# 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).

Single Sign-On (SSO) 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 yang telah dipaparkan, 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