangkat baru tidak ditampilkan		
		Perangkat user sudah terdaftar dan memiliki kunci fido2 tersimpan dalam perangkat	Tombol registrasi perangkat baru tidak ditampilkan		
2	Proses login menggunakan fido2 passkey	Perangkat support fido2 dan platform authenticator	Menampilkan tombol pilihan login dengan fido2 menggunakan		

			platform authenticator		
		Perangkat support fido2 tetapi tidak support platform authenticator	Menampilkan tombol pilihan login dengan fido2 menggunakan QR kode		
		Perangkat tidak support fido2	Tombol pilihan login dengan fido2 tidak ditampilkan		

Lampiran 4 Rancangan Verifikasi Whitebox Testing

VERIFIKASI WHITEBOX TESTING PENGUJIAN KONSEPTUAL FITUR AUTENTIKASI TANPA PASSWORD PADA SISTEM SSO UNDIKSHA DENGAN TEKNOLOGI FIDO2 PASSKEY

A. Pengujian…

1. Source code dan flow graph
2. Menghitung cyclomatic complexity
3. Tabel perhitungan independent path testing

No	Path	Input	Hasil yang diharapkan	Status

Lampiran 5 Lembar Uji Respon Pengguna

UJI RESPON PENGGUNA FITUR AUTENTIKASI TANPA PASSWORD PADA SISTEM SSO UNDIKSHA DENGAN TEKNOLOGI FIDO2 PASSKEY

A. PETUNJUK PENGISIAN ANGKET

1. Isilah identitas diri anda terlebih dahulu sebelum mengisi angket uji kelayakan ini
2. Beri tanda checklist (✓) pada salah satu kolom pilihan jawaban yang tersedia. Dengan item jawaban sebagai berikut:
    a. SS : Sangat Seteju
    b. S : Setuju
    c. TS : Tidak Setuju
    d. STS : Sangat Tidak Setuju

B. IDENTITAS RESPONDED

Nama :

Jabatan :

Hari/Tanggal :

Pernyataan Uji Respon Pengguna

No.	Kriteria	Alternatif Pilihan			
		SS	S	TS	STS
1	Saya merasa nyaman menggunakan fitur autentikasi FIDO2 ini untuk mengakses SSO Undiksha.				
2	Saya merasa langkah-langkah autentikasi FIDO2 mudah dipahami dan diikuti.				
3	Saya merasa fitur autentikasi FIDO2 memberikan tingkat keamanan yang memadai untuk melindungi akun saya.				

4	Saya merasa proses autentikasi menggunakan FIDO2 cukup cepat dan efisien				
5	Saya lebih memilih fitur autentikasi FIDO2 daripada metode autentikasi lain yang telah saya gunakan di SSO Undiksha sebelumnya.				
6	Tampilan antarmuka fitur autentikasi FIDO2 ini terlihat menarik dan mudah dipahami.				
7	Saya akan merekomendasikan penggunaan fitur autentikasi FIDO2 ini kepada pengguna lain				

Singaraja,

Responded

…….